UNIVERSITY
OF TRENTO - Italy
Faculty of Law
Department of Legal Sciences

lawtech

Trento Law and Technology Research Group
Student Paper n. 27

Privacy and Health Data: A Comparative Analysis

CAROLINA FOGLIA

a cura di Roberto Caso e Paolo Guarda

ISBN: **978-88-8443-546-0**

COPYRIGHT © 2016 CAROLINA FOGLIA

This paper can be downloaded without charge at:

Trento Law and Technology Research Group

Student Papers Series Index:

http://www.lawtech.jus.unitn.it

IRIS:

http://hdl.handle.net/11572/143778

This paper Copyright © 2016 **Carolina Foglia**

is published with Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Further information on this licence at:

http://creativecommons.org/licenses/by-nc-nd/4.0/

KEYWORDS

Privacy – e-Health – Data Protection – Anonymization – Electronic Health Records

About the author

Carolina Foglia (carolina.foglia92@gmail.com) graduated in Law, *magna cum laude,* at the University of Trento, under the supervision of Prof. Roberto Caso and Dr. Paolo Guarda (March 2016) and obtained a LL.M. in IP & Technology Law in May 2014 from Washington University in St. Louis (U.S.A.) within the Transnational Law Program.
The opinion stated in this paper and all possible errors are the Author's only.

ABSTRACT

The sensitivity of health data has been left unquestioned for centuries, as they translate into words, numbers, and graphs some of our deepest weaknesses. At the same time, information lies at the core of health care, which is largely based on a relationship of trust between physician and patient. This delicate balance has been shaken by the advent of e-Health, a phenomenon that lies at the intersection of Information and Communication Technology (ICT) and health care.

The technological developments of our era increasingly place a blind trust in efficiency as a value per se, avoiding submitting technology to a moral assessment. Maximizing efficiency is extremely appealing, since we are afraid of what goes beyond our control, but it is crucial to realize that efficiency is not an end in itself but rather a means to achieve other goals. In the field of health data, the primary goals should be the protection of human dignity and adherence to the complexity of reality. Instead, the excessive pursuit of efficiency encourages creating simplistic, bright-line solutions that fail to take into account the different nuances and the inherent intricacy of human relationships and activities. The protection of health data must account for the inefficiency and the imperfection embedded in all human things. Therefore, law should not make deceptive promises of perfection and ought to treasure and value inefficiency.

This work is articulated into three chapters, aimed at comparing the legal frameworks of the European Union (with a focus on Italy) and the United States and identifying the challenges engaging legislators on either side of the Atlantic Ocean.

The first Chapter provides an overview of the rules on health data protection, highlighting what triggered the adoption of the relevant legislation and whether it successfully takes into account all the competing interests. Overly technical standards, born more from a desire for smoother transactions rather than for protecting human dignity, often create incentives to formally comply with the standards rather than on achieving the goals.

The second Chapter focuses on electronic health records, which aim at collecting in one place all health data concerning a patient, and inquires into how they have been implemented in Europe and in the United States. Despite several advantages, EHRs also create several risks to patient privacy and often suffer from an excessive simplification of the concept of consent. Technology should be welcomed in the delivery of health care without forgetting that healing is a human activity and patients are not just stacks of data.

The third Chapter concerns the topic of anonymization in the field of health data and criticizes the outdated dichotomy between personal and anonymous data, showing how anonymization should not be regarded as a silver bullet and anonymous data should be surrounded by further layers of protection.

This work shows that rules in health data protection should not be black-and-white and should adopt a risk-analytic approach. "There is a crack in everything […], that's how the light gets in" [L. Cohen]: the impossibility to achieve perfect outcomes is a precious reminder that "data processing systems are designed to serve man" [EU Directive 95/46, Recital 2].

CONTENTS

Introduction

Ring the bells that still can ring
Forget your perfect offering
There is a crack, a crack in everything
That's how the light gets in

(Leonard Cohen, "Anthem", 1992).

Health data translate into words, numbers, and graphs some of our deepest, most sensitive weaknesses. Therefore, this type of data appears inherently worthy of protection. The "sensitivity of and value in protecting health information has been left relatively unquestioned"[1] since the dawn of Western civilization[2]. Information about our frailties deserves significant protection as it touches the core of our personal life. Improper disclosures of health data may not only lead to dignitary harm and stigmatization but also undermine a patient's trust, which is necessary for an accurate diagnosis. Information lies at the core of health care, especially considering that an effective delivery of services largely depends on the accuracy of the information provided to the physician[3]. Therefore, we must carefully assess the consequences of transferring the storage of health data to electronic media.

Health care provision is one of the many fields undergoing thorough transformations with the advent of new technology. Increasingly more activities of our daily life, such as communicating or purchasing goods, are performed through an electronic device within a network. The developing phenomenon of e-Health, which lies at the intersection of Information and Communication Technology (ICT) and health care, features particularly complex paradoxes.

The technological developments of our era increasingly perceive efficiency as the highest value we can pursue[4], as there is a widespread belief that technology is the answer to most issues. It is obviously accurate to say that technology has the potential to solve many problems, but we should not place a blind trust in efficiency as a value *per se*. As Bauman & Lyon have noted in "Liquid Surveillance", this can lead to "adiaphorization", or

---

[1] P. OHM, *Sensitive Information*, 88 *S. Cal. L. Rev.* (forthcoming 2015), at 22. *See also* T. K. HERVEY & J. V. MCHALE, *Health Law and the European Union*, Cambridge University Press, 2004, at 163.

[2] The Hippocratic Oath recites: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about". *See* L. EDELSTEIN, *The Hippocratic Oath: Text, Translation, and Interpretation*, in R.M. VEATCH, *Cross-cultural Perspectives in Medical Ethics*, 2000, at 3. In the original version: Ἃ δ' ἂν ἐν θεραπείῃ ἢ ἴδω, ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπηίης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλέεσθαι ἔξω, σιγήσομαι, ἄῤῥητα ἡγεύμενος εἶναι τὰ τοιαῦτα.

[3] *See* U. IZZO, *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, in *Danno e resp.*, 8-9, 807, 807-08 (2000).

[4] See the critique of "solutionism" by Evgeny Morozov in E. MOROZOV, *To Save Everything Click Here: The Folly of Technological Solutionism*, 2014. He defines "solutionism" as "[r]ecasting all complex social situations either as neatly defined problems with definite, computable solutions or as transparent and self-evident processes that can be easily optimized". *Id.* at 5.

the tendency to avoid submitting technology to a moral assessment and to exclude morality from the discussion[5]. Since we are afraid of realities that go beyond our control, efficiency is appealing because it allows us to manage complex issues and reduce them to a minimum. Our "unquenched and insatiable thirst for order"[6] and for "an ultimate peace of body and mind"[7] makes us "experience every reality as disorderly and calling out for reform"[8]. Thus, the reason why the maximization of efficiency is so appealing is linked with our deep nature, which makes it even more important to avoid addressing such needs with wrong or misused tools. Indeed, efficiency is not an end in itself but rather a means to achieve other goals. As Morozov points out, transparency is an "instrumental" rather than an "intrinsic" value[9]. Replacing our goals with efficiency or with its close friend, transparency, deprives society of discovering what the actual goals should be and instead encourages creating simplistic solutions that disregard the complexity of reality.

Looking more specifically at the realm of health care and data protection, these reflections can shed some light on several of the most debated issues. Due to the particularly sensitive nature of health data, policymakers and legislators should regard the protection of the individual as their primary goal, as in this field data protection amounts to protection of life and human dignity[10]. Nevertheless, the spark for the implementation of data protection legislation has often been the promotion of easier and more efficient data transfers, and data have been mostly seen in light of their flow rather than of their connection with each and every individual.

One of the main underlying arguments of this work is that the pursuit of efficiency as a goal in the delicate transition toward a more technologically advanced health care world has led to overly simplistic black-and-white alternatives with respect to some crucial issues. Because all human things are imperfect, law should not make deceptive promises of perfection but should accept inefficiency and design rules that account for it. The analysis in this work has been carried out through this lens and, when necessary, proposes approaches that better take into account all the nuances.

This work is articulated into three chapters, which also represent three examples of oversimplification. The analysis we have carried out aims at comparing the legal frameworks of the European Union and the United States, which has been enabled and deepened by a period of research in the United States at Washington University in St. Louis. Despite the deep differences, legislators on either side of the Atlantic Ocean seem to be engaged in several common challenges. The analysis of the European scenario has been enriched by a focus on Italy, which not only is my country of origin but also offers a bright example of implementation of the European Data Protection Directive and an interesting approach to e-Health, particularly with respect to electronic health records (EHRs). Indeed, the Italian experience features many excellent local EHR and Personal Health Record

---

[5] Z. BAUMAN & D. LYON, *Liquid Surveillance*, 2013, at 7.

[6] *Id.* at 117.

[7] *Id.* at 116. Bauman writes: "the hub of the human, all-too-human and inherent urge for transcendence is the drive towards comfort and convenience; to a habitat that is neither worrisome nor wearisome, that is fully transparent, holding no surprises and mysteries, never taking us aback or catching us unprepared; a world with not contingencies or accidents, 'unanticipated consequences' or reverses of fate".

[8] *Id.* at 117.

[9] MOROZOV, supra note 4, at 80.

[10] Interview to Antonello Soro (Garante per la protezione dei dati personali), RaiNews 24, October 20, 2015, available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4345229 ("[…] facendo crescere nel nostro Paese, a tutti i livelli, la cultura della protezione dei dati personali, protezione che mai come nella sanità significa protezione della vita: se un mio dato sanitario viene alterato, manipolato, rubato, utilizzato in modo improprio il rischio per me può essere altissimo").

(PHR) systems (such as the TreC project in Trentino Alto-Adige) and an innovative legislation on this topic.

The first Chapter provides an overview of the legal frameworks on health data protection in the European Union and in the United States, by analyzing what triggered the adoption of the relevant legislation and evaluating whether it successfully takes into account all the different interests at stake. This has been carried out, firstly, by discussing the relevant international treaties and provisions of the European Data Protection Directive, and by evaluating the potential impact of the long-awaited General Data Protection Regulation. Secondly, the analysis of the Italian legislation provides some deeper insights with respect to how the Directive operates in practice. Finally, the description of the United States framework looks at the sector-specific Health Insurance Portability and Accountability Act and at the privacy-protective provisions. As we will see, companies and data controllers tend to focus on their compliance with the law rather than on the effective protection of health data, and the implementation of security measures largely amounts to a mere check-the-box activity.

The second Chapter focuses on electronic health records, which represent a very interesting phenomenon within the broader transformation linked to e-Health and the advent of Information and Communication Technology (ICT) in the realm of health care. EHRs aim at collecting in one place all health data concerning a patient, "from the cradle to the grave", and create numerous concerns. Despite the advantages of EHRs, namely less mistakes, lower costs, and more efficient public health reporting, there are also several risks to patient privacy and security. In addition, the law concerning EHRs suffers from an excessive simplification of the issue of consent, a notion we cannot rely on too heavily. Discussing these paradoxes and describing the relevant legal provisions, Chapter II will inquire into how electronic health record systems have been implemented in Europe and in the United States.

The third Chapter concerns the topic of anonymization in the field of health data, which has traditionally been featured by the outdated dichotomy between personal and anonymous data. The Chapter analyzes the relevant provisions in Europe and in the United States and highlights the most significant issues with respect to anonymization – especially of health data that needs to be re-used for scientific research – and proposes some changes in how this topic is usually addressed.

Despite the three chapters deal with different aspects of health data privacy, we can read between the lines the same paradox, consisting in the pursuit of efficiency as a goal and not as a means to a greater end. This work will try to identify the effects of this misunderstanding and propose some paths forward.

Chapter I • An Overview of Health Data Protection in Europe and in the United States

1. Preliminary Considerations

As much as processing personal data has always been integral to human interaction, we are now in the age of "information society" and there is a rapidly growing market in which personal data is traded, so as to be called "the new oil"[1]. This transformation has not only increased the need to establish effective safeguards around the processing of personal data, but it has also opened up a new field of opportunity whereby data privacy law can be used to strike a proper balance between all contrasting stakeholders. The principles and ideals of data privacy law "are amongst the central counterweights to technocratic imperatives, such as increased organizational efficiency and maximization of financial profit"[2]. Data privacy law consists in the "attempt to secure the privacy, autonomy, and integrity of individuals and thereby the bases for democratic, pluralist society in the face of massive growth in the amount of personal data gathered and shared by organizations"[3]. Nowadays, as much as "some of the principles underlying the system of personal data protection are being slowly eroded", "the strong protection of personal data continues to be a 'necessary utopia' (S. Simitis) if one wishes to safeguard the democratic nature of our political systems"[4]. This attempt proves to be particularly relevant when the data is extremely sensitive and close to the core of private life that each person has a fundamental right (as enshrined in most Constitutions and international conventions) to see respected. Health data represent an example of data that are intrinsically linked to the very heart of human life and thus need to be surrounded by such layers of protection so as to take into account all the different implications of processing this kind of data.

This chapter is aimed at providing an overview of the data protection legislation in Europe and the United States, with a focus on the processing of health data. The discussion of the European system will be deepened by an overview of the Italian legal framework, which provides an example of how the Directive has been implemented in practice and faces the challenges posed by health data protection. This will also lead us to investigating the genesis of the relevant provisions, which has largely been triggered by market-related concerns rather than an interest in preserving the privacy and dignity of the individual. Our analysis will compare the two frameworks, highlighting the differences as well as the common features, and inquire into how they balance the interest in safeguarding privacy with the need to allow for efficient transactions and data transfers.

2. Health Data Protection in Europe

In order to understand the privacy legal framework in Europe, it is necessary to analyze both the legal instruments issued by the Council of Europe, paying particular

[1] L.A. BYGRAVE, *Data Privacy Law: An International Perspective*, Oxford University Press 2014, at 4.
[2] *Id.* at 5.
[3] *Id.* at 8.
[4] S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?*, Springer, 2009, p. 78.

attention to the European Charter of Human Rights, and the European Union legislation, which is currently undergoing a process of deep reform with the upcoming General Data Protection Regulation.

2.1 Council of Europe and Other International Law

"Everyone has the right to respect for his private and family life, his home and his correspondence"[5], declares Article 8.1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Indeed, the need to safeguard this fundamental right is the basis of European data protection law[6], even if it has been juxtaposed to the goal of creating a common European market (see paragraph 2.2).

This crucially important provision goes on to specify that "[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[7]. Hence, the ECHR mandates that every public interference with the right to privacy comply with three criteria. First, the basis for the interference must be "set out in an ascertainable law"[8]. For these purposes, rules created by case law fall within the concept of "law", which does not refer to a formal criterion but rather to a substantial one: it must be an accessible, clear and predictable rule[9]. Second, the interference must be pursuing an identified legitimate aim among those listed in Article 8.2. The ends mentioned in this exhaustive list must be given a restrictive interpretation, in compliance with the Strasbourg court jurisprudence[10]. The third requirement, namely the public interest ("necessary in a democratic society"), embodies a case-by-case evaluation based on the concrete circumstances[11]. This balancing test is aimed at allowing the restriction of an individual's right only as long as there is a pressing social need, because "the state cannot use a sledgehammer to crack a nut"[12].

The strength of the ECHR is definitely linked to the case law of the European Court of Human Rights, which has broadly interpreted Article 8 ECHR so as to include

---

[5] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5 [hereinafter "ECHR"], art. 8.1.

[6] *See* P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002, p. 1.

[7] ECHR, art. 8.2.

[8] J. WADHAM, *Human Rights and Privacy – The Balance*, speech given at Cambridge (Mar. 2000), available at: http://www.liberty-human-rights.org.uk/mhrp6j.html.

[9] PALLARO, *supra* note 6, p. 9 (original document in Italian: "Sul dato formale prevale quello sostanziale, che esige norme accessibili, chiare e prevedibili: l'accessibilità dipende dalla pubblicazione o comunque dalla presenza di procedure di comunicazione della "legge"agli interessati; chiarezza e prevedibilità implicano una formulazione che permetta di comprendere l'esatto volere della norma e le conseguenze dei propri comportamenti in relazione ad essa"). In *Sunday Times v United Kingdom* (1979) 2 EHRR 245, at paragraph 49, the Strasbourg court has explained that "the citizens must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case" and that the norm must be "formulated with sufficient precision to enable the citizen to regulate his conduct". Some cases of the European Court of Human Rights have further specified this concept, such as: *Malone/UK* (2 August 1984), *Leander/Sweden* (26 March 1987).

[10] *See* PALLARO, *supra* note 6, at 9.

[11] *See id.*, at 10-11.

[12] WADHAM, *supra* note 8.

telephone conversations, telephone numbers, computers, video-surveillance, voice-recording and Internet and e-mail under its scope[13].

Looking at the history of European data protection, it can be regarded as an "example of legal creativity and perseverance of some of the visionary in the policy making world, realizing that the right to privacy in Article 8 of the European Convention for the protection of human rights and fundamental freedoms […] needed to be complemented to meet some of the challenges created by emerging technologies"[14]. With respect to this endeavor, the Council of Europe was one of the first international bodies to engage in reacting to the challenges arising from new technologies with respect to privacy interests, and it is the only one to have drafted a multilateral treaty dealing directly with this issue[15]. The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[16] represents "the Council of Europe's crowning achievement in the field of data privacy"[17] and sets out some basic principles for the processing of personal data, which at the time had already been largely established but had never before been collected in such an international document. Article 5 of Convention 108 embodies the requirements of data quality, as well as the principles of fair and lawful processing, purpose limitation and minimality, whereas Article 6 mandates stricter rules for certain particularly sensitive categories of data, i.e. data relating to a person's 'intimate private life' or data which 'might lead to unfair discrimination'[18]. This also includes data concerning a person's 'health or sexual life'[19].

The Convention "continues to be a key reference point for shaping regulatory policy", especially given the chance for states that are not members of the Council of Europe to accede to it[20]. The Council of Europe, though, has created some other international documents specific to the field of health data, which we will look at in more detail.

The so-called Oviedo Convention, or Convention on Human Rights and Biomedicine, includes several provisions as to the processing of health data, stipulating that "[e]veryone has the right to respect for private life in relation to information about his or her health" (Article 10 (1))[21]. The Convention is aimed at "protect[ing] the dignity and identity of all human beings and guarantee[ing] everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine" (Article 1) and further specifies a right "to know any information

---

13 P. DE HERT & S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action,* in S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?*, Springer 2009, at 16. For a deeper analysis of the European Court of Human Rights case law, see BYGRAVE, *supra* note 1, at 87-97.

14 DE HERT & GUTWIRTH, *supra* note 13, at 5.

15 BYGRAVE, *supra* note 1, at 31.

16 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) [hereinafter Council of Europe Convention 108], available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. *See* G. GREENLEAF, *'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?*, 29 *Computer Law & Security Review* 430 (2013).

17 BYGRAVE, *supra* note 1, at 42.

18 They have been so described in some resolutions of the Council of Europe. *See* Council of Europe, Committee of Ministers, *Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector*, 26 September 1973; Council of Europe, Committee of Ministers, *Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector*, 20 September 1974.

19 For a deeper analysis of the basic principles and the gaps of Convention 108, see BYGRAVE, *supra* note 1, at 36-41.

20 BYGRAVE, *supra* note 1, at 42-43.

21 Council of Europe, *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, 1997, Article 10 (1), available at: http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm.

collected about his or her health", except for instances in which a wish not to be so informed has been expressed, and exceptional cases which justify restrictions placed by law[22].

Another sectorial document specifically dealing with health data protection is the Council of Europe Recommendation R(97)5[23], which states that health data can be collected and processed, if provided for by law, for public health reasons, for the prevention of a real danger, for the suppression of a specific criminal offense or for another important public interest[24]. Such data can also be used, if allowed by law, for preventive medical purposes or for diagnostic or therapeutic purposes with regard to the data subject or a relative in the genetic line, or for other specified aims[25]. The definition of medical data provided by the Recommendation is "all personal data concerning the health of an individual", including "data which have a clear and close link with health as well as to genetic data"[26]. The Recommendation includes some provisions tackling the issue of secondary uses of health data for scientific research. Under Article 12, "[w]henever possible, medical data used for scientific research purposes should be anonymous"[27], but a relevant exception is carved out if "the project is to be carried out for legitimate purposes": "if such anonymisation would make [the] scientific research project impossible, […] it could be carried out with personal data" in three different scenarios[28]. First, it is allowed if the data subject (or his or her representative) has given his or her informed consent[29]. Alternatively, "disclosure of data for the purpose of a defined scientific research project concerning an important public interest [must have] been authorised by the body or bodies designated by domestic law", as long as "the data subject has not expressly opposed disclosure", and "despite reasonable efforts, it would be impracticable to contact the data subject", and where "the interests of the research project justify the authorisation"[30]. Finally, the exception also applies when "the scientific research is provided for by law and constitutes a necessary measure for public health reasons"[31]. For further thoughts on anonymization in the field of health data, see Chapter III.

The consent of the data subject plays a pivotal role in the Recommendation, and it needs to be "free, express and informed"[32]. The Recommendation echoes Directive 95/46/EC (see paragraph 2.2) providing that "in general, medical data shall be kept no longer than necessary to achieve the purpose for which they were collected and processed"[33] or, if it proves necessary to conserve it for a longer period of time, "technical arrangements shall be made to ensure their correct conservation and security, taking into account the privacy of the patient"[34].

The data subject has the right to have access to his or her medical data, as well as the right to "ask for rectification of erroneous data concerning him/her"[35]. Also, the data

---

[22] *Id.*, Article 10 (2) and (3).
[23] Council of Europe, Committee of Ministers (1997), *Recommendation R(97)5 to member states on the protection of medical data*, 13 February 1997.
[24] *Id.*, art. 4.3 (a).
[25] *Id.*, art. 4.3 (b).
[26] *Id.*, art. 1.
[27] *Id.*, art. 12.1.
[28] *Id.*, art. 12.2.
[29] *Id.*, art. 12.2 (a) and (b).
[30] *Id.*, art. 12.2 (c).
[31] *Id.*, art. 12.2 (d).
[32] *Id.*, art. 6.
[33] *Id.*, art. 10.1.
[34] *Id.*, art. 10.2.
[35] *Id.*, art. 8.1 and 8.3.

subject has the right to see his or her medical data erased upon his or her request, unless "they have been made anonymous or there are overriding and legitimate interests, in particular those stated in Principle 10.2 not to do so, or there is an obligation to keep the data on record"[36].

In order to guarantee data security, the Recommendation encourages the adoption of "appropriate technical and organizational measures"[37], which "shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks"[38]. Articles 7 and 11 refer to the cases of communication of data and trans-border data flows, and aim at the creation of policies in order to maintain an adequate level of privacy.

2.2 Data Protection in the European Union

The principal EU law on data protection is the Data Protection Directive 95/46/EC[39], which is widely considered "the most significant piece of data protection legislation in the world today"[40], and "has served as a blueprint for data protection regimes subsequently established across the globe"[41]. Despite being "a rare example of EU regulatory supremacy"[42], its application throughout the years has revealed some shortcomings that the European legislators are trying to address[43].

The Data Protection Directive "introduces a relatively comprehensive vision of what protection of data privacy should involve and it lays down a relatively rigorous set of rules", specifying "in relatively great detail a baseline for data privacy from which member states cannot derogate"[44]. Member states can establish or maintain a higher level of privacy, but they cannot derogate from any of the mandatory requirements, nor can they introduce more narrowly framed exemptions to the Directive's general rules than the ones specified[45].

The goal pursued by the Directive consists in striking a balance between, on one hand, the acknowledgment of how "data-processing systems are designed to serve man"[46] and the objective of free movement of personal data, and on the other hand, the protection of "fundamental rights and freedoms, notably the right to privacy"[47]. On this reading, it looks like the Directive has a "split personality": which of these two potentially contradictory goals (protection of fundamental rights vs. market integration) is the overriding one? The Court of Justice has not always been unequivocal as to the definition

---

[36] *Id.*, art. 10.3.
[37] *Id.*, art. 9.1.
[38] *Id.*
[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, November 23, 1995, P. 0031 - 0050 [hereinafter Data Protection Directive], available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[40] O. TENE, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 *Ohio St. L.J.* 1217, 1220 (2013).
[41] O. LYNSKEY, *From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis*, in S. GUTWIRTH ET AL. (eds.), *European Data Protection: Coming of Age*, Springer, 2013, p. 59.
[42] *Id.*
[43] *See* TENE, *supra* note 40, at 1224.
[44] BYGRAVE, *supra* note 1, at 59.
[45] *Id.* at 60.
[46] Data Protection Directive, Recital 2.
[47] *Id. See also* Art. 1.1.

of the "identity" of the Directive, but in recent years it has leaned towards highlighting the fundamental rights dimension at the expense of the "market-making" objective[48].

Yet, the creation of a "uniform market at the European level for personal data" was the "initial dream" of the drafters of the Directive[49]. According to the European legislator, a consistent regulation of the cross-border flow of personal data is "vital to the internal market"[50] because "the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data" could create a hurdle for the transmission of data between Member States, ultimately causing a distortion of competition[51]. The importance of the market harmonization goal is demonstrated by the choice of Article 100a of the EC Treaty (now Article 114 TFEU) as legal basis[52]. In fact, this provision allows the adoption of measures to approximate national law, regulation or administrative action aiming at the establishment and functioning of the internal market[53]. However, the choice of this (only) legal basis, which "ignores [the] fundamental rights objectives[54] of the Directive, has been considered "at best, controversial", as the goal of securing a high level of fundamental rights protection in the field of data processing was never considered secondary[55]. Now, the question as to the legal basis of data protection law is moot due to the introduction – with the Treaty of Lisbon of 2009[56] – of a directly effective right to data protection in Article 16 TFEU, which states that "[e]veryone has the right to the protection of personal data concerning them"[57].

Indeed, "rights language permeates the text of the Directive as a whole"[58], as we can see in the very first provision (Article 1.1), and this has arguably had implications in terms of its interpretation. It has been argued that the Court of Justice case law has had "the effect of loosening the Directive's links with its stated market harmonization objective", due to a broad interpretation of the Directive's scope of application and to the great degree of leeway left to national authorities in the implementation[59]. Just shy of ten years ago, it was already true that this broad discretion left to the Member States in implementing the Directive made it difficult to compare the different national regimes[60]. The new General Data Protection Regulation[61] resulted from a need for deeper integration, and "signal[ed] a very important shift in the way data protection will be handled in the future throughout the

---

48 LYNSKEY, *supra* note 41, at 59.
49 Y. POULLET, *The Directive 95/46/EC: Ten years after*, 22 *Computer Law & Security Report* 206, 207 (2006).
50 Data Protection Directive, Recital 8.
51 *Id.*, Recital 7.
52 LYNSKEY, *supra* note 41, at 60.
53 Consolidated Version of the Treaty on the Functioning of the European Union art. 114, 2008 O.J. C 115/47.
54 LYNSKEY, *supra* note 41, at 60.
55 *Id.* at 63. For a discussion as to whether the Directive should have been enacted using two legal bases, *see id.* at 64-65.
56 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306.
57 Consolidated Version of the Treaty on the Functioning of the European Union, O.J. C 115/47, 2008, art. 16,
58 T.K. HERVEY & J.V. MCHALE, *Health Law and the European Union*, Cambridge University Press 2004, at 167.
59 LYNSKEY, *supra* note 41, at 65. *See* Data Protection Directive, Recital 9 and Article 5.
60 POULLET, *supra* note 49, at 207.
61 The consolidated text of the new Regulation can be found at: http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf. *Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, December 15, 2015 [hereinafter GDPR – Consolidated text].

European Union"[62], first and foremost with respect to the chosen legislative instrument. The choice of a regulation, instead of another directive, for the new data protection framework "should provide greater legal certainty by introducing a harmonized set of core rules that will be the same in each Member State"[63], but arguably will also lead to growing tensions between the Member States[64].

If ever the objective of protecting fundamental rights was merely ancillary to the market integration goal (which it probably was not), the inclusion of data protection among the fundamental rights enshrined in the EU Charter of Fundamental Rights[65] would appear even more noteworthy[66]. Article 7 of the EU Charter echoes Article 8 of ECHR establishing a "right to respect for his or her private and family life, home and communications", whereas Article 8 specifically concerns the protection of personal data. It lists the general baselines for the processing of data, which must be fair, "for specified purposes" and based on "the consent of the person concerned or some other legitimate basis laid down by law". Also, it provides for the data subject's "right of access to data concerning him or her, and the right to have it rectified"[67].

The recognition of data protection as a fundamental right in the EU legal framework constitutes a very important step in many respects. It clearly emphasizes the fundamental rights dimension of the Directive, which had until then been shadowed by the many business-friendly provisions[68]. Furthermore, it accounts for the distinction between "data protection" and "privacy", which are not interchangeable[69] insofar as "data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualisations of privacy"[70]. It is thus "the final point of a long evolution, separating privacy and data protection"[71].

Article 8 is part of the attempt by the EU Charter to tackle the issues arising from scientific and technological innovation while "plac[ing] the individual at the heart of its activities"[72]. The protection of the physical body is entrusted to Article 3 ("Right to the integrity of the person"), whereas Article 8 deals with "the electronic body"[73]. Both are

---

62 F. GILBERT, *European Data Protection 2.0: New Compliance Requirements in Sight – What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 *Santa Clara Computer & High Tech. L.J.* 815, 816 (2012).

63 F. GILBERT, *Proposed EU Data Protection Regulation: The Good, The Bad, And The Unknown*, 15 *Journal of Internet Law* 1, 3 (2012).

64 LYNSKEY, *supra* note 41, at 81.

65 *Charter of Fundamental Rights of the European Union of the European Parliament*, December 7, 2000, O.J., No. C 364, 2000 [hereinafter EU Charter of Fundamental Rights].

66 LYNSKEY, *supra* note 41, at 80.

67 The full text of Article 8 ("Protection of personal data") of the EU Charter of Fundamental Rights reads: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

68 DE HERT & GUTWIRTH, *supra* note 13, at 9.

69 *Id.*

70 *Id.* at 10 (citing L. BYGRAVE, *'The Place Of Privacy In Data Protection Law'*, *University of NSW Law Journal*, 2001, (6p.), sub § 18 (via http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html)). See *id.*, arguing that the recognition of a separate right to data protection is also more respectful of the European constitutional history, which is composed of many distinctive approaches throughout the different countries.

71 RODOTÀ, *supra* note 4, at 79. He underlines that the right to respect one's private life "mirrors, first and foremost, an individualistic component", as "this power basically consists in preventing others from interfering with one's private and family life", whereas data protection "is a dynamic kind of protection", as it "sets out rules on the mechanisms to process data".

72 EU Charter of Fundamental Rights, Preamble.

73 RODOTÀ, *supra* note 4, at 80.

directly linked to human dignity, and therefore "data protection contributes to the constitutionalisation of the person"[74], as "it has turned into an essential tool to freely develop one's personality"[75].

Together with the Data Protection Directive, which represents the main existing legal instrument concerning privacy in the EU, there are some other Directives in the same field. First of all, the 'Directive on Privacy and Electronic Communications' (Directive 2002/58/EC) [76] applies "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". The Directive factors in recent developments in electronic communications technologies, so as to be "technologically neutral and hence to apply to transactions over the Internet in the same way as to transactions using telephone or fax"[77]. It represents an extra set of rules which applies only to the electronic communications sector. Also, the EU has adopted a Directive on 'e-Commerce' (Directive 2000/31/EC)[78], which harmonizes law with respect to "information society services", including commercial communications, electronic contracts and codes of conduct. Since this Directive applies to online services, it applies to online medicine and, more broadly, to "for example, the use of electronic cancer registration files by physicians who pay a fee for accessing the file, the setting up of a web site of a physician promoting his activities, the sending of medical information among physicians for compensation"[79]. Under the Directive, Member States have a duty to ensure that any information society services offering is done in compliance with national professional rules, such as professional secrecy[80].

2.3 The Processing of Personal Data in Europe

First and foremost, we need to focus on the definition of "processing" and "personal data" provided by the Directive. "Processing" means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"[81]. It cover processing of data both by automatic means (computer)[82] and by other means "which form part of a filing system or are intended to form part of a filing system"[83]. In the health care field, this encompasses hospital records, records held by medical professionals that operate outside a hospital context and records relating to medical research, as long as data is sufficiently

---

[74] *Id.* (internal quotation marks omitted).
[75] *Id.*
[76] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications) 2002 O.J. (L 201) 37 (July 31, 2002).
[77] P. CAREY, *Data Protection Law. A Practical Guide to UK and EU Law*, Oxford University Press, 2nd edition, 2004, at 11.
[78] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (E-Commerce Directive), 2000 O.J. (L 178) 1 (July 17, 2000).
[79] S. CALLENS, *Telemedicine and the E-Commerce Directive*, 9 *European Journal of Health Law* 93, 95 (2002).
[80] HERVEY & MCHALE, *supra* note 58, p. 166.
[81] Data Protection Directive, Art. 2(b).
[82] *Id.*, Art. 3(c).
[83] *Id.*, Art. 3(1).

individualized and held in a systematic manner[84]. Even the traditional manual filing systems of health care practitioners are covered since the data do not need to be held in electronic form[85].

Article 2(a) of the Data Protection Directive provides a very broad definition of "personal data" – reflecting the intention of the European legislator [86] – that includes "any information relating to an identified or identifiable natural person ('data subject')[87]. The text goes on to specify that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[88]. Article 2(a) of the Convention 108 of the Council of Europe[89] and the European Court of Human Rights' jurisprudence[90] follow in the same direction (see Paragraph 2.1). All of these sources grant protection to information containing data about a person, both when the individual is identified in this information and when the individual, though not identified, is described in a way which makes it possible to find out who he is through further research[91]. Chapter III of this work will provide some further insights on the concept of "personal data" while dealing with anonymization.

The aforementioned European legal documents establish a number of core principles in the field of data protection that we will try to briefly analyze[92].

The main principle of data protection laws, which "embraces and generates the other core principles of data protection"[93], is that "[p]ersonal data must be processed fairly and lawfully"[94]. While the notion of "lawfulness" is "relatively self-explanatory", that of fairness is "[l]ess obvious in meaning but potentially broader", as well as subject to change over time[95]. At a general level, it surely includes an obligation for data controllers to "take account of the interests and reasonable expectations of data subjects" and to collect and process personal data so as to not unreasonably intrude upon the data subjects' privacy[96], following standards of balance and proportionality. Not only does fairness "militate[ ] against surreptitious collection and further processing of personal data", but it also forbids deception as to the nature and purposes of the processing; therefore, processing can be called "fair" only if it is "transparent"[97].

Strictly connected to the fair and lawful processing principle is the minimality principle, requiring that "the amount of personal data collected should be limited to what is

---

[84] HERVEY & MCHALE, *supra* note 58, p. 169.

[85] *Id.*

[86] *See* European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, at 4 (June 20, 2007) [hereinafter Article 29 WP Opinion 4/2007 on the concept of personal data], available at http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/opinion_04-2007_personal_data_/Opinion_04-2007_personal_data_en.pdf.

[87] Data Protection Directive, Art. 2(a).

[88] *Id.*

[89] Council of Europe Convention 108, Art. 2(a). It establishes that "'personal data' means any information relating to an identified or identifiable individual ("data subject")".

[90] *See, e.g.*, *Amann v. Switzerland*, No. 27798/95, 2000-II Eur. Ct. H.R., § 65.

[91] Handbook on European data protection law (2014), available at http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law, at 39.

[92] *See* L.A. BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits,* Kluwer Law International 2002, at 57-69, 334-362; HERVEY & MCHALE, *supra* note 58, at 168-69; CAREY, *supra* note 77, at 5-8.

[93] BYGRAVE, *supra* note 92, at 58.

[94] Data Protection Directive, Art. 6 (1) (a).

[95] BYGRAVE, *supra* note 92, at 58.

[96] *Id.*

[97] *Id.* at 59.

necessary to achieve the purpose(s) for which the data are gathered and further processed"[98]. The Data Protection Directive clearly sets out this principle in Article 6 (1) (c), according to which personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[99], and Article 5 of the CoE Convention is almost identically worded[100]. Both documents attempt at ensuring minimality not only at the stage of data collection, but also subsequently, by requiring "personal data to be erased or anonymised once they are no longer required for the purposes for which they have been kept"[101].

Pursuant to another fundamental guideline – the "purpose specification" or "use limitation" principle – personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"[102]. This principle is "prominent in all of the main international data protection instruments as well as in most of the national laws"[103]. The wording of the Directive evokes a "legitimacy" requirement, as does Convention 108. However, some laws require that purposes shall be "lawful": as much as it can be argued that "the notion of 'legitimate' denotes a criterion of social acceptability", "[t]he bulk of data protection instruments comprehend legitimacy *prima facie* in terms of procedural norms hinging on a criterion of lawfulness", and "[v]ery few expressly operate with a broader criterion of social justification"[104].

A fourth principle is the data quality principle, requiring personal data to be, first, "valid with respect to what they are intended to describe" and, secondly, "relevant and complete with respect to the purposes for which they are intended to be processed"[105]. With respect to the first prong, concerning validity, personal data must be "accurate and, where necessary, kept up to date"[106], and "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"[107]. Under the second prong, the Directive requires personal data to be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[108].

Finally, there is an obligation upon data controllers to implement measures, both technical and organizational, to protect personal data, as established by Article 17 of the Data Protection Directive[109] and Article 7 of Convention 108[110].

---

[98] *Id.*

[99] Data Protection Directive, Art. 6 (1) (c).

[100] Council of Europe Convention 108, Art. 5 (c) ("Personal data undergoing automatic processing shall be: […] adequate, relevant and not excessive in relation to the purposes for which they are stored").

[101] BYGRAVE, *supra* note 92, at 60. Article 6 (1) (e) of the Data Protection Directive provides that "[p]ersonal data must be […] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". Council of Europe Convention 108 similarly states, in Article 5 (e), that personal data must be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored". See Chapter III for a deeper analysis of the legal issues concerning anonymization.

[102] Data Protection Directive, Art. 6 (1) (b).

[103] BYGRAVE, *supra* note 92, at 61. *See* Council of Europe Convention 108, Art. 5 (b); Principle 3 of the UN Guidelines; para 9 of the OCED Guidelines.

[104] BYGRAVE, *supra* note 92, at 61-62.

[105] *Id.* at 62.

[106] Data Protection Directive, Art. 6 (1) (d); Council of Europe Convention 108, Art. 5 (d).

[107] Data Protection Directive, Art. 6 (1) (d).

[108] *Id.*, Art. 6 (1) (c).

[109] *Id.*, Art. 17. Article 17 (1) states: "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful

2.4 The Processing of Health Data in the EU

2.4.1 Definition of Health Data

Before engaging in an analysis of when the Directive allows for some exceptions concerning the processing of sensitive categories of data, we need to inquire into what the concept of "data concerning health" encompasses in the current legal environment, as the Directive does not provide a definition (a gap which will be bridged by the Regulation, see paragraph 2.5.1). It is interesting to point out that "[t]here is an implicit assumption that health data is different and sensitive"[111]. The assumption that all health care information is *prima facie* confidential is in accord with traditional approaches to confidentiality, but some commentators argue that this is highly relative[112]. For instance, the European Court of Justice considered "information on a home page stating that a [person] has injured her foot and is on half-time on medical grounds" as included in "personal data concerning health" within the meaning of Article 9[113]. This kind of information may be unlikely to be sensitive, while other conditions are regarded as inherently sensitive (e.g. AIDS or mental illness) because of the risk of stigmatization[114]. The Directive adopts the approach that these two extreme situations and everything in between is sensitive information, but that exceptions may be recognized[115]. Yet, it is unclear whether health data as such can be construed to include data that is not strictly related to health but may concern health if analyzed with reference to a complex illness, such as information concerning lifestyle or environmental conditions[116]. Arguably, though, this kind of data can be included because it "concerns" health.

2.4.2 When Is The Processing of Health Data Allowed?

Under Article 7, 'ordinary' personal data may only be legitimately processed if the data subject has unambiguously expressed his or her consent; however, in a number of specific circumstances (which will be explained in further detail below) implied consent will be seen as sufficient[117]. Article 8 (1), as well as Article 6 of the Council of Europe

---

destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".

[110] Council of Europe Convention 108, Art. 7 – Data Security: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination".

[111] HERVEY & MCHALE, *supra* note 58, p. 171.

[112] *Id.*

[113] European Court of Justice, Judgment of 6 November 2003, Case C-101/01 - *Bodil Lindqvist*.

[114] *See* HERVEY & MCHALE, *supra* note 58, p. 171-72.

[115] *Id.* at 172. Harvey and McHale note that there have been suggestions in favor of a process of "negotiated confidentiality" (*see*, e.g., I. THOMPSON, *The Nature of Confidentiality*, 5 *Journal of Medical Ethics* 57 (1979)), but that this kind of approach would be in practice disproportionately expensive and cumbersome.

[116] T. SCHULTE IN DEN BÄUMEN, D. PACI, D. IBARRETA, *Data Protection in Biobanks – A European challenge for the long-term sustainability of Biobanking*, in *Revista de Derecho y Genoma Humano*, 31, 2009, at 13, 19.

[117] Data Protection Directive, Art. 7. The data subject's consent is not needed when: "(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are

Convention No. 108, forbids the processing of certain categories of personal data deemed more sensitive[118]. Among such strongly protected categories are "data concerning health or sex life". Indeed, medical data are among the most intuitively "sensitive" types of information, as confirmed by the findings of the Eurobarometer 2011. According to this survey, 74% of Europeans consider "medical data" as personal information [119]. Interestingly, Internet users appear to be more likely to agree with this view compared with respondents who do not use the Internet[120].

As hinted at, some exceptions to the general prohibition of the processing of personal "data concerning health" are carved out in the Directive: "mandatory derogations" are laid down in Article 8 (2) and (3) and an "optional exemption" is provided by Article 8 (4)[121]. All these provisions "are limited, exhaustive and have to be construed in a narrow fashion"[122].

Pursuant to Article 8 (2) (a) of the Directive, the first possible justification for the processing of sensitive data is the consent of the data subject, which is valid only if it consists in a "freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2 (h)). These features must be the object of a careful assessment, as described by the Article 29 Working Party. Consent must be "unambiguously given" and therefore explicit, but it does not need to be written[123]. As complicated as it can be to obtain consent, the data controller must be able to prove that he or she has obtained the explicit consent of the data subject and that it was given based upon sufficiently detailed information [124]. Interestingly, a minority of Member States restricted these exceptions further: for example, "the Belgian law requests a 'written' consent instead of an 'explicit' consent to process health-related data"[125].

Consent is "freely given" only if it is "a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion". Therefore, in the medical environment, any consent given either "under the threat of non-treatment or lower quality treatment", or without having had "the opportunity to make a genuine choice", or that "has been presented with a *fait accompli*" cannot be considered as free[126].

---

overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)". *See* HERVEY & MCHALE, *supra* note 58, at 169-70.

[118] Council of Europe Convenion 108, Article 6 – Special categories of data: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions".

[119] Special Eurobarometer 359 – "Attitudes on Data Protection and Electronic Identity in the European Union" (2011) (i.e, the largest public opinion survey ever conducted about European citizens' behavior about privacy, on behalf of the European Commission), available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, p. 12. *See also id.* at 16.

[120] *Id.* at 16.

[121] European Union Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, 00323/07/EN WP 131 (February 15, 2007) [hereinafter Article 29 WP Working Document 2007 on EHR], available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, at 8.

[122] *Id.*

[123] *Id.* at 9.

[124] *Id.*

[125] J. DUMORTIER & G. VERHENNEMAN, *Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the U.S.*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (eds.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 29.

[126] Article 29 WP Working Document 2007 on EHR, at 9.

Also, consent needs to be "specific", i.e., it "must relate to a well-defined, concrete situation in which the processing of medical data is envisaged": a general agreement is not considered sufficiently specific[127].

The concept of consent is understood to be "informed", that is, "based upon an appreciation and understanding of the facts and implications of an action", which also includes "an awareness of the consequences of not consenting"[128]. The Directive itself does not clarify the exact boundaries of informed consent, though, and there is considerable divergence across the EU Member States[129].

In some instances, as specifically envisaged by Article 8 (2) (a), not even consent can lift the general prohibition, and Member States are left free to regulate such hypotheses, which is particularly relevant in the context of Electronic Health Records (see Chapter II). This provision shows an awareness of the risk lurking in treating consent as an automatic, never-failing protection. This is especially the case in the context of health services relationships, featured by an imbalance of power and where the data subject is more often than not subject to pressure, especially considering how the possibility of obtaining goods and services is nowadays more and more dependent on the transfer of personal data[130]. It is interesting to highlight how in the Directive consent is given a crucial role yet it is nevertheless one of the exceptions to the general prohibition. The same path was followed by the French legislator, whereas in Italy consent is viewed as the main requirement for the processing of sensitive data rather than an exception to a general ban. The French and EU perspective has been defined as "more consistent with the actual role of consent resulting from the balancing of the implicated interests", also considering that not even in the Italian legislation is consent per se sufficient, as there are plenty of elements which downsize its importance[131]. Other commentators, though, have taken the view that the Directive should not start with a prohibition but rather should allow the processing of health data under certain conditions or limit the ban specifically to the communication of health data, as opposed to all kinds of processing[132].

It is easy to understand how consent represents an effective protection as long as the data subject is provided with exhaustive and thorough information. Recital 38 underlines that "the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection" (see paragraph 2.4.3).

Another justification for processing sensitive data, envisioned by Article 8 (2) (c), is represented by the necessity to "protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent". In

---

127 *Id.*

128 *Id.* at 9. *See also* Data Protection Directive, Art. 6, stating that data may be collected only for "specific, explicit and legitimate purposes"; Art. 7 (a), requiring consent to be given "unambiguously"; Recital 70, referring to "informed consent".

129 HERVEY & MCHALE, *supra* note 58, p. 176.

130 V. PEIGNÉ, *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e divergenze*, in *Diritto dell'Internet*, 2008, 3, 296, 298. See also S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 600.

131 PEIGNÉ, *supra* note 130, p. 298 (original document in Italian: "L'esigenza di non accordare un ruolo assoluto all'autonomia è sottolineata dalla posizione del consenso nelle norme, comunitarie e francesi, dove esso appare come una delle eccezioni al divieto di trattare i dati sensibili. Tale impostazione appare più conforme al ruolo effettivo del consenso conseguente al necessario bilanciamento degli interessi coinvolti e rispetto al quale la legge italiana non fa eccezione, stabilendo numerose previsioni che ne ridimensionano l'efficacia".)

132 *See* S. CALLENS, *The Privacy Directive and the Use of Medical Data for Research Purposes*, 2 *European Journal of Health Law* 309, 320 (1995), cited by HERVEY & MCHALE, *supra* note 58, at 179.

the medical context, this refers to life-saving treatments in situations where the data subject is not able to express his intentions and "processing of his personal data [is] needed in order to facilitate emergency treatment necessary to save his life"[133]. This provision therefore only applies to a handful of cases and cannot be stretched so as to apply to general medical research[134].

Article 8 (3) lays down another situation in which the processing of sensitive personal data is allowed, i.e., "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". As we can see, the protection of privacy is here pursued through the creation of a strict set of boundaries around the data processing activity[135]. This rule applies in the presence of three cumulative requirements. First, the processing must take place "for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these health care services, e.g. invoicing, accounting or statistics"[136]. The exception carved out by Article 8 (3) does not cover further processing which does not aim at these specific goals. Medical research and the procedures related to claims in the health insurance system are outside the scope of this rule[137]. Secondly, the processing of personal data must be "required", and not merely useful, for the afore-mentioned specific purposes[138]. The third condition refers to the subjects entitled to perform the data processing, who must be subject to "professional secrecy" or "an equivalent obligation of secrecy". The extension of such obligation of secrecy – which is indeed one of the 'traditional' tools of privacy protection – to subjects who are not physicians but nevertheless have contacts with sensitive data for a health care purpose follows the evolution of medicine. This field is no longer featured by bilateral relationships but rather by an increasing variety of subjects who participate in providing medical treatment[139]. As pointed out by the Article 29 Working Party, the obligation of professional secrecy must be either set up by the national laws of the Member states or by binding rules established by national competent professional bodies, and such rules must provide for effective sanctions in case of breach[140]. An equivalent level of confidentiality and protection must be ensured for the cases in which it is necessary for non-medical staff to process such data. Rules containing an obligation that the data will only be used for the specific purposes mentioned under Article 8 (3) must be implemented[141].

An "optional exemption" is set up by Article 8 (4), which allows the Member States to lay down additional exemptions "for reasons of substantial public interest", a possibility that is also envisioned by Recital 34. This exemption, according to Article 8 (4), must have a "special legal basis"[142], as it needs to be established "either by national law or by decision of the supervisory authority". Recital 34 provides examples of areas where cases of "substantial public interest" are more likely to occur, such as "public health and social

---

133 HERVEY & MCHALE, *supra* note 58, at 176.
134 Article 29 WP Working Document 2007 on EHR, at 9-10.
135 *See* PEIGNÉ, *supra* note 130, p. 301.
136 Article 29 WP Working Document 2007 on EHR, at 10.
137 *Id.*
138 *Id.*
139 *See* PEIGNÉ, *supra* note 130, at 301.
140 Article 29 WP Working Document 2007 on EHR, at 11.
141 *Id.*
142 *Id.* at 12.

protection – especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system – scientific research and government statistics". Other cases of public interest can be implied "from the general tenor of the Directive, which makes special provisions among others for national security, the investigation and prosecution of crimes, legitimate journalistic activities, and research"[143]. The Member State bears the burden of showing the substantial public interest for each case, and the processing must be necessary in the light of the interest and proportionate[144]. Under Recital 34, Member States also have an obligation to "provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals"[145].

2.4.3 Individual Rights

The EU data protection framework affords to individuals a set of rights in light of the fact that "[i]ndividuals are handicapped in the data processing process, in that processing does not take place in the open but rather behind closed doors", which makes them "mostly unaware when and how their data are being processed"[146]. In the health care field, after many years of debates as to whether it is wise for patients to be entitled to access their own health records, it is now a well-established principle that data subjects have control rights over their personal information, as provided by Articles 10 and 11 of the Data Protection Directive[147]. The fundamental rights approach adopted by the Directive has prevented Member States from adopting "paternalistic models of regulation, under which data with respect to a patient is kept from him 'for his own good', or is communicated to a patient only by the intermediary medical professional"[148].

Thus, the data subject has first of all a right to be informed. Articles 10 and 11 give further details on the information to be provided. Pursuant to Article 10, in case the data have been collected from the data subject, national laws should require the controller to inform the subject about (a) the identity of the controller (and of his representative, if any), (b) the purposes of the processing, and (c) any further information insofar as it is necessary pertaining to the specific circumstances. Some examples of the last type of information are: the recipients of the data, the consequences of failure to reply to the questions, the existence of the right to access and of the right to rectify the data. On the contrary, under Article 11, where the data have not been collected from the data subject, Member States are asked to set out a requirement that the controller give the data subject the information mentioned in Article 10 "at the time of undertaking the recording of personal data or if disclosure to a third party is envisaged, no later than the time when the data are first disclosed". Article 11 (2), however, creates an exception to such an obligation in which Member States need to "provide appropriate safeguards", under two different circumstances. The first instance concerns cases where informing the data subject "proves

---

[143] G. LAURIE, *Genetic Privacy*, Cambridge: CUP, 2002, at 253.

[144] Article 29 WP Working Document 2007 on EHR, at 12. Furthermore, the Article 29 Working Party highlights that, for any interference with the right to private and family life, this provision must also be read in light of Article 8 of the European Convention on Human Rights and of the Strasbourg jurisprudence, which means that it must be done "in accordance with the law" and be "necessary in a democratic society" for a public interest purpose. *See id.*

[145] More concisely but consistently, Article 8 (4) requires "the provision of suitable safeguards".

[146] P. DE HERT & V. PAPAKONSTANTINOU, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, 28 *Computer Law & Security Review* 130 (2012).

[147] Data Protection Directive, Art. 10.

[148] HERVEY & MCHALE, *supra* note 58, at 187.

impossible or would involve a disproportionate effort", "in particular for processing for statistical purposes or for the purposes of historical or scientific research" [see paragraph 2.4.4]. The second exception applies to cases where "recording or disclosure is expressly laid down by law" [149].

Also, under Article 12 there is a right to access personal data "without constraint, at reasonable intervals and without excessive delays or expense". Such right of access concerns: "confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed"; "communication to him in an intelligible form of the data undergoing processing and of any available information as to their source"; and "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of [certain] automated decisions"[150].

Member States may establish limitations to the scope of these rights under Article 13, in order to safeguard, *inter alia*, the data subject himself[151]. Because these provisions need to be passed with "legislation", the provision of a professional ethical code probably would not comply with the Directive. However, as long as legislation so provides, the access to one's own medical records can be restricted when it would cause harm[152]. Thus it has been said that "whilst it is the case that privacy rights are enhanced through the Directive, the right to privacy is circumscribed by paternalism where there is a perceived clinical need to safeguard the interests of the patient"[153].

We can note that "Member States restrictions to the data subject's access right vary a lot": for instance, in Portugal it "can only be exercised via a physician", whereas in Belgium "the patient should be able to access his health-related data directly unless the disclosure of the information can be prejudicial to the patient's medical or physical health"[154].

2.4.4 Clinical and Scientific Research

Particularly significant is the issue of the application of the Directive in the context of clinical and scientific research.

The scope of the Directive does not cover data that does not refer to the living – which allows the processing of data held over long periods of time – nor anonymized data, i.e., data that does not refer to an identified or identifiable data subject (for a deeper analysis of this issue, see Chapter III].

Furthermore, Article 6 provides that "[f]urther processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards"[155]. This has been argued to be "potentially controversial", as "a data subject may disagree with his or her data being used for a specific

---

[149] Data Protection Directive, Art. 10 and Art. 11. *See* HERVEY & MCHALE, *supra* note 58, at 182-83; CAREY, *supra* note 77, at 7-8.
[150] *Id.*, Art. 12.
[151] *Id.*, Art. 13 (1) (g).
[152] HERVEY & MCHALE, *supra* note 58, at 183.
[153] *Id.* at 184.
[154] DUMORTIER & VERHENNEMAN, *supra* note 125, at 30. "This difference causes a Belgian patient receiving eHealth services from a provider established in Portugal to need a physician to access his electronic health record", whereas "[w]hen his electronic health record would be processed by a healthcare professional in Belgium, he would be allowed to access it directly". *Id.*
[155] Data Protection Directive, Art. 6.1(b).

research project, and in general it is unwise to assume that consent to process the data can necessarily be implied"[156].

Pursuant to Article 11 (1), if health researchers receive the data from third parties, when the data is recorded or no later than when it is first disclosed, they must inform the data subject as to the controller's identity, purpose of the processing and some other relevant information[157]. However, as already mentioned, this obligation does not arise when, "in particular for processing for statistical purposes or for the purposes of historical or scientific research", providing such information "proves impossible or would involve a disproportionate effort" or "if recording or disclosure is expressly laid down by law"[158]. In these instances, involving a "proportionality test"[159], Member States are required to "provide appropriate safeguards"[160].

Several members of the research community have been pointing out the flaws of the consent provisions. For instance, a literal reading of the requirement for consent "would seem to impede research using health data collected from young children, or adults who are mentally incompetent to give consent": this scenario does not fall within Article 8 (3), nor can Article 8 (2) (c) apply (research may be desirable but cannot be said to be necessary)[161]. Hence, in this situation the Member States would need to resort to the "substantial public interest" exemption laid down by Article 8 (4), which is "consistent with the general thrust of regulation of clinical research in the EU, seen for instance in the Clinical Trials Directive [Directive 2001/20/EC][162], which requires consent to be obtained from an appropriate person, be that a parent or other 'legal representative'"[163].

Another major issue refers to the transfer of data within the EU, which is crucial in order to carry out effective clinical and scientific research. It has been pointed out that "[t]he importance of [this] goal […] can be downplayed by an approach adopted by Member States impeding the free flow of data based on the protection of the right to privacy as interpreted in the different national legal traditions"[164].

Also, as to public health monitoring of infectious diseases, the Directive does not seem well equipped to deal with it. Member States are allowed to create exemptions on grounds of "substantial public interest" under Article 8 (4), but this provision has been criticized "for its extremely broad terms"[165].

---

156 HERVEY & MCHALE, *supra* note 58, at 180.
157 Data Protection Directive, Art. 11 (1).
158 *Id.*, Art. 11 (2).
159 HERVEY & MCHALE, *supra* note 58, at 181.
160 Data Protection Directive, Art. 11 (2).
161 HERVEY & MCHALE, *supra* note 58, at 179.
162 Directive 2001/20/EC on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, OJ 2001 L 121/34.
163 HERVEY & MCHALE, *supra* note 58, p. 179.
164 *Id.*, p. 181.
165 *Id.*, p. 182 (citing P. CASE, *Confidence Matters: The Rise and Fall of Informational Autonomy in Medical Law*, 11 (2) *Medical Law Review* 208, 230 (2003)). An example is section 60 of the Health and Social Care Act 2001 in the UK, which enables the introduction of secondary legislation to allow the disclosure of confidential patient information related to the diagnosis of communicable diseases and other public health risks. *See* Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, reg 4.

2.5 The Proposed General Data Protection Regulation

The European Commission has engaged in the "herculean task" of "replac[ing] nothing less than the entire EU data protection edifice"[166]. The Data Protection Directive, which "has by now become the international data protection metric against which data protection adequacy is measured", now needs some modernization, insofar as it "was designed at an age when the number of computing equipment and processing operations was expected to be finite, traceable and identifiable", and it "ultimately did not achieve the desired harmonisation effect"[167]. Thus, the reform aims at dealing with "the considerable differences that persist between national data privacy regimes across the EU" and "strengthening data privacy in line with its status as a fundamental right in the EU constitutional order" [168].

In 2012 the Commission proposed a new General Data Protection Regulation[169], which was supposed to provide unified data protection legislation for the European Union, with immediate binding legal force throughout the Member States and no need for further implementation[170]. In the words of the proposal, "[r]apid technological development and globalisation have brought new challenges for the protection of personal data"[171], and "[t]hese developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market"[172]. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") voted on October 21, 2013 to adopt some proposed amendments[173]. On March 12, 2014 the European Parliament voted in favor of the new regulation, which will have to be adopted using the ordinary co-decision procedure by being approved also by the Council of the European Union[174]. The Council met and reached a general approach on June 11, 2015,

---

166 DE HERT & PAPAKONSTANTINOU, *supra* note 146, at 130. This task is meant to be carried out through two instruments: the General Data Protection Regulation and the Police and Criminal Justice Data Protection Directive. *Id. See* European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012, COM(2012).

167 DE HERT & PAPAKONSTANTINOU, *supra* note 146, at 131.

168 BYGRAVE, *supra* note 1, at 71. However, increased harmonization might "undermine more effective data protection regimes already in place in some EU member states, especially Scandinavian countries". L. FRANCIS, *Privacy and Health Information: The United States and the European Union*, 103 *Kentucky Law Journal* 419, 427 (2015).

169 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter GDPR – Commission Proposal], available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

170 "A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFUE will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market". GDPR – Commission Proposal, paragraph 3.1.

171 Council of the European Union, Interinstitutional File: 2012/001 (COD), 11 June 2015, *available at* http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [hereinafter: GDPR – Council General Approach], Recital 5.

172 *Id.*, Recital 6.

173 *See* European Commission, MEMO/13/923 (October 22, 2013), http://europa.eu/rapid/press-release_MEMO-13-923_it.htm.

174 *See* European Commission, MEMO/14/186, March 12, 2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm. The Amendments approved by the European Parliament in 2014 are

which gave start to the trilogue phase. Finally, on December 15, an agreement was reached[175], and we will analyze the new consolidated text.

The new regulation aims at introducing many important changes[176], including the well-known "right to be forgotten"[177], but this analysis will only focus on the provisions that are potentially relevant for the issue of health data privacy that we are examining.

The proposed Regulation, after including the "right to the protection of personal data" among the "fundamental rights and freedoms of natural persons"[178], engages in providing the EU with new definitions of some crucial concepts: "personal data" is defined very broadly as "any information relating to an identified or identifiable natural person ('data subject')"[179], and we can also find brand new definitions of "genetic data"[180], "biometric data"[181], and "data concerning health"[182].

A critical point is represented by the new purpose limitation principle envisaged by the new GDPR. Pursuant to Article 6 ("Lawfulness of processing"), processing of personal data is only allowed if "the data subject has given consent"[183], or if it is necessary in some listed situations[184]. The Article specifies that with respect to the situations involving a legal obligation (i.e., Article 6 (1)(c) and 6 (1)(e)) the "basis for the processing […] must be laid down by Union law, or Member State law"[185]. Also, "Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing"[186].

In the Council's version of the Regulation, under Article 6(4) (now deleted), further processing for a purpose which is "incompatible with the one for which the personal data have been collected"[187] would have been allowed if the data subject has provided consent

---

available at: European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) [hereinafter GDPR – EP Resolution], available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

175 *See* European Commission - Press release, Agreement on Commission's EU data protection reform will boost Digital Single Market, Brussels, 15 December 2015, available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

176 *See* GILBERT, *supra* note 63.

177 *See* GDPR – Consolidated text, Art. 17. For a quick overview, see European Commission, *Factsheet on the "Right to be Forgotten" ruling*, available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited October 6, 2015); FRANCIS, *supra* note 168, at 426.

178 GDPR – Consolidated text, Art. 1(2).

179 *Id.*, Art. 4(1). For a deeper analysis of the issue of "identifiability", see Chapter III.

180 GDPR – Consolidated text, Art. 4(10).

181 *Id.*, Art. 4(11).

182 *Id.*, Art. 4(12).

183 *Id.*, Art. 6(1)(a).

184 *Id.*, Art. 6(1)(b)-(f). Such situations include: "the performance of a contract to which the data subject is party", "compliance with a legal obligation to which the controller is subject", the protection of "the vital interests of the data subject or of another natural person", "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", and "legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data". This last provision "shall not apply to processing carried out by public authorities in the performance of their tasks".

185 *Id.*, Art. 6(3).

186 *Id.*, Art. 6(2a).

187 GDPR – Council General Approach, Art. 6(4).

or under some listed situations where the processing is necessary[188]. This looked like a "compromise […] between rights protection and business interests", as "[t]he processing of personal information for purposes unforeseeable at the time of data collection […] undermines the principle of purpose specification"[189]. The new consolidated text of the Regulation no longer includes this provision. If the purpose of the processing is different from the one for which the data have been collected, the processing is first of all lawful if there is consent, or if it is based "on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard" certain objectives[190]. Otherwise, the controller needs to ascertain whether the new purpose is compatible with the initial one, by "tak[ing] into account, inter alia: (a) any link between the [two] purposes […]; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed […]; (d) the possible consequences of the intended further processing for data subjects"; (e) the existence of appropriate safeguard, which may include encryption or pseudonymisation"[191].

On a different note, greater importance is given to the role of consent: it must be "freely-given, specific, informed and unambiguous", carried out "either by a statement or by a clear affirmative action"[192]. The text of the proposal put forward by the Parliament went even further by requiring "explicit" consent[193], but the Council's General Approach switched back to the "unambiguous" language[194]. The data controller bears the burden of demonstrating that the data subject has given consent to processing[195].

As far as individual rights are concerned, "[s]ubstantial work towards the strengthening of the position of individuals has apparently been undertaken" in the proposed GDPR[196]. The data subject has a right to be fully informed when personal data about him or her is collected[197]. Article 14 deals with the "[i]nformation to be provided where the data are collected from the data subject", whereas Article 14a refers to when the data are not collected from him or her. The data subject has the right to know "that the controller intends to transfer personal data to a recipient in a third country or international organization"[198], as well as the right to receive information on the intention "to further process the data for a purpose other than the one for which the data were collected"[199]. Also, the data subject shall have the right to access the data and obtain information on their processing[200], and the right to obtain the rectification of inaccurate personal data[201]. The provision that has probably been the most commented on so far, though, is Article 17, or the so-called "right to be forgotten": "[t]he controller shall have the obligation to erase

---

188 *See id.*, Art. 6.1 (a)-(e).
189 DE HERT & PAPAKONSTANTINOU, *supra* note 146, at 135.
190 GDPR – Consolidated text, Art. 6(3a). Such objectives are listed in Article 21(1)(aa)-(g).
191 *Id.*
192 *Id.*, Art. 4(8) and Recital 25 (which provides further guidance with respect to various ways of providing consent).
193 *See* GDPR – EP Resolution, Art. 4(8) and Recital 25.
194 *See* GDPR – Council General Approach, Art. 4(8) and Recital 25.
195 GDPR – Consolidated text, Art. 7(1).
196 DE HERT & PAPAKONSTANTINOU, *supra* note 146, at 136.
197 GDPR – Consolidated text, Art. 14 and 14a.
198 *Id.*, Art. 14.1(e) and 14a(1)(da). This also includes the information on "the existence or absence of an adequacy decision by the Commission". *Id.*
199 *Id.*, Art. 14(1b) and 14a(3a).
200 *Id.*, Art. 15.
201 *Id.*, Art. 16.

personal data without undue delay" in many circumstances including when the data are no longer necessary for the purpose, when the data subject withdraws consent or objects to the processing, and when the processing of the data has been unlawful[202]. The proposed Article 18 will provide data subjects with the "[r]ight to data portability", i.e., "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine-readable format and have the right to transmit those data to another controller"[203].

The requirements imposed on data controllers are going to be stricter under the new framework: the concept of "accountability" is introduced[204], as well as new requirements of data protection by design and by default[205]. Furthermore, Articles 31 and 32 impose an obligation on data controllers to notify the data subject and the relevant supervisory authority of any personal data breaches[206]. The duty to notify the supervisory authority is triggered by any personal data breach unless it "is unlikely to result in a high risk for the rights and freedoms of individuals"[207]. Such communication must be done "without undue delay"[208], and shall include a description of "the nature of the personal data breach"[209], "the name and contact details of the data protection officer or other contact point where more information can be obtained"[210], a description of "the likely consequences" of the breach[211], and a description of "the measures taken or proposed to be taken by the controller to address the personal data breach" including "where appropriate, [an indication of measures] to mitigate its possible adverse effects"[212]. However, in several instances it is not necessary to communicate that a personal data breach has occurred to the data subject[213]. First, there is no such duty if the data affected by the breach had been treated with "appropriate technological and organisational protection measures", such as encryption[214], or "subsequent measures [have been taken] which ensure that the high risk […] is no

---

[202] *Id.*, Art. 17. *See also id.*, Recitals 53, 54, 54a. This represents an issue with respect to the coordination with some national provisions. For instance, the Ministry of Health Ministerial Circular of 19 December 1986, no. 900.2 / AG. 454/260 requires some data to be kept forever (clinical records) and some others for twenty years (e.g. diagnostic documentation).

[203] GDPR – Consolidated text, Art. 18(2). In exercising this right, the data subject "has the right to obtain that the data is transmitted directly from controller to controller where technically feasible". *Id.*, Art. 18(2a).

[204] *Id.*, Art. 22.

[205] *Id.*, Art. 23.

[206] *Id.*, Art. 31 and 32.

[207] *Id.*, Art. 31(1). The Council's General Approach phrased this provision differently, by requiring notification whenever a personal data breach "is likely to result in a high risk for the rights or freedoms of individuals", and listed some examples of such risks ("discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage". GDPR – Council General Approach, *supra* note 171, Art. 31(1). The new text does not make a list of risks that trigger this duty, probably in order to highlight that this duty is general in scope. Article 32 on the communication of data breaches to the data subject still adopts the "likely to result" language. GDPR – Consolidated text, *supra* note 61, Art. 32(1).

[208] *Id.*, Art. 31(1) and 32(1). The notification to the supervisory authority should be done, "where feasible, not later than 72 hours after having become aware of it". Failure to meet this deadline imposes a duty to provide "reasoned justification". *Id.*, Art. 31(1).

[209] *Id.*, Art. 31(3)(a) and 32(2).

[210] *Id.*, Art. 31(3)(b) and 32(2).

[211] *Id.*, Art. 31(3)(d) and 32(2).

[212] *Id.*, Art. 31(3)(e) and 32.2.

[213] *Id.*, Art. 32(3).

[214] *Id.*, Art. 32(3)(a).

longer likely to materialise"[215]. The communication is also not required if "it would involve disproportionate effort" [216].

Also, the proposed Article 33 asks the controllers to carry out an assessment of the impact of the processing on the "rights and freedoms of individuals[217]. A Data Protection Impact Assessment (DPIA) can be defined as "a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects"[218]. Such assessment shall in particular be required, for instance, in the case of "processing on a large scale of special categories of data"[219].

2.5.1 The New General Data Protection Regulation and Personal Data Concerning Health

"Personal data concerning health" include "data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject"[220]. With respect to their treatment, the proposal "builds to a large extent on the same structure as the Data Protection Directive"[221]. The processing of special categories of personal data, including data concerning health or sex life, is prohibited unless one of the exceptions applies[222]. It is important to note that "Member States may maintain or introduce further conditions, including limitations"[223].

Processing is allowed either if the data subject has given explicit consent[224], or if it is required by some predominant interest [225]. The exceptions largely overlap with those

---

[215] *Id.*, Art. 32(3)(b).

[216] *Id.*, Art. 32(3)(c). In these situations, "there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner". *Id.*

[217] *Id.*, Art. 33(1). Again, the Council's General Approach included a non-exhaustive list of risks, which has been deleted in the new text. *See* GDPR – Council General Approach, Art. 33(1).

[218] DE HERT & PAPAKONSTANTINOU, *supra* note 146, at 140 (citing D. WRIGHT, "*Should privacy imapct assessments be mandatory?*", Communications of ACM, July 2011; D. WRIGHT & P. DE HERT (eds.), *Privacy Impact Assessment, Series: Law, Governance and Technology Series*, Vol. 6, Dordrecht, Springer, 2012, at 523). Article 33(3) provides a detailed description of what the assessment shall contain, including at least: "(a) a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned". GDPR – Consolidated text, Art. 33(3)(a)-(d).

[219] *Id.*, Art. 33(2)(b).

[220] *Id.*, Recital 26. This includes "information about the individual collected in the course of the registration for and the provision of health care services as referred to in Directive 2011/24/EU to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test". *Id.*

[221] J. REICHEL & A. LIND, *The New General Data Protection Regulation – Where Are We Are and Where Might We Be Heading?*, in D. MASCALZONI (ed.), *Ethics, Law and Governance of Biobanking. National, European and International Approaches*, Springer 2015, at 98.

[222] GDPR – Consolidated text, Art. 9(1).

[223] *Id.*, Art. 9(5).

[224] *Id.*, Art. 9(2)(a). The data subject's consent does not lift the prohibition, however, when Union law or Member State law so provides. *Id.*

[225] *Id.*, Art. 9(2)(b)-(i).

established by the Directive. Particularly interesting for our analysis is, for instance, the exception established for processing "necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent"[226]. Furthermore, another exception is carved out for when "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law"[227]. Processing of health data is also allowed when it is "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract with a health professional"[228]. In this instance, the professional must be "subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies"[229]. "Reasons of public interest in the area of public health" represent another viable exception: this includes "protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices"[230]. Pursuant to Recital 42b, this "should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies"[231].

We can now look at when processing of health data is allowed for purposes of research. Article 9(2)(i) allows processing when it is "necessary for […] scientific and historical research purposes […] in accordance with Article 83(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects" [232]. Article 83 requires "appropriate safeguards", which "shall ensure that technical and organisational measures are in place in particular in order to ensure the respect of the principle of data minimisation" [233]. These measures "may include pseudonymisation, as long as these purposes can be fulfilled in this manner"[234]. The provision also specifies that "[w]henever these purposes can be fulfilled by further processing of data which does not permit or not any longer permit the identification of data subjects", it should be carried out this way[235]. It is crucial to note that "Union or Member State law may provide for derogations from [data

---

[226] *Id.*, Art 9(2)(c).

[227] *Id.*, Art. 9(2)(g). This law "shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". *Id.*

[228] *Id.*, Art. 9(2)(h).

[229] *Id.*, Art. 9(4).

[230] *Id.*, Art. 9(2)(hb). This must be based on "Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy". *Id. See also id.*, Recital 42b (specifying that "'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality"). *See also* Y. COPPIETERS & A. LEVEQUE, *Ethics, privacy and the legal framework governing medical data: opportunities or threats for biomedical and public health research*, 71 *Archives Of Pub. Health*, no. 15, 2013, at 1; M. STENBECK & P. ALLEBECK, *Do the planned changes to European data protection threaten or facilitate important health research?*, *Eur. J. Public. Health* 2011, 21(6): 682-3.

[231] GDPR – Consolidated text, Recital 42b.

[232] *Id.*, Art. 9(2)(i).

[233] *Id.*, Art. 83(1).

[234] *Id.*

[235] *Id.*

subject's rights] subject to the [aforementioned] conditions and safeguards […] in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of these purposes"[236]. The approach adopted in the consolidated text – which is quite open to research – reflects the view expressed by the Council[237], whereas the scenario envisioned by the Parliament established stricter requirements[238]. The Article 29 Working Party had endorsed the Parliament's approach, stating that "[a]ny proposals to weaken and thereby broaden the scope of this type of further processing […] should [have been] negatively assessed in view of the real risks for data subjects of unequal/unfair treatment, based on the further processing, for example through profiling, of intimate data concerning their private life"[239].

The proposed Recital 25aa) recognizes that "[i]t is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection",

---

[236] *Id.*, Art. 83(2). The rights that can be derogated are those referred to in Articles 15, 16, 17a and 19. *Id.*

[237] *See* GDPR – Council General Approach, Art. 9(2)(h), 9(4), and Recital 42a).

[237] DE HERT & PAPAKONSTANTINOU, *supra* note 146,

[238] Pursuant to the text proposed by the European Parliament, Article 81 established that the processing of personal data concerning health "must be on the basis of Union law or Member State law which shall provide for suitable, consistent, and specific measures to safeguard the data subject's interests and fundamental rights, to the extent that these are necessary and proportionate, and of which the effects shall be foreseeable by the data subject, for" some listed purposes. GDPR – EP Resolution, Art. 81(1). The purposes are: (a) preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services; (b) reasons of public interest in the area of public health; (c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system and the provision of health services. *Id.* The provision clarifies that "[w]hen [such purposes] can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law". *Id.*, Art. 81(1a). As to research, "[p]rocessing of personal data concerning health which is necessary for historical, statistical or scientific research purposes shall be permitted only with the consent of the data subject". *Id.*, Art. 81(2) (for an example of the critiques made to this provision, *see* http://www.leru.org/index.php/public/news/press-release-the-eps-position-on-the-general-data-protection-regulation-threatens-eu-research/). Such consent, where "required for the processing of medical data exclusively for public health purposes of scientific research", "may be given for one or more specific and similar researches". *Id.*, Art. 81(1b). The data subject may withdraw the consent at any time. This seems to imply that if the purpose of the research is public health, personal data can be collected for new purposes. *See* REICHEL & LIND, *supra* note 221, at 99. *See*, in contrast, Data Protection Directive, Art. 6.1(b) (providing that "[f]urther processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards"). Exceptions to the consent requirement could be created by Member States for "research that serves a high public interest, if [it] cannot possibly be carried out otherwise". There is a duty to anonymize or at least pseudonymize "under the highest technical standards" the data, and take "all necessary measures . . . to prevent unwarranted re-identification". Furthermore, the data subjects would be provided with the right to object to the aforementioned exceptions. GDPR – EP Resolution, Art. 81(2a); *see also* Art. 19. The previously proposed Article 83 surrounded the processing of health data for research with particular safeguards: (a) it is only possible if the "purposes [of historical, scientific or statistical research] cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject"; (b) "data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects". *Id.*, Art. 83.

[239] European Union Article 29 Data Protection Working Party, Annex – health data in apps and devices, Feb. 5, 2015, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [hereinafter Article 29 WP Annex on health data in apps 2015] (attached to a letter responding to the European Commission's request to clarify the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps).

therefore "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research" and "should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose"[240].

It is important to point out that the regulatory competence under the proposed Regulation will largely be shifted from the Member States to the EU, which "may be beneficial to cross-border bio-medical research" but "will hardly be helpful if the rules themselves are so strict that they in practice render bio-medical research on health data unmanageable"[241].

3. Health Data Protection in Italy

In order to have a better understanding of the European legal framework on health data privacy, we will now analyze the Italian legislation. Among the reasons why we have chosen Italy we can find not only the familiarity with and deeper knowledge of this country, but also its relevance in the European law landscape, especially in the field of health data privacy.

The so-called Personal Data Protection Code (Legislative decree no. 196 of 2003)[242] thoroughly reformed the Italian legal framework previously based on L. 675/1996 by absorbing the changes in technology and in the European legal context. A pivotal role is played by the Italian Data Protection Authority (Garante per la protezione dei dati personali), whose authorizations and guidelines largely shape the applicable rules. Indeed, the requirement for an authorization issued by the Garante for data processing is the way the Italian legal framework copes with the fact that sometimes requiring the data subject's

---

[240] *Id*., Recital 25aa).

[241] REICHEL & LIND, *supra* note 221, at 100.

[242] Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003 (as translated at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932) [hereinafter Italian Personal Data Protection Code]. For insights and comments on the Italian Data Protection Code and the Italian privacy legislation, see R. ACCIAI (ed.), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004; C.M. BIANCA, F.D. BUSNELLI (eds.), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003 n. 196 ("Codice Privacy")*, Padova, 2007; A. BIASIOTTI, *Codice della privacy e misure minime di sicurezza: d.lgs. 196/2003*, II ed., Roma, 2004; F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (eds.), *Il codice dei dati personali. Temi e problemi*, Milano, 2004; G. CASSANO, S. FADDA (eds.), *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy d.lgs. 30 giugno 2003, n. 196*, Milano, 2004; G. CIACCI, *Privacy e sanità*, Roma 2005; G.P. CIRILLO (ed.), *Il Codice sulla protezione dei dati personali*, Milano, 2004; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *Il codice del trattamento dei dati personali*, Torino, 2007; L. DIMASI, *Il trattamento dei dati personali in sanità e la circolazione delle informazioni nell'era dell'informatizzazione*, in *Sanità Pubblica e Privata*, 2011, fasc. 4, 28-43; F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 121; G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli 2012; A. FLORIO, *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in *Ciberspazio e dir.*, 2010, 111; M.G. LOSANO (ed.), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001; J. MONDUCCI, G. SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004; G. PASCUZZI, *Il diritto dell'era digitale*, II ed., Bologna, 2010, at 53-59; F. PIZZETTI, *Sette anni di protezione dati in Italia: un bilancio e uno sguardo sul futuro*, Torino, Giappichelli, 2012; R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; P. PERRI, *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Giuffrè, Milano, 2007; S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normative: il nuovo codice sulla privacy, in Europa e diritto privato*, 2004; G. SANTANIELLO (ed.), *La protezione dei dati personali*, in G. SANTANIELLO (ed.), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005, 131; S. SICA, P. STANZIONE (eds.), *La nuova disciplina sulla privacy: commento al d.lgs. 30 giugno 2003, n. 196*, Bologna, 2004; V. ZAMBRANO, *Dati sanitari e tutela della sfera privata*, in *Dir. informazione e informatica*, 1999, 1. For a deeper analysis of the protection of health data privacy in the Italian health care system, see R. ACCIAI, *La tutela della privacy ed il s.s.n.*, in *Ragiusan*, fasc. 225/226, 20 (2003).

consent is not enough to provide protection whenever the data subject is in an imbalanced position[243]: the knowledge and influence of the DPA is able to reestablish an adequate power balance[244].

3.1 The Right to Protection of Personal Data

The Italian Data Protection Code starts by affirming that "[e]veryone has the right to protection of the personal data concerning them"[245]. This right, the recognition of which is consistent with Art. 8 ECHR and Art. 16 TFEU, presents some features that make it different from the traditionally recognized "personality rights" [246], even if it shares with them a "relational dimension", i.e., the fact that they all have to do with social relationships[247]. In the traditional personality rights, personal data are only protected where other values (such as honor or personal identity) would otherwise be damaged[248]. On the contrary, under the Italian Data Protection Code, the right to protection of personal data is triggered regardless of the damage to other protected values[249].

The purpose of the Italian legislation is to "ensure that personal data are processed by respecting data subjects' rights, fundamental freedom and dignity, particularly with regard to confidentiality, personal identity, and the right to personal data protection"[250]. Interestingly, the Italian Code puts more emphasis on the notion of "dignity" than the EU Directive[251]. As to "personal identity", this is a right that was created by case law and scholars in an effort to protect the individual's need for his image to accord with the social, moral and political principles he believes in[252].

A general rule with respect to the treatment of personal data is the data minimisation principle: processing[253] of personal and identification data should be avoided "if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity"[254].

The Italian Data Protection Code provides some definitions in Section 4. Particularly relevant is the definition of "personal data", meaning "any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number"[255]. Thus, pursuant to this definition, relevance is given to any information as long as it is somehow connected, even indirectly, with an identified or identifiable person[256]. Consequently, "identification data" are "personal data allowing a data subject to be identified directly"[257].

---

243 PEIGNÉ, *supra* note 130, at 298.
244 *Id.* at 299.
245 Italian Personal Data Protection Code, Section 1.
246 S. NIGER, *Il diritto alla protezione dei dati personali*, in J. MONDUCCI, G. SARTOR (eds.), *Il Codice in materia di protezione dei dati personali. Commento sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004, at 7.
247 *Id.* at 10.
248 *Id.* at 7.
249 *Id.* at 7-8.
250 Italian Personal Data Protection Code, Section 2.1.
251 NIGER, *supra* note 246, at 8. *See also* RODOTÀ, *supra* note 130, at 584.
252 NIGER, *supra* note 246, at 9.
253 The definition of "processing" is aimed at encompassing the whole 'life' of the personal data from its collection to its destruction. NIGER, *supra* note 246, at 13. *See* Italian Personal Data Protection Code, Section 4.1 a).
254 Italian Personal Data Protection Code, Section 3.
255 *Id.,* Section 4.1 b).
256 NIGER, *supra* note 246, at 14. *See also* G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012, at 32.
257 Italian Personal Data Protection Code, Section 4.1 c).

3.2 Personal Data Suitable for Disclosing Health

The Italian Constitution (Article 32) specifically refers to "health" as a "fundamental right of the individual" and provides that "[n]o one may be obliged to undergo any health treatment except under the provisions of the law", and which "may not under any circumstances violate the limits imposed by respect for the human person"[258]. As much as this provision may seem to apply only to "compulsory health treatments", "respect for the human person" has instead come to play a pivotal role in the treatment of health data in any and all circumstances[259]. This is due to the understanding that health represents an integral part of the human person, so that respect of the latter cannot be achieved without protecting the former[260].

Looking more specifically to the processing of health data under the Italian Data Protection Code, they fall within the definition of "sensitive data" and they are more specifically called "personal data suitable for disclosing health"[261]. This definition does not require that there is a direct connection between the information and the health status, but rather looks at whether there is merely a potential link between such information and the disclosure of the health situation[262] (unlike Directive 95/46/EC[263]). Arguably, this would include data which are able to disclose even a normal or healthy status, but based on the rationale of these provisions some scholars conclude that we are only referring to data disclosing unhealthy statuses[264]. Nevertheless, others have highlighted that "health" rather refers to the global status of the individual, encompassing physical as well as psychological and relational elements[265]. For instance, a paycheck explicitly referring to a worker as "disadvantaged" has been deemed to fall within the definition, as well as receipts explicitly naming purchased medicines[266].

3.3 The Processing of Sensitive Data and Health Data

The rules on the processing of sensitive data, and particularly of health data, represent the attempt by the Italian legislator to balance all the different interests at stake: this balancing activity is particularly complex in that it features several conflicts of interest[267]. Not only is it clear that the data subject must give up at least part of his or her privacy to receive health care services, but the need to re-use health data to protect third parties or the community as a whole and to perform scientific research requires a careful

---

258 Constitution of the Italian Republic, Article 32 (available at https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf).

259 E. LAMARQUE, *Privacy e salute*, in M.G. LOSANO (ed.), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni. Roma-Bari*, 2001, p. 335, 359, 360-61.

260 *Id.* at 360.

261 Italian Personal Data Protection Code, Section 4.1 d).

262 *See* FINOCCHIARO, *supra* note 256, at 58.

263 J. MONDUCCI, G. PASETTI, *Il trattamento dei dati sanitari e genetici*, in J. MONDUCCI, G. SARTOR (eds.), *Il Codice in materia di protezione dei dati personali. Commento sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004, at 256.

264 FINOCCHIARO, *supra* note 256, at 62.

265 MONDUCCI & PASETTI, *supra* note 263, at 257; PEIGNÉ, *supra* note 130, at 296.

266 FINOCCHIARO, *supra* note 256, at 64-65. *See* Garante per la protezione dei dati personali, June 18, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1640331; Garante per la protezione dei dati personali, April 29, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1611565.

267 *See* F. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *Il codice del trattamento dei dati personali*, Torino, 2007, at 411.

coordination of all the different circumstances, having regard to the several subjects involved in the processing of data and the different goals it pursues[268].

As to the processing of sensitive data, including personal data suitable for disclosing health, it can be carried out by public bodies only if expressly authorized by a law specifying "the categories of data that may be processed and the categories of operation that may be performed as well as the substantial public interest pursued"[269], or pursuant to a determination of the Garante (the Italian Data Protection Authority) of "the activities that pursue a substantial public interest among those they are required to discharge under the law"[270]. The processing must occur "in accordance with arrangements aimed at preventing breaches of data subjects' rights, fundamental freedoms and dignity"[271], and only inasmuch as it is "indispensable for [the public bodies] to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature"[272]. The Data Protection Code further expands this principle by providing that "[n]o data that is found to be excessive, irrelevant or unnecessary […] may be used, except for the purpose of keeping – pursuant to law – the record or document containing that data"[273].

With respect to the processing of sensitive data by private entities, it can only occur "with the data subject's written consent and the Garante's prior authorization"[274], which can be accompanied by "measures and precautions in order to safeguard the data subject"[275]. The Garante communicates its decision as to the request for authorization within 45 days; otherwise, its silence is deemed as a rejection[276]. However, sensitive data may "be processed without consent, subject to the Garante's authorization", in the following circumstances[277]:

a) within "not-for-profit associations, bodies or organisations", with regard to data about members and/or entities having regular contacts with such associations, in connection with their "specific, lawful purposes";

b) if "necessary to protect a third party's life or bodily integrity";

c) if necessary to protect the data subject's life or bodily integrity when he or she is unable to provide consent and it is provided by other authorized subjects[278]. The latter provision shows the importance the Italian legislation gives to individual autonomy[279], as consent must anyways be manifested by "the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted"[280];

d) if "necessary for carrying out the investigations by defense counsel […] or else to establish or defend a legal claim", as long as it is not "overridden by the data subject's claim". It is important to note that this only applies to health data if the claim consists "in a personal right or another fundamental, inviolable right or freedom";

---

[268] *See id.* at 411-12.
[269] Italian Personal Data Protection Code, Section 20.1.
[270] *Id.*, Section 20.3.
[271] *Id.*, Section 22.1.
[272] *Id.*, Section 22.3.
[273] *Id.*, Section 22.5.
[274] *Id.*, Section 26.1.
[275] *Id.*, Section 26.2.
[276] *Id.*, Section 26.2.
[277] *Id.*, Section 26.4.
[278] *See id.*, Section 82.2; see Paragraph 3.5.
[279] PEIGNÉ, *supra* note 130, p. 299.
[280] Italian Personal Data Protection Code, Section 26.4 b).

e) if "necessary to comply with specific obligations and/or tasks laid down by laws, regulations, or [EU] legislation in the employment context".

Personal data disclosing health are surrounded by particular safeguards and their processing is also specifically dealt with in Part II, Title V.

For instance, data must "be kept separate from any other personal data that is processed for purposes for which they are not required"[281], and they "may not be disseminated"[282].

There are two different sets of provisions that apply to the processing of health data, depending on who is handling the data and for what purpose.

When personal data disclosing health are processed by "[h]ealth professionals and public health care bodies", they are not subject to the afore-mentioned provisions (Section 20) but rather to special rules, pursuant to Section 76[283]. On the other hand, data processing that falls within the scope of the tasks committed to the National Health Service is governed by the Section 20 framework, and is permitted only as long as there is a law specifying the substantial public interest goals. Section 85 lists some public interest activities within the tasks of the National Health Service[284].

As mentioned, the scenario envisioned by Section 76 refers to public health care bodies and health professionals, i.e. those who perform their task in close contact with patients and pursuant to a license issued by public authorities[285]. Generally speaking, the data subject's consent and the Garante's authorization must both be present. We can imply this from the fact that Section 76 carves out two exceptions to this rule with respect to the processing of data for specified purposes[286]. Section 76 applies "also within the framework of activities in the substantial public interest pursuant to Section 85"[287].

The first excepted scenario refers to when the processing is necessary to safeguard the data subject's bodily integrity and health: here the data subject's consent must be present, but there is no need for the Garante's authorization[288]. In any event, this needs to happen pursuant to the general principles referenced above; thus, data can only be processed as long as they are necessary to pursue the specified goals[289]. Consent can be provided "in accordance with the simplified arrangements" pursuant to Sections 77 and following[290] (see Paragraph 3.4).

Secondly, when the purpose is the safeguard of a third party or of the community as a whole, the data subject's consent is not required but the Garante's prior authorization

---

[281] *Id.*, Section 22.7.

[282] *Id.*, Section 22.8 and 26.5.

[283] *Id.*, Section 76 and Section 85.2. *See* MONDUCCI & PASETTI, *supra* note 263, at 258.

[284] Italian Personal Data Protection Code, Section 85.1 ("a) administrative activities related to prevention, diagnosis, care and rehabilitation of the persons assisted by the National Health Service, including aliens in Italy and Italian citizens abroad as well as the health care provided to seamen and airport staff; b) planning, management, control and assessment of health care; c) monitoring of testing and drugs, authorization for marketing and importing medical drugs and other health-related products; d) certification activities; e) application of provisions concerning occupational hygiene and safety and population health and safety; f) administrative activities related to organ and tissue transplantations and human blood transfusions, also pursuant to Act no. 107 of 4 May 1990; g) setting up, managing, planning and monitoring the relationships between the administration and the entities bound by contractual agreements with and/or recognised by the National Health Service").

[285] MONDUCCI & PASETTI, *supra* note 263, at 258.

[286] FINOCCHIARO, *supra* note 256, at 210.

[287] Italian Personal Data Protection Code, Section 76 and 85.2.

[288] *Id.*, Section 76.1 a).

[289] MONDUCCI & PASETTI, *supra* note 263, at 261.

[290] Italian Personal Data Protection Code, Section 76.2

must nevertheless be present[291]. Most scholars maintain that there should still be an attempt to obtain the data subject's consent, and that only in cases where it is denied should the data controller request the Garante's authorization[292]. This authorization "shall be granted after seeking the opinion of the Higher Health Care Council except for emergencies"[293].

A general authorization has been issued by the Garante in 2014 (Authorisation No. 2/2014)[294] concerning the processing of data suitable for disclosing health or sex life. The subjects to which this authorization applies are:

a) health care professionals, who can thereby process data suitable for disclosing health whenever it is indispensable to safeguard bodily integrity and health – either of a third party or of the community as a whole – and the data subject has not given or cannot give his/her consent;

b) private health care organisations and other private entities, who are allowed to process health data with the data subject's consent;

c) public health care bodies, who can process health data as long as the processing is aimed at protecting bodily integrity and health of a third party, or of the community as a whole; or in cases where the data subject's consent is missing and no administrative activities are involved as related to prevention, diagnosis, treatment, and rehabilitation in pursuance of Section 85, paragraphs 1 and 2, of the Code;

d) other entities, who are allowed to process data suitable for disclosing health if necessary and in order to: protect a third party's life or bodily integrity, or protect the data subject's life or bodily integrity, if he or she cannot give his or her consent, and it has been given either by an entity legally representing the data subject or by a next of kin, a family member, a person cohabiting with the data subject, or, failing these, the manager of the institution where the data subject is resident.

More specifically, the authorization is granted to three categories of data processing. The first category concerns physicians and other health care professionals, nursing and other staff in the health care sector, private health care institutions and organizations. In these cases, the authorization also refers to discharging the tasks provided by laws or EU regulations, and to the drafting of medical records and documents[295]. The situations falling within the second category are those connected to the following activities: scientific research purposes[296], performance of institutional purposes by voluntary or assistance organizations or rehabilitation and support centers, nursing homes and specialized clinics, operations by religious bodies and associations, the fulfillment of pre-contractual obligations entailing the supply of goods and/or services to the data subject, the assessment of fitness for participation in sports or competitions by sports facilities, and the operations which are necessary for performing organ and tissue transplantation and blood

---

[291] *Id.*, Section 76.1 b).

[292] MONDUCCI & PASETTI, *supra* note 263, at 263-64.

[293] Italian Personal Data Protection Code, Section 76.3.

[294] Garante per la protezione dei dati personali, Authorisation No. 2/2014 Concerning Processing of Data Suitable for Disclosing Health (published in Italy's Official Journal No. 301 of 30 December 2014) [hereinafter Garante – Authorisation No. 2/2014].

[295] Garante – Authorisation No. 2/2014, Paragraph 1.1. The tasks specifically mentioned are: "public health care and hygiene, occupational disease and accident prevention, medical treatment and diagnosis, including organ and tissue transplantation, rehabilitation of the physically and mentally disabled or incapacitated, preventive treatment of infectious and endemic diseases, mental health protection, pharmaceutical assistance, health care in connection with schools, health care in respect of sports activities, and investigations - pursuant to law - into the offences that are referred to in the legislation applying to sports".

[296] *See* Paragraph 3.7.

donations[297]. Third, the authorization is also granted when the processing of data suitable for disclosing health is necessary to carry out the investigations by a defense counsel or to establish or defend a legal claim, or to fulfill obligations within employer-employee relationships[298].

The authorization further provides that processing of data suitable for disclosing health "shall only be carried out via such operations and on the basis of such logic and organisational data arrangements as are absolutely indispensable with regard to the [aforementioned] obligations, tasks and purposes", and that "[t]he data shall be collected, as a rule, from the data subject"[299]. As to the communication of the data, it must be made "as a rule either directly to the data subject or to the latter's delegate[300] […] by using a closed envelope" or taking "suitable measures […] in order to prevent unauthorised persons from having access to said data, including the requirement of waiting to be served at a reasonable distance"[301].

In compliance with the general principles[302], "the data may be kept for no longer than is necessary" to carry out the tasks and achieve the purposes referred to above[303]. Therefore, it must be regularly verified "that the data are closely relevant, not excessive, and indispensable with regard to the existing, planned or terminated relationship, performance or tasks"[304]. This also concerns the data provided by the data subject on his or her initiative[305]. If the outcome of such verification reveals any excessive, irrelevant or non indispensable data, it cannot be used except for complying with data retention requirements[306].

3.4 Consent and Information in the Field of Health Data

The Data Protection Code allows for the data subject's consent and the provision of information to him or her to be set up with simplified arrangements[307].

Consent, as we can imply from Section 76, can be considered a general requirement for the processing of personal data disclosing health. It plays a very important role in the Italian legal framework, as it provides the individual with the chance to adjust the flow of the information about him or her[308]. Nevertheless, it would be naïve to completely rely on consent, as within the provision of health care the individual is often in a disadvantaged position[309].

Pursuant to the simplified arrangements, it "may be provided by means of a single statement, also verbally"[310]. The health care professional and/or public health care body must document the consent by writing a notice in which reference must be made to the

---

[297] Garante – Authorisation No. 2/2014, Paragraph 1.2.
[298] *Id.*, Paragraph 1.3.
[299] *Id.*, Paragraph 3.
[300] *See* Italian Personal Data Protection Code, Section 84.1
[301] Garante – Authorisation No. 2/2014, Paragraph 3.
[302] *See* Italian Personal Data Protection Code, Section 11.1 e).
[303] Garante – Authorisation No. 2/2014, Paragraph 4.
[304] *Id.*
[305] *Id.*
[306] *Id.*
[307] Italian Personal Data Protection Code, Section 77.
[308] PEIGNÉ, *supra* note 130, p. 297.
[309] *Id.* at 298. This is why, for instance, the Italian legislation couples consent with the Garante's authorization, whereas in France the law requires a notification to the DPA. *See id.* at 298-99.
[310] Italian Personal Data Protection Code, Section 81.1.

processing of data and to the information provided to the data subject[311]. In case the data subject maintains he has never provided his consent, he bears the burden of proof[312]. Despite providing for simplified arrangements with respect to information and consent, the Italian legislator has designed a rather strict set of formal rules: consent is required even when the purpose of the data processing is cure, diagnosis and therapeutic activities performed by a physician or a health care body[313]. Conversely, in these instances consent is not required pursuant to Directive 95/46/EC[314], nor is it required under the privacy laws of other countries such as France, Germany and the United Kingdom[315]. Nevertheless, the simplification of consent sometimes renders it a mere "check the box" activity rather than a real safeguard for the data subject's autonomy[316].

The Data Protection Code also envisaged the possibility to adopt simplified arrangements for the provision of information to the data subject[317], and makes a distinction between information provided by general practitioners and physicians, and information provided by health care bodies and by other public bodies[318]. It is important to bear in mind that this does not exempt them from the duty to include all the required elements[319]; after all, the provision of information really is the main device aimed at enforcing the right to data protection in that it makes the data subject aware of all the relevant information[320]. Here, too, simplification does not mean that the level of protection is lower[321].

When information is provided by general practitioners and physicians, it can regard "the overall personal data processing operations"[322] and it "may also concern personal data collected from third parties"[323]. Unless otherwise specified, "the information shall also concern data processing operations that are related to those carried out by [the physician], being performed by either a professional or another entity, who should be identifiable on the basis of the service requested and" that either replaces the physician, provides advice at his request, is one of his professional partners, supplies prescribed drugs, or communicates personal data to the physician[324]. Despite the simplified arrangements, the information "shall highlight, in detail, processing operations […] that may entail specific risks for the data subject's rights and fundamental freedoms and dignity", in particular if the processing is performed for scientific purposes including research, within tele-aid or tele-medicine services, or to supply other goods or services via electronic communications networks[325].

As to information provided by health care bodies, they can employ the simplified arrangements "with regard to several services delivered also by different divisions and units of a selfsame body or else by several specifically identified hospitals and local entities"[326].

---

311 *Id.* For an overview of the relevant provisions as to when the documentation of consent is done electronically, see FINOCCHIARO, *supra* note 256, at 212-13.
312 FINOCCHIARO, *supra* note 256, at 214.
313 *Id.*
314 *See* Data Protection Directive, Art. 8.3.
315 *See* FINOCCHIARO *supra* note 256, at 215-16.
316 *See* PEIGNÉ, *supra* note 130, p. 301.
317 Italian Personal Data Protection Code, Section 77.1 a).
318 *Id.*, Sections 78-80.
319 *Id.*, Section 78.1. *See id.*, Section 13.
320 *See* FINOCCHIARO, *supra* note 256, at 218-19.
321 *See* MONDUCCI & PASETTI, *supra* note 263, at 270.
322 Italian Personal Data Protection Code, Section 78.2.
323 *Id.*, Section 78.3.
324 *Id.*, Section 78.4.
325 *Id.*, Section 78.5.
326 *Id.*, Section 79.1.

This provision is particularly relevant insofar as this is what happens with electronic health records (see Chapter II). Health care bodies can also provide the information "in a homogeneous, consistent manner with regard to all the processing operations concerning personal data that are carried out by all the entities pertaining to a given health care agency"[327]. The provision of information and consent must be recorded in a unified manner, such as to allow verification by other divisions and units[328].

Finally, other public bodies are allowed to "provide a single information notice in connection with several data processing operations performed in different periods for administrative purposes with regard to data collected both from a data subject and from third parties"[329].

3.5 Emergencies

The necessity to deal with some extreme situations allows for information and consent to be provided "after the relevant service has been delivered, without delay"[330]. This reflects a balancing between privacy and "life" or "health", whereby the Italian legislator gives preeminence to the latter[331].

The situations in which this is allowed are: (a) medical emergencies[332]; (b) public hygiene emergencies when a contingent emergency order has been issued[333]; (c) impossibility of the data subject or other listed subjects to provide consent[334]; (d) serious, impending and irretrievable danger for the data subject's health or bodily integrity[335]; (e) cases where the need to obtain consent would negatively affect the provision of medical care by making it less timely or less effective[336].

Whenever the emergency ceases, there is a duty to request the data subject's consent. The data subject has the right to deny his consent, which does not make the previous processing activity unlawful, but creates a prohibition on any further data processing (as long as it does not impair the health care activity)[337].

3.6 Other Provisions

Pursuant to Section 83, the entities must "take suitable measures to ensure that data subjects' rights, fundamental freedoms and dignity, as well as professional secrecy requirements are respected". The Italian legislator provides a non-exhaustive list of such measures, in order to offer guidance and balance the various interests in some cases[338]. The

---

327 *Id.*, Section 79.3.
328 *Id.*, Section 79.2.
329 *Id.*, Section 80.1.
330 Italian Personal Data Protection Code, Section 82.
331 E. VARANI, *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario. Dalla Carta dei diritti fondamentali dell'Unione Europea al decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 2005, at 1784. This has been welcomed with some perplexities as it looks like a "suspension" of the right to give consent, occurring in one of the most delicate moments for the life of the individual. *See id.*
332 Italian Personal Data Protection Code, Section 82.1.
333 *Id.*
334 *Id.*, Section 82.2 a). This occurs "if the data subject is physically impaired, legally incapable or unable to distinguish right and wrong, and the consent cannot be obtained from the entity legally representing the data subject, or else a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted". *Id. See* FINOCCHIARO, *supra* note 256, at 220.
335 Italian Personal Data Protection Code, Section 82.2 b).
336 *Id.*, Section 82.3.
337 MONDUCCI & PASETTI, *supra* note 263, at 268-69.
338 MONDUCCI & PASETTI, *supra* note 263, at 272.

codified measures include, for example, solutions aimed at preserving individual privacy during waiting time[339] and during interviews[340], as well as at preventing medical care activities from being carried out in privacy-unfriendly situations[341]. Also, these measures include "respect for the data subject's dignity when providing the specific medical treatment as well as in connection with all data processing operations"[342] and "suitable arrangements to ensure that the provision of emergency aid can be notified or confirmed also by phone, if necessary, exclusively to third parties entitled thereto"[343]. As to data subjects inside medical wards, these measures must, on one hand, suitably inform third parties who have the right to visit on the whereabouts of data subjects, and on the other hand, inform data subjects of such visits in advance and respect their legitimate denial of authorization[344]. Procedures should also be implemented "to prevent third parties from establishing a link between a data subject and a given ward or department such as to disclose a specific medical condition"[345]. Furthermore, "persons in charge of the processing that are not bound by professional secrecy under the law [should be subjected] to rules of practice that are similar to those based on professional secrecy"[346].

Another important provision is Section 84, according to which health data can be communicated by health care professionals and health care bodies either to the data subject or to subjects able to 'represent' him or her[347]. This communication does not merely consist in making the data subject aware, but falls within the broader goal of protecting his or her well being[348].

This communication can be performed only by the agency of a physician who has been designated by the data subject or by the data controller[349] or by other health care professionals authorized in writing by the data controller or processor[350]. These other health care professionals are such that have direct contact with patients and are in charge of processing health data[351].

3.7 Health Data and Scientific Research

There is a set of provisions in the Italian Data Protection Code referring specifically to processing for statistical or scientific purposes. Personal data that is processed for such

---

339 Italian Personal Data Protection Code, Section 83.2 a)-b). The solutions specifically envisioned by the rule are: "a) solutions aimed at respecting precedence and order in calling up data subjects regardless of their specific names as regards medical care activities and administrative requirements entailing a waiting time, b) setting up appropriately spaced waiting lines by having regard to the use of voice messages and/or barriers". *Id.*

340 Italian Personal Data Protection Code, Section 83.2 c) ("solutions to prevent third parties from unduly getting to know information disclosing health during an interview").

341 *Id.*, Section 83.2 d).

342 *Id.*, Section 83.2 e).

343 *Id.*, Section 83.2 f).

344 *Id.*, Section 83.2 g).

345 *Id.*, Section 83.2 h).

346 *Id.*, Section 83.2 i).

347 *See id.*, Section 82.2 a) ("the entity legally representing the data subject, or else a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted").

348 MONDUCCI & PASETTI, *supra* note 263, at 273.

349 Italian Personal Data Protection Code, Section 84.1. This does not apply to data that had been previously provided by the data subject. *Id.*

350 *Id.*, Section 84.2. The authorization should set out adequate arrangements and precautions having regard to the context within which the data are to be processed". *Id.*

351 *Id.*

purposes cannot be used for taking decisions or measures with regard to the data subject, nor can they be used for processing for other purposes[352]. Statistical or scientific purposes need to be "specified unambiguously and made known to the data subject"[353], also pursuant to the codes of conduct and professional practice[354]. Here, too, consent can be given in accordance with simplified arrangements[355], but some exceptions to the consent requirement are carved out with respect to medical, biomedical and epidemiological research[356]. First, consent is not required for research activities that are expressly provided for by legislation or are included in a bio-medical or health care research program, as long as they have been communicated to the Garante forty-five days earlier[357]. Secondly, consent is not necessary "if data subjects cannot be informed on specific grounds" and the research programme has been approved by "a reasoned, favourable opinion by the geographically competent ethics committee as well as […] authorised by the Garante also in pursuance of Section 40"[358].

The Garante issued a General Authorisation to Process Personal Data for Scientific Research Purposes in 2014[359], referring to data processing which is "necessary to conduct studies that do not entail any significant personalized impact on data subjects and rely on data that was collected beforehand for health care purposes and/or to implement prior research projects and/or on data that was extracted from biological samples removed beforehand for health care purposes and/or to implement prior research projects"[360]. The authorization does not apply whenever research purposes can be achieved by processing anonymous data[361]: information systems must be set up so to rule out the processing of identifying information in this situation[362]. Furthermore, the authorization only applies to the processing of data relating to subjects who cannot be informed[363]. This does not rule out the obligation to obtain consent if it proves possible to inform the subjects in the course of the study[364]. The impossibility to inform data subjects must be based either on ethical grounds, when the data subject does not know about the research and providing information might cause him or her tangible or mental harm[365], or organizational grounds, due to the fact that failure to include the data relating to the data subject that cannot be contacted would significantly alter the findings[366].

---

352 *Id.*, Section 105.1

353 *Id.*, Section 105.2. *See also* Section 13 and Section 106.2 b).

354 *See id.*, Section 106.

355 *Id.*, Section 107.

356 *Id.*, Section 110.

357 *Id.*, Section 110.1. Such bio-medical or health care research program must be pursuant to Section 12-bis of Legislative Decree No. 502 of 30 December 1992, as subsequently amended.

358 *Id.*, Section 110.1.

359 Garante per la protezione dei dati personali, Authorisation No. 9/2014 - General Authorisation to Process Personal Data for Scientific Research Purposes (published in Italy's Official Journal No. 301 of 30 December 2014) [hereinafter Garante – Authorisation No. 9/2014].

360 *Id.*, Paragraph 2.1.

361 *Id.*, Paragraph 2.2.

362 *Id.*, Paragraph 3.

363 *Id.*, Paragraphs 2.2 and 4.

364 *Id.*, Paragraph 4.

365 *Id.*, Paragraph 4. An example is "the case of an epidemiological study on distribution of a (possibly) predictive factor of a disease for which no known treatment is available". *Id.*

366 Au *Id.*, Paragraph 4. "[A]ccount shall be taken in this connection especially of the inclusion criteria applied in the study, the enrolment mechanisms, the statistical size of the sample to be considered, and the time elapsed since the information relating to the data subject was first collected – e.g. if the study concerns data subjects affected by high-death-rate diseases or terminal-phase diseases, or else elderly patients in poor health". *Id.* The authorization specifies that "it shall be permitted to process the data relating to any individual

Security measures must be adopted which comply with the general requirements set forth in the Data Protection Code[367] and with the "Guidelines for the Processing of Personal Data in Medical Clinical Trials" issued by the Garante[368].

If a data subject exercises his or her rights to access personal data and to obtain updating, rectification and integration of the data, such updates, rectifications and additions shall be reported without modifying the data themselves if the outcome of these operations does not significantly affect the results of the research[369].

According to Authorization 2/2014 concerning processing of data suitable for disclosing health, "natural or legal persons, bodies, associations and other private entities [can perform such processing] for scientific research purposes, including statistical purposes, if the research is aimed at protecting the health of the data subject, third parties or the community as a whole in the medical, biomedical or epidemiological field, whenever the relationships between risk factors and human health are to be assessed also in connection with clinical drug trials or investigations are scheduled concerning diagnostic, therapeutic or preventive medicine activities or else with regard to the utilisation of health care facilities, and the availability of exclusively anonymous data concerning population samples does not allow achieving the purposes of said research. In these cases the processing may also concern data suitable for disclosing sex life and racial or ethnic origin exclusively if such data are indispensable to achieve the research purposes. Furthermore, the data subjects' consent shall be required as per Sections 106, 107, and 110 of the Code and the data, once collected, shall be processed in such a way as to prevent data subjects from being identified even indirectly, unless matching of the research data with the data subjects' identification data is performed on a temporary basis, is fundamental for the research purposes, and is accounted for in writing. Research findings may only be disclosed in anonymous form"[370].

3.8 The Processing of Some Specific Kinds of Health Data

Genetic data are the most protected kind of data under the Italian legal framework[371], as their processing is "allowed exclusively in the cases provided for in ad-hoc authorisations granted by the Garante, after having consulted with the Minister for Health who shall seek, to that end, the opinion of the Higher Health Care Council"[372]. Such authorization must contain some particular elements: for example, the information

---

that - following all reasonable efforts made to contact them such as by checking whether they are still alive, browsing through their clinical records, contacting such telephone numbers as may be available, or obtaining contact information from population and/or health care registers – are found to be either deceased or past contact at the time of their enrolment for the given study". *Id.*

367 *See* Italian Personal Data Protection Code, Sections 33-35.

368 *See* Garante per la protezione dei dati personali, Guidelines for Data Processing within the Framework of Clinical Drug Trials - 24 July 2008, as published in the Official Journal of the Italian Republic (no. 190 dated 14 August 2008).

369 Italian Personal Data Protection Code, Section 110.2 and Section 7.

370 Garante – Authorisation No. 2/2014, Paragraph 1.2.

371 FINOCCHIARO, *supra* note 256, at 224. *See* M. CASINI, C. SARTEA, *La consulenza genetica in Italia: problemi, regole di consenso informato, trattamento dei dati genetici e privacy*, in *Medicina e morale*, 2009, 1121; M. HÄYRY, R. CHADWICK, V. ARNASON, G. ARNASON (eds.), *The ethics and governance of human genetic databases, European perspectives*, University Press, Cambridge (2007); D. MASCALZONI (ed.), *Ethics, Law and Governance of Biobanking. National, European and International Approaches*, Springer 2015; G. PASCUZZI, U. IZZO, M. MACILOTTI (eds.), *Comparative Issues in the Governance of Research Biobanks*, Springer 2013; E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Cedam, Padova, 2008.

372 Italian Personal Data Protection Code, Section 90.1.

provided to the data subject must make specific reference to "the purposes sought and the results to be achieved also in connection with the unexpected information that may be made known on account of the processing as well as with the data subject's right to object to the processing on legitimate grounds"[373]. The Garante has issued a general authorization for the processing of genetic data in 2014, thereby surrounding this activity with very strict safeguards[374].

The Code also includes specific provisions on medical prescriptions: the rules are different depending on whether or not the drugs are paid by the National Health Service.

As to drugs which are paid by the National Health Service, the provisions aim at "allow[ing for the] establish[ment of] the data subject's identity only if this is necessary in order to check that the prescription is correct or else with a view to administrative controls or for epidemiological and research purposes"[375]. To this end, the prescriptions must be written in a paper form supplemented by a paper tag or a carbon-copy tag[376], which needs to be affixed on the name and address of the patient so that such information is visible only upon transiently removing the tag[377]. Such removal is allowed for two purposes: either to allow a chemist to check that the prescription is correct[378], or to allow the performance of administrative audits or epidemiological surveys or researches[379]. A decree by the Minister of Health, after seeking the Garante's opinion, may lay down further technical solutions[380] aimed at keeping the identity of the patient hidden unless otherwise necessary[381].

On the other hand, when drugs are not paid by the National Health Service the data subject's identity is not specified in the prescriptions[382], unless a physician "considers that it is indispensable to make said data subject personally identifiable on account of an actual requirement that is related either to the data subject's specific condition or to the special arrangements to be made for preparing or using the drug"[383].

The requirements to affix a paper tag on the name of the patient when the drug is paid by the NHS and to avoid identifying the patient in the other cases are conditional upon the data subject's request whenever the involved entities are general practitioners and paediatricians, referred to in Section 78[384].

Finally, there are two special cases where a different regime applies. The first one regards specific laws requiring prescriptions not to allow identification of data subjects or to bear specific notice[385], whereas the second one concerns the Act applying to narcotic drugs and psychotropic substances, prevention, care and rehabilitation of drug addiction, as approved by presidential decree no. 309 of 9 October 1990[386]. In the latter situation, "the

---

373 *Id.*, Section 90.2.

374 Garante per la protezione dei dati personali, General Authorisation No. 8/2014 for the Processing of Genetic Data (published in Italy's Official Journal No. 301 of 30 December 2014).

375 Italian Personal Data Protection Code, Section 87.1.

376 *Id.*, Section 87.2.

377 *Id.*, Section 87.3.

378 *Id.*, Section 87.4.

379 *Id.*, Section 87.5.

380 *Id.*, Section 87.6.

381 *See* MONDUCCI & PASETTI, *supra* note 263, at 276.

382 Italian Personal Data Protection Code, Section 88.1.

383 *Id.*, Section 88.2.

384 *Id.*, Section 89.2-bis.

385 *Id.*, Section Section 89.1. The law mentioned by the Code is Decree-law no. 23 of 17 February 1998 as converted, with amendments, into Act no. 94 of 8 April 1998, which regulates sperimentation of a cancer treatment. *See* MONDUCCI & PASETTI, *supra* note 263, at 277.

386 Italian Personal Data Protection Code, Section 89.2.

relevant prescriptions shall be kept separate from any other document that does not require their use"[387].

Another situation that the Code specifically regulates is the processing of data suitable for disclosing health that are "stored on cards, including non-electronic cards and the national services card, or that are processed by means of said cards"[388]. It is allowed only if absolutely necessary, pursuant to the necessity principle (Section 3) and in compliance with the measures and precautions laid down by the Garante, because it is deemed to imply specific risks for fundamental rights and freedoms[389].

With respect to clinical records, Section 92 requires public and private health care bodies to take "suitable precautions […] to ensure that the data are understandable as well as to keep the data concerning a patient separate from those concerning other data subjects"[390]. Medical records have deeply evolved over the twentieth century and they no longer just represent a way to record clinical data, but rather they enable efficient programming and continuity in the provision of health care services to the same patient[391]. Despite its importance, it has never been the subject of a comprehensive regulation[392].

Access to clinical records is subject to different rules depending on who is requesting access. The data subject has a right to access clinical records about him, as there is no conflict between privacy rights and access rights[393]. Such conflict only arises when the data subject / patient is incapacitated: total incapacitation triggers the possibility for the legal guardian to request access, whereas partial incapacitation raises issues as to whether requesting access to clinical records is among the acts entrusted to the legal guardian[394]. Third parties can only inspect or obtain a copy of the clinical records if "justified because of the proven need to establish or defend a legal claim [… or] to establish a legally relevant claim in pursuance of the legislation concerning access to administrative records"[395]. Such "proven need" must be shown in connection to the data minimization principle[396]. Importantly, such claims must be "equal in rank to the data subject's right or else consisting in a personal right or another, fundamental, inviolable right or freedom"[397] as the patient's right to privacy must be adequately protected[398]. The assessment of whether the claim is "equal in rank" is not an easy task: it is not enough to refer to the constitutionally recognized right to action and defense[399], but rather it is necessary to look at the underlying right that the third party wants to enforce[400]. Some examples in the case law have concerned the right to work or an action brought to annul a marriage[401], whereas

---

387 *Id.*

388 *Id.*, Section 91.

389 *See* MONDUCCI & PASETTI, *supra* note 263, at 278-79.

390 Italian Personal Data Protection Code, Section 92.1.

391 G.M. CAVO, *La cartella clinica e la tutela della riservatezza del malato*, in *Sanità Pubblica e Privata*, 2011, fasc. 2, at 41.

392 MONDUCCI & PASETTI, *supra* note 263, at 279. *See* Royal Decree no. 1631 of 30 September 1938, Presidential Decree No. 128 of 27 March 1969, Decree of the Department of Health of 5 August 1977.

393 CAVO, *supra* note 391, at 46-47. Also, the request can be done orally, even if it is common for health care bodies to require written requests pursuant to their internal regulations. *Id.* at 47.

394 *See* CAVO, *supra* note 391, at 47-48.

395 Italian Personal Data Protection Code, Section 92.2.

396 P. BAICE, *La cartella clinica tra diritto di riservatezza e diritto di accesso*, *Ragiusan* n. 280/290, Sez. 1, 2008.

397 *Id.*

398 *See* CAVO, *supra* note 391, at 50.

399 *See* Constitution of the Italian Republic, Article 24.

400 BAICE, *supra* note 396.

401 *See id.*; Council of State, Section VI, no. 6440/2006; Council of State, Section V, no. 6681/2006.

patrimonial rights have been considered not to be equally ranked with the right to data protection[402].

Section 93 concerns the certificate of attendance at birth, whereby the process of issuing a birth certificate is replaced by a declaration containing only the data that must be entered into the register of births[403]. If the mother has objected to being referred to, the certificate of attendance at birth or clinical records must be subject to suitable precautions to prevent identification[404], and can be issued in full only after one hundred years[405].

4. Health Data Protection in the United States

Health data privacy in the United States, just like privacy in general, "is governed by a myriad of different laws and regulations"[406]. First of all, it is important to note the distinction between the state level and the federal level. State law, namely privacy torts, has traditionally been the main protection for health data, regulating the remedies afforded for intrusions or disclosure of medical information, as well as the confidentiality of the relationship between patients and health caregivers[407]. However, the concern over the use and distribution of medical records has led to the implementation of a more formalized legal scenario. Furthermore, the U.S. Constitution protects health privacy with respect to data maintained by government officials and entities[408]. For our analysis we will focus on the federal legislation, and more specifically on the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[409], which guarantees a minimum level of protection for all states.

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and although its primary goal was "enabl[ing] employees to switch employers without losing health coverage for existing conditions, it also requires states to enact certain privacy protections, such as obtaining consent prior to distributing personal information to marketers"[410]. Thus, it was also meant "to reduce the costs of administrative operations in

---

402 *See* T.A.R. (Regional Administrative Tribunal) Emilia Romagna, Bologna, Section 1, no. 1207/2001.

403 Italian Personal Data Protection Code, Section 93.1. *See* Presidential Decree no. 396/2000, Section 30.

404 Italian Personal Data Protection Code, Section 93.3.

405 *Id.*, Section 93.2. *See* Presidential Decree no. 396/2000, Section 30.1.

406 D. J. SOLOVE, M. ROTENBERG & P. M. SCHWARTZ, *Information Privacy Law,* 2nd edition, Aspen 2006, at 345. *See also* L. GOSTIN, *Health Information Privacy*, in *Georgetown Law Faculty Publications and Other Works*, 1995; M.A. ROTHSTEIN, *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, New Haven, 1997; W.H. ROACH, *Medical Records and the Law*, Sudbury, 2008. For an interesting and useful analysis of the American approach to privacy, see U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano 2008.

407 According to many courts, the disclosure of medical information can give rise to a claim for public disclosure of private facts, which is one of the traditional tort claims established by William Prosser (*see, e.g. Urbaniak v. Newton*, 277 Cal. Rptr. 354 (Cal. App. 1991), *Susan S. v. Israels*, 67 Cal. Rptr. 2d 42 (Cal. App. 1997)). SOLOVE ET AL., *Information Privacy Law*, *supra* note 406, p. 378. In addition to tort law, protection is also provided through state statutes. *See id.* p. 378-79.

408 The leading cases are *Whalen v. Roe*, 429 U.S. 589 (1977), *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977), *United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 578 (3rd Cir. 1980). "The Supreme Court did not elevate privacy rights in medical information to the same level as for physical privacy or decisional autonomy, though the Court acknowledges the existence of the privacy right". W. T. DEVRIES, *Protecting Privacy in the Digital Age*, 18 *Berkeley Tech. L.J.* 283, 302 (2003).

409 Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 5-42 U.S.C.). For a general overview on HIPAA, see S. WU, *A Guide to HIPAA Security and the Law*, Chicago, 2007; P. CARTER, *HIPAA Compliance Handbook*, Gaithersburg, - Alphen, 2014.

410 DEVRIES, supra note 408, at 303. *See also* B. K. HOOVER & M. BRADSHAW, *Not So Hip?: The Expanded Burdens on and Consequences to Law Firms as Business Associates Under HITECH Modifications to HIPAA*, 13 *Rich. J. L. & Pub. Int.* 313, 315-17 (2010).

the healthcare industry by simplifying the exchange of electronically stored medical information", as well as "preventing fraud or unauthorized access, use, and disclosure of" individually identifiable health information[411]. "Although HIPAA was not primarily enacted by Congress to serve as a federal medical privacy act, its privacy implications have been the most far-reaching and broadly impacting part of the legislation"[412], and it "has morphed into a maze of intertwined and interlocking puzzle pieces all intended to protect private health information, increase accessibility of health care, and streamline provider reimbursement through electronic transactions"[413]. As we will further discuss, the primary goal of HIPAA was enhancing efficiency and "reduc[ing] the "back-end," transactional costs of healthcare delivery"[414]. Some have argued that this "instrumental approach", which "see[s] the generation, dispersal, and processing of longitudinal patient health information primarily as a necessity to reduce overall healthcare costs and to minimize medical error"[415], is somehow dangerous and problematic. The introduction of the HIPAA Privacy Rule was not due to "a principled commitment to patient privacy or confidentiality", but aimed at "minimiz[ing] objections to and maximiz[ing] participation in a transactional model desired by industry and promoted by government"[416]. This causes "individual autonomy […] to be viewed as subordinate to broader goals (e.g. lower costs and a reduction in medical errors) that may or may not directly benefit the individual involved"[417].

4.1 The HIPAA Privacy Rule

The implementation of a uniform set of transaction codes to process insurance claims would enable a greater ease of data sharing and transmission, which led to a concern regarding the privacy and security of medical data[418]. This issue was not addressed until the creation of certain regulations by the Department of Health and Human Services (HHS) – the so-called Privacy Rule. They "represent the first systematic national privacy protection of health information"[419] and stem from a recognition of privacy as a "fundamental right"[420]. However, we should not forget that "Congress was barely concerned with issues of privacy when it passed HIPAA", and this omission was recognized only later[421]. The final version of such regulations was released in 2002 and was published at 45 C.F.R. parts 160 through 164.

In *South Carolina Medical Association v. Thompson* (4th Cir. 2003)[422] some arguments were raised challenging the constitutionality of HIPAA, among which was the assertion

---

411 J. T. SOMA, S. D. RYNERSON & E. KITAEV, *Privacy Law in a Nutshell*, 2nd edition, West Academic Publishing 2014, at 114.

412 M. J. POSTER, *HIPAA Confusion: How the Privacy Rule Authorizes "Informal" Discovery*, 44 *University of Baltimore Law Review* 491, 493 (2015).

413 T.J. WHITE & C.A. HOFFMAN, *The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 *W. Va. L. Rev.* 709, 712 (2004).

414 N.P. TERRY, *What's Wrong With Health Privacy?*, 5 *J. Health & Biomedical L.* 1, 12 (2009).

415 N.P. TERRY & L.P. FRANCIS, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 *U. Illinois Law Review* 681, 698-99 (2007).

416 TERRY, *supra* note 414, at 12.

417 *Id.* at 24.

418 SOLOVE ET AL., *supra* note 406, at 379.

419 L. O. GOSTIN & J. G. HODGE, JR., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 *Minn. L. Rev.* 1439 (2002).

420 POSTER, *supra* note 412, at 495 (citing Standard for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,464).

421 P. OHM, *Sensitive Information*, 88 *S. Cal. L. Rev.* (forthcoming 2015), at 20. *See also id.*, at 49.

422 327 F.3d 346 (4th Cir. 2003).

that Congress "unconstitutionally relinquished its lawmaking function"[423] by entrusting an agency with the establishment of privacy regulations. The court disagreed, explaining that "Congress did not abdicate its legislative responsibilities in passing HIPAA, but outlined a broad set of principles to guide HHS action"[424]. Nevertheless, some have maintained that this regime is "not a result of any direct congressional statutory command but instead arose from a fairly broad interpretation of the statute by the implementing agency, and the current state of HIPAA culture bears little resemblance to the original statutory privacy suggestions"[425]. Furthermore, as much as the declared goals of HHS regulations were flexibility and efficiency, some believe that "HIPAA regulatory enforcement has frustrated these goals"[426].

The HIPAA privacy regulations were significantly amended in 2013 after the promulgation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009[427]. The purpose of the amendments in the words of the Office of the Secretary of the Department of Health and Human Services was "strengthen[ing] the privacy and security protections […] for individual's health information maintained in electronic health records and other formats"[428].

4.1.1 Balancing Privacy Against the Common Good: Was HIPAA Successful?

Before diving into an analysis of the most relevant HIPAA privacy provisions, we should take a glance at their outcomes and at how they have been received by the academic community. There have been many critiques of HIPAA, yet most scholars agree that "[p]rivacy is an essential part of providing and receiving medical care, and HIPAA successfully raised the privacy-protection standards"[429]. Indeed, before this law was enacted, personal information sharing policies mostly focused on "what was the least disruptive" to the health care providers rather than on privacy rights, and there was not a nationwide minimum level of protection[430].

Nevertheless, there is much disagreement as to whether HIPAA correctly strikes the right balance between individual privacy and the public good. On one hand, some have argued that some HIPAA provisions give too much room to individual privacy and does not sufficiently take into account the need to use health data for the common interest[431]. On the other hand, HIPAA has been defined as "a national policy promulgated by unelected government officials who succumbed to the interests of commercial enterprise and marginalized the citizen's right to privacy"[432].

---

423 327 F.3d 346, 352 (4th Cir. 2003).

424 *Id.*

425 J. J. WILKES, *The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care*, 2014 *BYU L. Rev.* 1213, 1219 (2015) (citing I. N. MOORE ET AL., *Confidentiality and Privacy in Health Care from the Patient's Perspective: Does HIPAA Help?*, 17 *Health Matrix* 215, 228 (2007)).

426 WILKES, *supra* note 425, at 1220.

427 Health Information Technology for Economic and Clinical Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

428 *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule*, 78 Fed. Reg. 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. part 160 and 164) [hereinafter Modifications to HIPAA Rules].

429 WILKES, *supra* note 425, at 1234.

430 *Id.*

431 *See* GOSTIN & HODGE, *supra* note 419.

432 M. HATCH, *HIPAA: Commercial Interests Win Round Two*, 86 *Minn. L. Rev.* 1481, 1493 (2002). According to Hatch, HIPAA was endorsed by "a closely connected liaison of government agencies, pharmaceutical

As mentioned, some scholars maintain that "health information privacy laws should carefully balance the need for individual privacy with the benefits of using health data for the common good", and that "individual interests […] should not be regarded as absolute"[433]. Thus, Gostin and Hodge, on the common good side of the debate, have suggested a framework that arguably "go[es] beyond the traditional conception of individual autonomy as a dominating factor" and "values both privacy and common goods, without *a priori* favoring either"[434]. Their framework subjects acquisition, use, or disclosure of health information to strict protections whenever it is harmful, and more relaxed rules whenever it aims at important public purposes, provided that "uses are restricted to the purposes for which the data are collected" and "subsequent disclosures for other purposes are prohibited without individual authorization"[435]. This would result in "maximiz[ing] individual privacy interests where the risks of harm are greatest […], and maximize common goods where the public interests are strongest"[436]. They criticize the trend of "us[ing individual autonomy] as a justification for preventing sharing of information irrespective of the good to be achieved", which results in "reduced efficiencies in clinical care, research, and public health"[437]. Highlighting that "more often than not, strict privacy rules dilute public benefits"[438], and that the traditional framework "failed to pay sufficient attention to the many advantages of systematic collection and use of electronic health data"[439], they conclude that "[p]rivacy may need to give way if necessary to promote certain public goods"[440]. Therefore, Gostin and Hodge criticize the general "anti-disclosure rule" embedded in health information privacy laws, which tends to prohibit disclosures of identifiable health information without the individual's consent[441] and is "used as a shield to prevent public and private sharing of health data for the public's health and security"[442]. Some other provisions, in turn, are considered to be "consistent with [their] approach", such as "the requirement for written authorization for many disclosures of health data outside the health care context", which "fulfills individual privacy interests where they matter most"[443].

On the opposite side of the debate, some commentators have argued that "[b]ecause HIPAA permits disclosure without patient authorization in [many] instances [see paragraph 4.1.4.5], the purpose of the patient authorization requirement becomes marginalized". The Gostin-Hodge balancing framework has been harshly criticized inasmuch as it is said to "reject the inherent importance of privacy in our culture"[444]. According to this researcher, since some HIPAA provisions "give commercial marketers access to data that our Constitution deems too sensitive, absent probable cause that a crime has been committed, to be routinely observed by the government", they make "the protections of the Fourth

---

companies, law enforcement agencies, medical device manufacturers, and marketing companies", and "[t]heir success in getting HIPAA adopted shows that their clout rivals that of the military industrial complex at the height of the Cold War". *Id.* at 1493-94.

433 GOSTIN & HODGE, *supra* note 419, at 1440-41.

434 *Id.* at 1441.

435 *Id.* at 1442.

436 *Id.* at 1478.

437 *Id.* at 1443.

438 *Id.* at 1446.

439 *Id.* at 1444.

440 *Id.* at 1449.

441 *Id.*

442 *Id.* at 1453.

443 *Id.* at 1478.

444 HATCH, *supra* note 432, at 1486.

Amendment become marginal"[445]. Therefore, HIPAA has been described as a "capitulation to commercial interests", which "can only be explained by looking to the many lobbyists and commercial interests that have a financial stake in obtaining [health data]"[446]. Another scholar has noted that "what is striking about the administrative standards and compliance mechanisms of the U.S. federal standards is the relatively low level of patient protection they contain", as "the complex regulations read more like a catalogue of exceptions than of rights"[447].

Some of these evaluations were mostly carried out over ten years ago but they nevertheless provide valuable insights as to the challenges inherent in the attempt to balance individual privacy with the public benefit.

4.1.2 Relationship with State Law

State laws that are contrary to the HIPAA Privacy Rule are preempted by the federal requirements[448]. Pursuant to the rule, "contrary" means that "[a] covered entity or business associate would find it impossible to comply with both the State and Federal requirements", or that "[t]he provision of State law stands as an obstacle to accomplishing the full purposes and objectives" of the Administrative Simplification provisions of HIPAA[449]. However, some exceptions are carved out for State laws falling within certain categories[450]. First, the State law applies if the HHS Secretary determines either:

- that it is necessary "to prevent fraud and abuse related to the provision of or payment for health care"[451], or "to ensure appropriate State regulation of insurance and health plans"[452], or "for State reporting on health care delivery or costs"[453], or "for purposes or serving a compelling need related to public health, safety, or welfare" when "the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served"[454];
- or that its "principal purpose" is "the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances"[455].

Other exceptions concern State laws "provid[ing] for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention"[456], or "requir[ing] a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals"[457].

It is important to point out that the contrary State law is also not preempted when it "relates to the privacy of individually identifiable health information and is "more

---

[445] *Id.*
[446] *Id.* at 1493 (also arguing that "[a]ny attempt to justify HIPAA's disclosure rules as reflecting a balance of communal interest versus individual rights is undermined and laid bare by the rules that permit telemarketers to obtain private health data for marketing and fundraising purposes", and that "[p]roponents of such rules should blush when they attempt to justify such activity on the basis of a 'communal interest'").
[447] TERRY, *supra* note 414, at 26.
[448] 45 C.F.R. § 160.203.
[449] 45 C.F.R. § 160.202.
[450] 45 C.F.R. § 160.203.
[451] 45 C.F.R. § 160.203(a)(1)(i).
[452] 45 C.F.R. § 160.203(a)(1)(ii).
[453] 45 C.F.R. § 160.203(a)(1)(iii).
[454] 45 C.F.R. § 160.203(a)(1)(iv).
[455] 45 C.F.R. § 160.203(a)(2).
[456] 45 C.F.R. § 160.203(c).
[457] 45 C.F.R. § 160.203(d).

stringent"[458] than the Privacy Rule[459]. Thus, the HHS regulations cannot preempt state laws that are more protective of privacy, but rather only "create a federal 'floor' of protections"[460]. If a state's laws are less stringent than the HIPAA Privacy Rule or are silent, the federal rules apply[461]. As much as "[t]his multi-level approach allows states to tailor health information privacy policies to the specific needs of their populations", it also triggers potential unfairness and inefficiency in cross-state transactions[462]. Furthermore, some have argued that the threshold was set too low and the minimum requirements should be raised, in addition to the fact that some states (as Ohio did) might decide to "place 'continuity of care' and consistency with the HIPAA Privacy Rule ahead of privacy and change more stringent laws to the minimum required"[463]

Courts interpreting the Privacy Rule are often unable "to make the threshold determination as to whether State law and Federal law are contrary", which is "crucial because if two laws are not contrary, they generally can be reconciled without one law preempting the other, thereby eliminating the need for a more problematic stringency analysis" [464]. However, courts sometimes unnecessarily analyze the "more stringent" requirement after determining that the State law is contrary to HIPAA[465]. This was done in *Law v. Zuckerman*[466], where the court "erroneously […] interpret[ed] "more stringent" to mean "the [increased] ability of the patient to withhold permission and to effectively block disclosure [of their PHI, or protected health information]"[467]. It "more appropriately should have found that if a state law can force disclosure it is impossible to comply with both the State and Federal requirements, thus triggering HIPAA preemption"[468]. A scholar has harshly noted that, in cases like this, "the Privacy Rule […] disrupts existing legal obligations [and] places an undue burden on the judiciary"[469].

4.1.3 When Does the HIPAA Privacy Rule Apply?

The first important and not easily defined issue concerns the circumstances triggering the applicability of HIPAA regulations, which in fact only apply to certain entities, certain types of transactions, and certain kinds of information.

Not all people or entities that have access to health information are subject to the regulations [470]. Rather, "covered entities" are only "health plan[s]", "health care clearinghouse[s]", and "health care provider[s] who [transmit] any health information in electronic form in connection with a [covered] transaction"[471]. This represents an important

---

458 See the definition of "more stringent" at 45 C.F.R. § 160.202.
459 45 C.F.R. § 160.203(b). *See also* WHITE & HOFFMAN, *supra* note 413, at 716.
460 GOSTIN & HODGE, *supra* note 419, at 1465.
461 D. J. SHEFFNER, State ex rel. Proctor v. Messina *and* Ex Parte *Communications Under the HIPAA Privacy Rule: The "Judicial Proceedings" Split*, 39 *Southern Illinois University Law Journal* 71, 76 (2014).
462 WHITE & HOFFMAN, *supra* note 413, at 716.
463 S.O. CORLEY, *Protection for Psychotherapy Notes Under the HIPAA Privacy Rule: As Private As A Hospital Gown*, 22 *Health Matrix: Journal of Law-Medicine* 489, 509-10 (2002).
464 POSTER, *supra* note 412, at 498.
465 *Id.*
466 *Law v. Zuckerman*, 307 F. Supp. 2d 705 (D. Md. 2004).
467 POSTER, *supra* note 412, at 498 (citing *Law*, 307 F. Supp. 2d at 711).
468 POSTER, *supra* note 412, at 499 (citations omitted).
469 *Id.* Poster concludes that "plaintiffs are no longer permitted to utilize the statutes as both a sword and shield to deflect defense counsel's requests for ex parte communications", *id.* at 518, because as much as "the 'informal' nature [of the practice of ex parte communication] has been removed […] the practice is very much alive and well", *id.* at 517.
470 *See* 42 U.S.C. §§ 1320d(5), 1320d-1(a).
471 45 C.F.R. § 160.102.

difference from the European standard: "[c]ontrary to Europe, the HIPAA's applicability depends on who is handling the health data and not on the concept of 'health data' or 'data processing'"[472]. Paul Ohm has recently argued that HIPAA "should be expanded to include any company possessing sensitive health information"[473].

Section 160.103 provides a list of entities included in the definition of "health plan", which can be broadly defined as "[an] individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care"[474]. Health plans "are covered whether they are private entities […] or government organizations"[475]. A health care clearinghouse is "a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity"[476]. A health care provider is "a provider of services […], a provider of medical or health services […], and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business"[477], such as physicians, hospitals, and pharmacists. Health care providers are only subject to HIPAA if they transmit health information in electronic form in connection with a covered transaction[478]. HIPAA lists nine electronic transactions: (A) Health claims or equivalent encounter information; (B) Health claims attachments; (C) Enrollment and disenrollment in a health plan; (D) Eligibility for a health plan; (E) Health care payment and remittance advice; (F) Health plan premium payments; (G) First report of injury; (H) Health claim status; (I) Referral certification and authorization; (J) Electronic funds transfers[479].

Furthermore, there are some entities (so-called "hybrid entities") which, while not falling within the definition of "covered entity", provide some products and services pertaining to health care[480]. "Hybrid entities are less stringently regulated than covered entities" inasmuch as only the component actually performing health care must comply with the regulations[481].

Covered entities must "adopt, implement, monitor, and maintain compliance programs to ensure that the minimal protections under HIPAA for individually identifiable health information are in place and effective", and this task is carried out by "having a designated compliance officer who is responsible for oversight and coordination of a compliance program"[482].

---

472 DUMORTIER & VERHENNEMAN, *supra* note 125, at 33.
473 OHM, *supra* note 421, at 6.
474 45 C.F.R. § 160.103.
475 GOSTIN & HODGE, *supra* note 419, at 1461.
476 45 C.F.R. § 160.103.
477 *Id.*
478 42 U.S.C. § 1320d-1(a)(3).
479 *Id.* §1320d-2(a)(2).
480 *See* 45 C.F.R. § 164.504.
481 SOLOVE et al, *supra* note 406, at 381.
482 WHITE & HOFFMAN, *supra* note 413, at 718; 45 C.F.R. § 164.530.

After the 2013 modifications the Privacy Rule also covers business associates[483], who are now "directly liable for HIPAA compliance"[484]. A business associate is, first of all, a person who "on behalf of [a] covered entity […] creates, receives, maintains, or transmits protected health information"[485]. Also, the definition includes a person who "[p]rovides […] management, administrative, accreditation, or financial services to or for [a] covered entity, […] where the provision of the service involves the disclosure of protected health information" [486]. The extension of the regulations to business associates is necessary because "[w]ithout a regulatory mechanism establishing a minimal and uniform set of obligations for these important non-covered entities that regularly have access to protected health information, HIPAA would be meaningless", as "[n]o covered entity could comply with HIPAA because of the dependent relationships with business associates without recognition of and creation of this vehicle for disclosure"[487]. The final rule makes some clarifications as to the inclusion of some subjects within the definition of business associate. It expressly considers as a business associate a "Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such PHI"[488]. Having "routine access" to PHI is what distinguishes business associates from "mere conduits": "such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to [PHI] to perform the service for the covered entity" [489]. The "conduit exception" is described as "a narrow one", meant to "exclude only those entities providing mere courier services, such as the U.S. Postal Service"[490]. Thus, "occasional, random access to protected health information would not qualify the company as a business associate" [491]. It is important to highlight that "the conduit exception is limited to transmission services", whereas "an entity that maintains [PHI] on behalf of a covered entity is a business associate and not a conduit" regardless of whether it actually views the information[492]. This is based on "the transient versus persistent nature of [the] opportunity" to access PHI[493]. Thus the definition of "business associate" is one who "[…] maintains […]" protected health information on behalf of a covered entity.

Furthermore, "a person who offers a personal health record to one or more individuals on behalf of a covered entity"[494] is also considered a business associate. This is another "fact specific determination"[495].

---

[483] *See* 45 C.F.R. § 160.103 (defining "business associate"). White & Hoffman list some examples of business associates, including "malpractice insurers, accountants, certain vendors, lawyers, and collection agencies", and specify that "a court reporter can be deemed a business associate to any attorney who is a business associate to a hospital client". WHITE & HOFFMAN, *supra* note 413, at 719.

[484] WILKES, *supra* note 425, at 1229. For an overview of business associates' liabilities, see Bryan Cave LLP Global Data Privacy and Security Team, *Business Associates At A Glance: Responsibilities And Liabilities* (2015), available at: http://bryancavedatamatters.com/wp-content/uploads/2015/12/Final-Business-Associates_At-A-Glance.pdf.

[485] 45 C.F.R. § 160.103.

[486] *Id.*

[487] WHITE & HOFFMAN, *supra* note 413, at 729.

[488] 45 C.F.R. § 160.103. *See* Modifications to HIPAA rules, at 5571.

[489] Modifications to HIPAA rules, at 5571.

[490] *Id.*

[491] *Id.* at 5572.

[492] *Id.*

[493] *Id.*

[494] 45 C.F.R. § 160.103. *See* Modifications to HIPAA rules, at 5571.

[495] *Id.* at 5572.

Last, the definition of "business associate" also includes a "subcontractor that creates, receives, maintains, or transmits [PHI] on behalf of the business associate"[496]. A subcontractor for this purpose is "a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate"[497].

In front of this "stark new HIPAA landscape", it has been noted that law firms that receive health information from their clients are now directly responsible for compliance[498], as long as they fall within the definition of business associate. For instance, the firm needs to "observe whether it receives any PHI from its [health care] clients in the course of representation", which triggers "expanded liability under post-HITECH HIPAA"[499].

Another important issue to determine the applicability of the HIPAA regulations is whether the health information is processed and transmitted in a "standard" format. A covered entity is subject to the regulations only as long as it engages in the type of standard transactions that will bring it within the scope of the privacy rule[500].

The kind of health information protected by the regulations (referred to as "PHI", or protected health information) is "individually identifiable health information"[501].

First of all, PHI is a "subset of health information", which in turn is "any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"[502].

Under the definition, "individually identifiable health information":

> "(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual"[503].

Protected health information includes only data which is "individually identifiable", i.e., that contains uniquely identifiable characteristics. Under § 164.502(d)(2), if health information is "de-identified", it is not considered to be subject to the regulations. The issue of de-identification under HIPAA will be dealt with in depth in Chapter III.

---

496 *Id.* at 5573.

497 *Id.*

498 HOOVER & BRADSHAW, *supra* note 410, at 328.

499 *Id.*

500 See the definition of "Transaction" at 45 C.F.R. § 160.103.

501 *See* 42 U.S.C. § 1320d(6).

502 45 C.F.R. § 160.103. *See* 42 U.S.C. § 1320d(4)(B).

503 *Id.* It also includes "demographic information collected from an individual". Furthermore, the statute specifies what is "protectable health information," that is, "individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years". *Id.*

The Rules, after their modification in 2013, do not protect the individually identifiable health information of subjects who have been deceased for more than fifty years[504]. This revision is aimed at "[p]romotion of historical research", as under the original rule the same document would be treated differently if held by a covered entity versus other possessors and "decedent health information was subject to the same protections as the health information of a living person"[505]. A scholar has partly criticized the revision as it "fails to balance the interests at stake by not distinguishing" between incidental health information and clinical records, which arguably should still be with unlimited protection[506].

4.1.4 Use and Disclosure of Protected Health Information

The use and disclosure of PHI under specific circumstances is restricted by the regulations, inasmuch as "[s]ome level of individual control […] is essential to ensure privacy because of the potential risks of harm from unlimited sharing of personal medical data"[507].

As a general rule, "[a] covered entity may not use or disclose protected health information, except either (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information […] authorizes in writing"[508].

Furthermore, regardless of the purpose of the disclosure, a covered entity must comply with a "minimum disclosure rule", i.e., "[w]hen using or disclosing PHI, [it] must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose"[509]. In order to comply with this rule, covered entities must then "develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary" and avoid "us[ing], disclos[ing], or request[ing] the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose"[510]. The "minimum necessary" standard does not apply in a number of listed circumstances, including disclosures to a health care provider for treatment, disclosures to the individual, uses or disclosures made pursuant to an authorization or required by law[511]. The compliance with this rule must be assured within the entities, too, by "develop[ing] and implement[ing] policies and procedures that restrict access and uses of [PHI] based on the specific roles of the members of their workforce"[512]. As for the procedures for disclosures and requests for disclosures, standard policies and protocols may be implemented for "routine, recurring disclosures, or requests for disclosures" in order to limit the PHI disclosed to the minimum amount necessary,

---

504 45 C.F.R. § 164.502(f); Modifications to HIPAA rules, at 5576.

505 M.A. ROTHSTEIN, *HIPAA Privacy Rule 2.0*, *The Journal of Law, Medicine and Ethics* 41(2), 525, 526 (2013).

506 *Id.* Rothstein points out that "[p]roviding unlimited protection for clinical records respects the privacy and confidentiality interests of the decedent and the decedent's family" and is "consistent with the AMA Code of Medical Ethics", which requires that "[a]ll […] information contained within a deceased patient's medical record, including information entered post-mortem, […] be kept confidential to the greatest degree possible". *Id.* (citing American Medical Association, Code of Medical Ethics § 5.051, Confidentiality of Medical Information Postmortem, 2011-2012 ed. (Chicago, American Medical Association)).

507 GOSTIN & HODGE, *supra* note 419, at 1466.

508 Summary of the HIPAA Privacy Rule, Dep't of Health & Human Services, available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf [hereinafter HHS Summary of the HIPAA Privacy Rule], at 4. 45 C.F.R. § 164.502(a).

509 45 C.F.R. § 164.502(b)(1).

510 45 C.F.R. § 164.514(d)(5). HHS Summary of the HIPAA Privacy Rule, at 10.

511 45 C.F.R. § 164.502(b)(2)(i)-(vi).

512 45 C.F.R. § 164.514(d)(2). HHS Summary of the HIPAA Privacy Rule, at 10.

with no need for individual reviews of each disclosure. For non-routine disclosures or requests, covered entities must develop adequate criteria and review each of the requests individually[513]. Whenever PHI held by one covered entity is requested by another covered entity, by a public official, by a business associate, or by a researcher providing the required documentation, the covered entity "may rely, if reasonable under the circumstances, on the request as complying with [the] minimum necessary standard"[514].

4.1.4.1 Required Disclosures

There are two situations in which disclosure is compulsory: first, when the patient requires access to his or her health care information, and secondly, when the Secretary of HHS requests access to the information within an investigation or enforcement action regarding a covered entity's compliance with HIPAA[515].

4.1.4.2 Uses and Disclosures Requiring an Authorization

In some instances, the covered entity needs to obtain the individual's authorization before using or disclosing the relevant PHI[516], and such use or disclosure needs to be consistent with the authorization[517].

Gostin and Hodge positively analyze the provisions requiring an authorization prior to use or disclosure of PHI for non-health care purposes, and say it is "an important privacy safeguard" in a context where "[d]isclosures […] can lead to significant harms" such as "discrimination, stigmatization, or embarrassment", but "are unlikely to achieve an important health-related objective"[518]. Nevertheless, it is important to bear in mind that "sole reliance on authorization *forms* by covered entities and researchers appears to add to the administrative and bureaucratic cloud surrounding research without increasing patient understanding or protection of information", as the authorization process should not focus on the "static […] event" of the authorization form "but rather on a series of dynamic and appropriately targeted conversations between the patient and the covered entity and/or researcher"[519]. It is necessary to rely on a human interaction rather than on bureaucratic requirements.

4.1.4.3 Requirements of a Valid Authorization

There are several requirements that the content of an authorization must meet in order for it to be valid[520]. Interestingly, the rule distinguishes between "elements" – which appear to be items requiring additional input from the covered entity – and "statements" – which seem to be general statements aimed at notifying the patient of a particular fact[521].

---

513 45 C.F.R. § 164.514(d)(3)(i)-(ii), § 164-514(d)(4)(ii)-(iii). HHS Summary of the HIPAA Privacy Rule, at 11.
514 45 C.F.R. § 164.514(d)(3)(iii). HHS Summary of the HIPAA Privacy Rule, at 11.
515 45 C.F.R. § 164.502(a)(2).
516 45 C.F.R. § 164.502(a)(1)(iv).
517 45 C.F.R. § 164.508(a)(1).
518 GOSTIN & HODGE, *supra* note 419, at 1470.
519 S.A. TOVINO, *The Use and Disclosure of Protected Health Information For Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 *South Dakota Law Review* 447, 474 (2004).
520 45 C.F.R. § 164.508(b)(1)(i). Also, the provision clarifies when an authorization is considered "defective". 45 C.F.R. § 164.508(b)(2).
521 TOVINO, *supra* note 519, at 461-62 fn. 69.

Such specific information must be included "to help individuals decide whether to permit disclosure or use"[522].

The "core elements"[523] an authorization ought to include are:

(1) a description of the information that identifies it "in a specific and meaningful fashion[524];

(2) a specific identification of the person(s) authorized to make the use or disclosure[525] and of those to whom it must be made[526];

(3) a description of each purpose of the requested use or disclosure[527];

(4) an expiration date or event[528];

(5) the signature of the individual and the date[529].

Two of these elements are somewhat controversial and deserve a deeper analysis. Element no. (3) used to be interpreted by HHS to mean that the statement must be "research study specific", and that it was not sufficient to identify a nonspecific or future research activity[530]. However, the 2013 amendments to the rules have clarified that an authorization for the use or disclosure of protected health information for research purposes does not need to be study-specific, yet it "must adequately describe [the future research] purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research"[531]. This description "could include specific statements with respect to sensitive research" but it is not mandated[532]. Furthermore, the modified rule "now permits authorizations to include, on an indefinite basis, future health records"[533], as "a description of the protected health information to be used for the future research may include information collected beyond the time of the original study"[534]. Some scholars have spotted a "clear conflict between the goals of protecting privacy and promoting research", because "it is unrealistic to expect that an individual will remember, perhaps several years later, that he or she executed an open-ended authorization for the disclosure of all future health records", thereby exercising his or her right to withdraw[535]. Therefore a better approach would arguably have involved "time-limited authorization[s] for future health records"[536].

Element (4) is "an expiration date or event that relates to the individual or the purpose of the use or disclosure"[537]. When the authorization is for use or disclosure of PHI

---

[522] GOSTIN & HODGE, *supra* note 419, at 1469.

[523] 45 C.F.R. § 164.508(c)(1).

[524] 45 C.F.R. § 164.508(c)(1)(i).

[525] 45 C.F.R. § 164.508(c)(1)(ii).

[526] 45 C.F.R. § 164.508(c)(1)(iii).

[527] 45 C.F.R. § 164.508(c)(1)(iv). "The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose". *Id.*

[528] 45 C.F.R. § 164.508(c)(1)(v).

[529] 45 C.F.R. § 164.508(c)(1)(vi).

[530] TOVINO, *supra* note 519, at 463. According to this scholar, this seemed "to promote patient autonomy and should be considered a positive development" in that it used to "[increase] the likelihood that a particular patient will be able to make a quality decision regarding the use and disclosure of her PHI", as well as "increase the chance that some individuals [would] authorize their information to be used and disclosed". *Id.* at 464.

[531] Modifications to HIPAA rules, at 5612. *See also* ROTHSTEIN, *supra* note 505, at 526.

[532] *Id.*

[533] ROTHSTEIN, *supra* note 505, at 526.

[534] Modifications to HIPAA rules, at 5613.

[535] ROTHSTEIN, *supra* note 505, at 526.

[536] *Id.*

[537] 45 C.F.R. § 164.508(c)(1)(v).

for research, it is sufficient to state "end of the research study", "none", or "similar language"[538]. This is how the Privacy Rule aims at "permit[ting] the completion of research studies that do not always have a specific "end" date [or] the creation of research databases, which are maintained indefinitely"[539]. However, the suggested statement "none" is not explanatory and possibly confusing, whereas the language "at the end of the research study" at least attempts to explain why there is no expiration date[540].

In addition, the authorization needs to contain "statements adequate to place the individual on notice"[541]: (I) of his right to revoke the authorization[542]; (II) of whether the treatment, payment, enrollment or eligibility for benefits may be conditioned on the authorization[543]; and (III) of the "potential for information […] to be subject to redisclosure by the recipient and no longer be protected"[544]. This would appear to increase the likelihood of quality decisions made by patients regarding the use and disclosure of their PHI, but this clashes with the complexity with which many covered entities draft their authorization forms[545]. Thus, as much as individuals need to know about the consequences of authorizing the disclosure of their PHI, "patients who have little understanding of federal or state privacy law may have difficulty understanding the covered entities' various attempts to put this idea on paper"[546].

Furthermore, the authorization needs to be written "in plain language"[547] and a copy of it must be provided to the individual[548].

Compound authorizations, i.e., authorizations combined with other documents, which then "[purport] to authorize more than one type of use or disclosure of PHI"[549], are only permitted in some limited cases[550]. For instance, authorizations concerning psychotherapy notes may only be combined with other authorizations for a use or disclosure of the same type of notes[551]. Also, an authorization related to a research study may be combined with other written permission for the same or another study[552]. This provision "allow[s] for the use of compound authorizations for any type of research activities, except to the extent that research involves the use or disclosure of psychotherapy notes", e.g., "for the use of [PHI] in a clinical trial and optional sub-studies, as well as for biospecimen banking that also permits future secondary use of the data"[553]. Unfortunately, "this can result in a situation in which information is presented to the patient in a disorganized fashion", which undermines the goal of allowing more thoughtful choices on the part of individuals[554].

---

538 *Id.*
539 TOVINO, *supra* note 519, at 466.
540 *Id.*
541 45 C.F.R. § 164.508(c)(2).
542 45 C.F.R. § 164.508(c)(2)(i).
543 45 C.F.R. § 164.508(c)(2)(ii).
544 45 C.F.R. § 164.508(c)(2)(iii).
545 TOVINO, *supra* note 519, at 466-67.
546 *Id.* at 468-69.
547 45 C.F.R. § 164.508(c)(3).
548 45 C.F.R. § 164.508(c)(4).
549 ROTHSTEIN, *supra* note 505, at 525.
550 45 C.F.R. § 164.508(b)(3).
551 45 C.F.R. § 164.508(b)(3)(ii).
552 45 C.F.R. § 164.508(b)(3)(i).
553 Modifications to HIPAA Rules, at 5610.
554 TOVINO, *supra* note 519, at 470.

The provision of research-related treatment is one of the narrow exceptions to the prohibition on conditioning treatment or enrollment in health plans on authorizations[555], and it is the only case in which an authorization conditioning the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits can be combined with another[556].

As just stated, conditioning the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization is generally prohibited[557], in order to "prevent covered entities from coercing individuals into signing an authorization for use or disclosure that is not necessary to carry out the primary services that the covered entity provides to the individual"[558]. Gostin and Hodge appreciate this provision because "an individual's choice is respected" as "[t]he exercise of the right of refusal [generally] cannot be used to deny the patient treatment or health insurance"[559]. There are some limited exceptions to this ban. Along with the aforementioned provision on conditioning research-related treatment by a health care provider [560], it is possible for a health plan to "condition enrollment in the health plan or eligibility for benefits on provision of an authorization"[561] if it is for the health plan's eligibility or enrollment determinations relating to the individual, or for its underwriting or risk rating determinations[562] (excluding psychotherapy notes[563]). It is also possible to "condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party"[564].

An authorization can always be revoked in writing unless the covered entity has already taken action or the authorization was a condition of obtaining insurance coverage and the insurer lawfully has the right to contest a claim[565].

4.1.4.4 Instances Requiring an Authorization

We can now look at the specific situations in which an authorization is required.

First of all, an individual's authorization must be obtained for the use or disclosure of psychotherapy notes[566]. Such notes, according to HHS, are the "personal notes of the treating provider" and are "not intended to communicate to, or even be seen by, persons other than the therapist"[567]. However, many claimed that psychotherapy notes should also include other data, including results of tests and summary of diagnosis, symptoms, and

---

555 "A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section". 45 C.F.R. § 164.508(b)(4)(i). When this happens, "any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization". 45 C.F.R. § 164.508(b)(3)(i).

556 45 C.F.R. § 164.508(b)(3)(iii).

557 45 C.F.R. § 164.508(b)(4).

558 TOVINO, *supra* note 519, at 471.

559 GOSTIN & HODGE, *supra* note 419, at 1469. 45 C.F.R. § 164.508(b)(4).

560 45 C.F.R. § 164.508(b)(4)(i).

561 45 C.F.R. § 164.508(b)(4)(ii).

562 45 C.F.R. § 164.508(b)(4)(ii)(A).

563 45 C.F.R. § 164.508(b)(4)(ii)(B).

564 45 C.F.R. § 164.508(b)(4)(iii).

565 45 C.F.R. § 164.508(b)(5).

566 45 C.F.R. § 164.508(a)(2).

567 *See* 65 Fed. Reg. at 82,623 (Dec. 28, 2000).

progress[568]. Arguably, not including these other kinds of data "failed to properly consider the changes to the health-care system caused by expanded use of [electronic health records], including the growing number of person [sic] who have access to a patient's medical records"[569]. Under HIPAA, then, psychotherapy notes are those taken by a mental health professional "documenting or analyzing the contents of conversation" during a counseling session[570], and they must be separated from the rest of the individual's medical record[571], i.e. kept separate in a distinct filing space[572].

A psychotherapist may use or disclose the notes without authorizations in multiple situations listed by the HIPAA privacy provisions:

1) to lessen the threat of imminent death or other severe consequences to a person or the public[573];
2) use by the covered entity who originated the notes for treatment[574];
3) use by a covered entity for training programs[575];
4) use by a covered entity to defend itself in legal proceedings brought by the individual[576];
5) use or disclosure to a health oversight agency that is required or permitted with respect to oversight of the originator of the notes[577];
6) when required to investigate or determine the covered entity's compliance with e-privacy of individually identifiable health information[578];
7) disclosure of PHI to a coroner or medical examiner[579];
8) when required by law[580].

These exceptions mostly represent "a reasonable risk-benefit ratio", as they are based, for instance, on "easily identifiable ethical reasons", or they do not cause excessive harm to the patient, or they are necessary for enforcement purposes[581]. However, exception 2) allowing the originator of the notes to use them for treatment without patient authorization "gives psychotherapists unilateral discretion to decide whether or not to use or disclose" them, which "may cause harmful consequences, such as a patient's decision to forego psychotherapy altogether"[582]. Another problem is that some psychotherapists record

---

568 CORLEY, *supra* note 463, at 512.
569 Id. at 513.
570 45 C.F.R. § 164.501. Therefore, "if notes are recorded from a psychological assessment conducted outside of a counseling session", or "if a patient discusses her mental health with a provider other than a mental health professional", the notes will not qualify as psychotherapy notes. Corley, *supra* note 463, at 513. These limitations are "reasonable because the purpose of the protection is full and frank disclosure in the context of psychotherapy". *Id.*
571 45 C.F.R. § 164.501.
572 CORLEY, *supra* note 463, at 514.
573 45 C.F.R. § 164.512(j)(1)(i) ("A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure: (i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and (B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat").
574 45 C.F.R. § 164.508(a)(2)(i)(A).
575 45 C.F.R. § 164.508(a)(2)(i)(B).
576 45 C.F.R. § 164.508(a)(2)(i)(C).
577 45 C.F.R. § 164.508(a)(2)(ii) (referring to § 164.512(d)).
578 45 C.F.R. § 164.502(a)(2)(ii).
579 45 C.F.R. § 164.512(g)(1).
580 45 C.F.R. § 164.512.
581 CORLEY, *supra* note 463, at 515-16.
582 Id. at 517.

all notes in the patient's general records, not perceiving an advantage in keeping separate notes, or are totally unaware of these provisions[583].

The second situation requiring an authorization concerns marketing communications[584], i.e. "communication[s] about a product or service that [encourage] recipients […] to purchase or use the product or service"[585]. This provision was modified based on the belief that "requiring authorizations for all subsidized communications that market a health related product or service is the best policy"[586]. Whenever marketing involves "financial remuneration […] to the covered entity from a third party, the authorization must state that such remuneration is involved"[587].

Pursuant to the Privacy Rule, "marketing" as defined does not apply in two instances. Firstly, the definition of marketing does not apply when the financial remuneration[588]received is reasonably related to the cost, and communications are made "to provide refill reminders or otherwise communicate about a drug […] currently […] prescribed". Secondly, communications are not considered to be marketing communications when the entity does not receive any financial remuneration and communications are made "for treatment of an individual by a health care provider", or "to describe a health-related product or service […] provided by […] the covered entity making the communication", or "for case management or care coordination"[589].

Also, some communications for marketing are excepted from the need to obtain an authorization, i.e., "face-to-face communication[s] made by a covered entity to an individual"[590], or "promotional gift[s] of nominal value provided by the covered entity"[591].

The commercial marketing exception has been heavily criticized in that it "infringes individual privacy interests by disclosing PHI to others for non-health related purposes that most do not view as societally beneficial"[592]. Thus, Gostin and Hodge wrote that "the claim for non-consensual access to PHI is [here] unjustified" in that "it is motivated by profit-oriented goals"[593]. However, the 2013 modifications have represented a remarkable switch. Under the pre-existing rules, individuals were vested with the right to opt out, but "[b]ecause the individual must now sign an authorization before the covered entity can make subsidized treatment communications, there is no longer any need to require each such communication to contain a clear and conspicuous opportunity for the individual to elect not to receive any more of these communications"[594].

---

583 Id. at 517-18. For some proposed amendments to these provisions, see id. at 525-34.
584 45 C.F.R. § 164.508(a)(3).
585 45 C.F.R. § 164.501.
586 Modifications to the HIPAA Rule, *supra* note 428, at 5595.
587 45 C.F.R. § 164.508(a)(3)(ii). This is one of the requirements for an authorization to be "valid". 45 C.F.R. §164.508(b)(1)(i).
588 "Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual". 45 C.F.R. § 164.501.
589 45 C.F.R. § 164.501.
590 45 C.F.R. § 164.508(a)(3)(i)(A).
591 45 C.F.R. § 164.508(a)(3)(i)(B).
592 GOSTIN & HODGE, *supra* note 419, at 1477.
593 *Id.* at 1477-78.
594 Modifications to HIPAA rules, at 5596. The opt out requirement, anyway, was subject to several criticisms. Hatch noted, for example, that "[g]iven the low response rate by bank depositors to the 'privacy notice' required by [the Gramm-Leach-Bliley Act], it [was] unlikely that many patients [would] have the presence of mind during a telemarketing call to request that the information be suppressed". HATCH, *supra* note 432, at 1484

The provision on marketing communications can be linked with data-mining practices, i.e., the purchase of prescription data from the pharmacies by companies who then sell aggregations and reports to drug manufacturers[595]. Indeed, pharmacies are covered entities under HIPAA, but there is an issue as to whether the prescription information constitutes protected health information, inasmuch as it is usually de-identified[596]. However, HIPAA marketing restrictions also concern "use" of information, and in order to de-identify information covered entities must "use" it[597]. The de-identification qualifies as a marketing use because its purpose was enabling sales of the PHI to the data miners[598]. Under this interpretation, "whenever the purpose of de-identification is marketing, the pharmacy must first obtain a written authorization from every individual whose protected health information is being so used"[599]: this would "[add] so much additional effort and cost to data mining that drug companies will probably no longer find it a cost-effective tool for detailing"[600]. Nevertheless, there is a continuing failure to apply the marketing provisions of the HIPAA Privacy Rule to data mining[601]. Many states have laws prohibiting pharmacies from selling de-identified prescription information to data miners, but according to the aforementioned interpretation of the HIPAA Privacy Rule it already restricts not only such sales, but even the de-identification of health information for marketing purposes without an authorization[602].

Another scenario involving the need to obtain an individual's authorization is the sale of protected health information[603], i.e., a disclosure of PHI by a covered entity or business associate where it "directly or indirectly receives remuneration from or on behalf of the recipient"[604]. The authorization must specify that the disclosure involves a remuneration[605]. However, several exceptions are carved out, and sale of PHI is not considered to include a disclosure of PHI in the following situations:

a. for public health purposes pursuant to § 164.512(b) [see paragraph 4.1.4.5] or § 164.514(e) [see analysis of the provisions on limited data sets in paragraph 4.1.4.5][606];
b. for research purposes pursuant to § 164.512(i) [see paragraph 4.1.4.5] or § 164.514(e) [see analysis of the provisions on limited data sets in paragraph 4.1.4.5], as long as the remuneration is only "a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes"[607]. Thus, "the covered entity may be compensated by a sponsor for performing

---

595 B. COHEN, *Regulating Data Mining Post*-Sorrell: *Using HIPAA To Restrict Marketing Uses of Patients' Private Medical Information*, 47 *Wake Forest Law Review* 1141, 1144, 1166 (2012).
596 *Id.* at 1168.
597 *Id.*
598 *Id.* at 1168-69.
599 *Id.* at 1170.
600 *Id.*
601 *Id.* at 1171.
602 *Id.* at 1182. Furthermore, Cohen subjects the HIPAA Privacy Rule to the analysis carried out by the Supreme Court in *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011), and concludes that the HIPAA Privacy Rule could not be deemed invalid for a violation of the First Amendment, in that it has a very different structure from the one of the state law invalidated by the Sorrell holding. *Id.*
603 45 C.F.R. § 164.508(a)(4); § 164.502(a)(5)(ii)(A).
604 45 C.F.R. § 164.502(a)(5)(ii)(B)(1).
605 45 C.F.R. § 164.508(a)(4)(ii). Without this clarification the authorization cannot be considered "valid". 45 C.F.R. §164.508(b)(1)(i).
606 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(i).
607 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(ii).

research" and "only the disclosure of PHI associated with the research is subject to this limitation"[608];

c. for treatment and payment purposes pursuant to § 164.506(a)[609];
d. for the sale, transfer, merger, or consolidation of all or part of the entity and for related due diligence[610];
e. for the activities undertaken by a business associate on behalf of a covered activity (or by a subcontractor on behalf of a business associate), as long as the remuneration is just for the performance of such activities[611];
f. to an individual, when requested under § 164.524 or § 164.528[612];
g. required by law as permitted under § 164.512(a)[613]; and
h. for any other permitted purpose, as long as the only remuneration is "a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law"[614].

Furthermore, use or disclosure of PHI for scientific research also requires the covered entity to obtain an authorization, unless it obtains a waiver or it employs limited data sets (see paragraph 4.1.4.5).

4.1.4.5 Permitted Uses and Disclosures With No Need for an Authorization

A covered entity is permitted to use and disclose PHI without an individual's authorization for some listed purposes or situations[615]:

1) to the individual who is the subject of the information[616];

2) for treatment, payment, and health care operations[617]: "[a] covered entity may use or disclose protected health information for its own treatment, payment, or health care operations"[618], as well as for the treatment activities of any health care provider[619], or the payment activities of another covered entity and of any health care provider[620]. Also, a covered entity may use or disclose PHI for the health care operation activities of another covered entity provided that "each entity either has or had a relationship with the individual who is the subject of the [PHI]", the information "pertains to such relationship", and the disclosure is for the purpose of either quality assessment and improvement, or competency assurance, or "fraud and abuse detection or compliance"[621]. In these instances obtaining consent is

[608] ROTHSTEIN, *supra* note 505, at 525.
[609] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(iii).
[610] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(iv).
[611] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(v).
[612] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(vi).
[613] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(vii).
[614] 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(viii).
[615] 45 C.F.R. § 164.502(a)(1).
[616] 45 C.F.R. § 164.502(a)(1)(i).
[617] 45 C.F.R. § 164.502(a)(1)(ii). See definitions of "treatment", "payment", and "health care operations" at § 164.501.
[618] 45 C.F.R. § 164.506(c)(1).
[619] 45 C.F.R. § 164.506(c)(2).
[620] 45 C.F.R. § 164.506(c)(3).
[621] 45 C.F.R. § 164.506(c)(4).

merely optional for all covered entities[622], and "[t]he content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent"[623];

3) incident to a use or disclosure otherwise permitted or required[624], as long as the shared information was limited to the "minimum necessary"[625] and the entity has in place "appropriate administrative, technical, and physical safeguards"[626];

4) with an opportunity to agree or to object[627]: in some instances the covered entity is allowed to use or disclose PHI if "the individual is informed in advance" and "has the opportunity to agree to or prohibit or restrict the use or disclosure", and these communications may occur orally[628]. Such situations may concern facility directories[629] or the purposes of the individual's care or notification[630]. Under the first provision, "[a] covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the […] facility"[631], whereas under the second one informal permission is deemed to be sufficient "to disclose to the individual's family, relatives, or friends, or to other [identified] persons, [PHI] directly relevant to that person's involvement in the individual's care or payment for care"[632]. If there is a situation of emergency or incapacitation, disclosures can be made in the patient's best interest[633]. Thus, familial notification represents one of the exceptions to the general anti-disclosure rule established for uses and disclosures not related to health care purposes[634].

Furthermore, covered entities do not need an authorization to use, or disclose to business associates or institutionally related foundations, some listed types of PHI for fundraising purposes[635], as long as they meet certain requirements, such as the right of the individual to have a "clear and conspicuous opportunity to elect not to receive any further fundraising communications"[636]. Also, entities may not condition treatment or payment on such choice[637], and must give the individual the opportunity to opt back[638].

---

622 45 C.F.R. § 164.506(b)(1).
623 HHS Summary of the HIPAA Privacy Rule, at 5.
624 45 C.F.R. § 164.502(a)(1)(iii).
625 45 C.F.R. § 164.502(b), 164.514(d)
626 45 C.F.R. § 164.530(c)(1).
627 45 C.F.R. § 164.502(a)(1)(v).
628 45 C.F.R. § 164.510
629 45 C.F.R. § 164.510(a).
630 45 C.F.R. § 164.510(b).
631 Summary of the HIPAA Privacy Rule, *supra* note 508, at 6; 45 C.F.R. § 164.510(a).
632 Summary of the HIPAA Privacy Rule, *supra* note 508, at 6; 45 C.F.R. § 164.510(b). For instance, a pharmacist may "dispense filled prescriptions to a person acting on behalf of the patient", and family members or others responsible for the individual may be notified of his or her location, condition, or death. Also, "[PHI] may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts". Summary of the HIPAA Privacy Rule, *supra* note 508, at 6.
633 45 C.F.R. § 164.510(b)(3).
634 *See* GOSTIN & HODGE, *supra* note 419, at 1471, 1475-76.
635 45 C.F.R. § 164.514(f)(1).
636 45 C.F.R. § 164.514(f)(2)(ii). "The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost". Id.
637 45 C.F.R. § 164.514(f)(2)(iii).
638 45 C.F.R. § 164.514(f)(2)(v).

Other situations allowing the use or disclosure of protected health information without the individual's authorization or consent are represented by twelve national priority goals[639], "in recognition of the important uses made of health information outside of the health care context"[640]. These situations represent exceptions to the general principle according to which use and disclosure of protected health information outside of health care purposes are subject to the individual's authorization[641].

a) Required by law[642]:

Use or disclosure of PHI is "required by law" whenever there is "a mandate contained in law that compels an entity to make [such] use or disclosure […] and that is enforceable in a court of law"[643]. This includes court orders, subpoenas, statutes, and regulations[644]. The applicability of this exception, though, is subject to the threshold preemption inquiry[645].

b) Public health activities[646]:

This broad exemption concerns disclosures of protected health information for routine public health activities[647], which is highly necessary in cases of threats coming from communicable diseases (e.g., to identify people who might be at risk for infection)[648]. This includes disclosures to (1) public health authorities authorized by law to collect and receive such information to prevent or control disease, injury, or disability, or to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as tracking of products and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease; and (4) employers, for information concerning a work-related illness or injury or workplace-related medical surveillance, in order for the employer to comply with the laws[649]. Noticeably, state reporting or other public health laws, even if they offer a lower standard of protection, are not preempted[650].

This exception from consent or authorization requirements has been said by Gostin & Hodge to "[reflect] a proper balance of individual and collective interests" because, as much as "the autonomous interests of individual are infringed to some extent", individuals are contributing to "greater goods in society"[651]. However, Swire & Steinfeld noticed that the statute only applies to covered entities or business associates, and not to public health

---

639 45 C.F.R. § 164.502(a)(1)(vi).
640 Summary of the HIPAA Privacy Rule, *supra* note 508, at 6.
641 *See* GOSTIN & HODGE, *supra* note 419, at 1470-71.
642 45 C.F.R. § 164.512(a).
643 45 C.F.R. § 164.103.
644 *See id.*
645 POSTER, *supra* note 412, at 497; see above paragraph 4.1.2.
646 45 C.F.R. § 164.512(b).
647 GOSTIN & HODGE, *supra* note 419, at 1471.
648 P.P. SWIRE & L.B. STEINFELD, *Security and Privacy After September 11: The Health Care Example*, 86 *Minn. L. Rev.* 1515, 1526-27 (2002).
649 HHS Summary of the HIPAA Privacy Rule, at 7; GOSTIN & HODGE, *supra* note 419, at 1471.
650 45 C.F.R. § 160.203(c). Indeed, the rule "leaves intact (1) existing state law requirements for the use or disclosure of identifiable health data by public health authorities; and (2) public health information privacy regulations under an inconsistent array of state laws". GOSTIN & HODGE, *supra* note 419, at 1472 (suggesting "the need for better privacy protections for state public health data").
651 GOSTIN & HODGE, *supra* note 419, at 1472.

agencies (or those who receive the PHI from them)[652]. These "largely unregulated instances" due to the fact that "the Department of Health and Human Services simply lacked authority to craft privacy and security protections once the data were in the hands of the public health agencies" are likely to result in significant privacy issues[653].

c) Victims of abuse, neglect, or domestic violence[654]:

This exception applies to disclosures of PHI to government authorities, when the information is "about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence"[655]. This is allowed either (1) if required by law[656], or (2) if the individual agrees[657], or (3) if the disclosure is expressly authorized by statute or regulation and the entity, "in the exercise of professional judgment, believes [it] is necessary to prevent serious harm to the individual or other potential victims"[658], or the individual is unable to agree and a public official authorized to receive the report represents that the PHI is not intended to be used against the individual and that an enforcement activity would be materially and adversely affected by waiting until the individual is able to agree[659]. The individual must be promptly informed that the report has been or will be made[660], unless – according to the professional judgment of the covered entity – this would place him at risk of serious harm[661], or the covered entity would be informing a personal representative whom it reasonably believes to be responsible for the abuse and informing him would not be in the best interest of the individual[662].

d) Health oversight activities[663]:

Pursuant to this exception, a covered entity can disclose PHI "to a health oversight agency for oversight activities authorized by law"[664]. These oversight activities may concern, for instance, the health care system, or government benefit programs[665], but cannot include investigations or activities "in which the individual is the subject [and which] does not arise out of and is not directly related to the receipt of health care or public benefits related to health"[666].

e) Judicial and administrative proceedings[667]:

Under this provision, PHI may be disclosed by a covered entity, first of all, "in the course of any judicial or administrative proceeding" in response to an order of a court[668]. Alternatively, there can be a disclosure in response to a subpoena or discovery request[669],

---

[652] SWIRE & STEINFELD, *supra* note 648, at 1528.
[653] *Id.* at 1528-29.
[654] 45 C.F.R. § 164.512(c).
[655] 45 C.F.R. § 164.512(c)(1).
[656] 45 C.F.R. § 164.512(c)(1)(i).
[657] 45 C.F.R. § 164.512(c)(1)(ii).
[658] 45 C.F.R. § 164.512(c)(1)(iii)(A).
[659] 45 C.F.R. § 164.512(c)(1)(iii)(B).
[660] 45 C.F.R. § 164.512(c)(2).
[661] 45 C.F.R. § 164.512(c)(2)(i).
[662] 45 C.F.R. § 164.512(c)(2)(ii).
[663] 45 C.F.R. § 164.512(d).
[664] 45 C.F.R. § 164.512(d)(1).
[665] 45 C.F.R. § 164.512(d)(1)(i)-(iv).
[666] 45 C.F.R. § 164.512(d)(2).
[667] 45 C.F.R. § 164.512(e).
[668] 45 C.F.R. § 164.512(e)(1)(i).
[669] 45 C.F.R. § 164.512(e)(1)(ii).

but only if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made: either to ensure that the individual who is the subject of the requested information has been given notice[670], or to secure a qualified protective order[671]. Without receiving such satisfactory assurance, disclosure pursuant to a lawful process, such as a subpoena, is allowed "if the covered entity makes reasonable efforts" to obtain it[672].

An important issue is whether HIPAA forbids *ex parte* communications, i.e. "oral communications between defense counsel and a plaintiff's treating, non-party health care provider, without the presence of plaintiff"[673]. It is "a long-established method of discovery that provides benefits to both plaintiffs and defendants", as it is "more conducive to spontaneity and less intimidating than depositions", and it is time-saving and efficient in that it only requires one party to be present[674]. In spite of this, many policy arguments have been raised against this practice, including the risk of disclosure of "confidential information unrelated to the lawsuit"[675]. The courts have adopted three different interpretations as to whether ex parte communications are banned by the HIPAA Privacy Rule. The first, more conservative, line of cases has found the answer to be in the positive[676], but it "represents the judiciary's growing tendency to liberally construe the Privacy Rule to fit each individual case before it, exemplifying the growing lack of uniformity with respect to HIPAA application"[677]. According to the second interpretation, *ex parte* communications are allowed as long as some requirements are met[678]. Within this trend, most courts have interpreted § 164.512(e)(1) holding that courts can order *ex parte* communications as long as the "protective order limit[s] the scope of such discussions to

---

[670] 45 C.F.R. § 164.512(e)(1)(ii)(A). For these purposes, receiving "satisfactory assurances" means receiving "a written statement and accompanying documentation demonstrating that (A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and (C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and: (1) No objections were filed; or (2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution". 45 C.F.R. § 164.512(e)(1)(iii).

[671] 45 C.F.R. § 164.512(e)(1)(ii)(B). For these purposes, receiving "satisfactory assurances" means receiving "a written statement and accompanying documentation demonstrating that: (A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or (B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal". 45 C.F.R. § 164.512(e)(1)(iv). A qualified protective order is "an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and (B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding". 45 C.F.R. § 164.512(e)(1)(v).

[672] "[A] covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section". 45 C.F.R. § 164.512(e)(1)(vi).

[673] SHEFFNER, *supra* note 461, at 72.

[674] POSTER, *supra* note 412, at 506-07.

[675] *Id.* at 507.

[676] *See id.* at 508-512.

[677] *Id.* at 512.

[678] *Id.*

medical information at issue in the case"[679]. According to some other courts, it is enough that the defendant has used "reasonable efforts" in securing a qualified protective order[680]. Finally, there is a third category of dispositions questioning HIPAA's applicability[681]. A case of the Supreme Court of Missouri[682] held that under the judicial proceedings exception *ex parte* communications are not authorized. First, the court found that there was no applicable state law on point and thus the HIPAA Privacy Rule provisions applied[683]. The court next analyzed the meaning of the words of the provision[684], presuming that they were used in accordance with their plain and ordinary meanings[685], and determined that in order for the language "in the course of a judicial […] proceeding" to apply, disclosures must be made "under the supervisory authority of the court either through discovery or through other formal court procedures" [686]. Because *ex parte* communications are informal proceedings over which trial courts in Missouri do not have supervisory authority, the court held that such communications are not authorized by the "judicial proceedings" exception[687]. According to a commentator, even if "Missouri stands alone"[688], *Proctor* was correctly decided because, while also complying with the most direct and plain reading of the provision, it comports with prevailing notions of public policy aimed at "protecting physicians from the risk of unfair sanctions caused by inadvertently divulging protected information during *ex parte* communications" [689] and at avoiding violations of the physician's duty of confidentiality[690]. However, others maintain that as much as informal *ex parte* communications are no longer possible, the mechanism created by the provision we are analyzing allows this kind of communications as long as it satisfies the formal requirements[691]. "These varying interpretations […] exemplify the need for immediate clarification" of the HIPAA Privacy Rule[692].

f) Law enforcement purposes[693]:

Covered entities are allowed under this exception to disclose PHI to law enforcement officials for law enforcement purposes in six situations:

1. as required by law, including laws that require the reporting of physical injuries[694], or in compliance with court orders, court-ordered warrants, subpoenas, or administrative requests[695];

---

679 SHEFFNER, *supra* note 461, at 78. *See Holmes v. Nightingale*, 158 P.3d 1039, 1044 (Okla. 2007). Interestingly, there is also a state law split as to whether such communications are permissible. Most states either explicitly prohibit this kind of communications or place strict restrictions on them, based on public policy reasons or on the protection of the physician-patient privilege or of the physician's confidentiality duty, but there have been some state courts holding that they are permitted. SHEFFNER, *supra* note 461, at 73. *See also* POSTER, *supra* note 412, at 512-14; *Smith v. Rafalin*, 800 N.Y.S.2d 357 (N.Y. Sup. Ct. Mar. 24, 2005); *Bayne v. Provost*, 359 F. Supp. 2d 234 (N.D.N.Y. 2005).

680 SHEFFNER, *supra* note 461, at 78. *See, e.g.*, *Holman v. Rasak*, 785 N.W.2d 98, 109 (Mich. 2009).

681 POSTER, *supra* note 412, at 514-516.

682 *State* ex rel. *Proctor v. Messina*, 320 S.W.3d 145 (Mo. 2010) (*en banc*).

683 *Id.* at 153.

684 *Id.* at 155-57.

685 *Id.* at 155.

686 *Id.* at 156.

687 *Id.* at 157.

688 SHEFFNER, *supra* note 461, at 78.

689 *Id.* at 80.

690 *Id.* at 81.

691 POSTER, *supra* note 412, at 517-18.

692 *Id.* at 508.

693 45 C.F.R. § 164.512(f).

694 45 C.F.R. § 164.512(f)(1)(i).

2. disclosure of limited information[696] to identify or locate a suspect, fugitive, material witness, or missing person[697];
3. disclosure in response to a law enforcement official's request for information about a victim or suspected victim of a crime[698], as long as he or she agrees[699] or, if unable to agree, there is a representation by the official that the information is needed to determine whether a law violation has occurred and is not intended to be used against the victim[700], and that failure to timely disclose the requested PHI would materially and adversely affect immediate law enforcement activity[701], and the disclosure is in the best interests of the individual according to the covered entity's professional judgment[702];
4. disclosure to alert law enforcement of a person's death, if the covered entity suspects that it was caused by criminal conduct[703];
5. disclosure of PHI that the covered entity believes in good faith constitutes evidence of criminal activity that occurred on its premises[704];
6. disclosure by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or of its victims, and the perpetrator of the crime[705].

When health data is shared for law enforcement purposes, it is difficult to balance the competing interests[706]. On one hand, there is an understandable concern of the individuals about the sharing of their data with government officials who have the power to use such data in ways that may negatively affect them, but on the other hand, law enforcement officials may need the data to protect the health or lives of the individual or of others[707]. The HIPAA Privacy Rule "specifically treats public safety as a national priority that, under certain circumstances, trumps the need to obtain patient permission for disclosures of health information"[708]. It has been argued, however, that these regulations too broadly allow unauthorized disclosures to law enforcement officials, and should rather require a court order prior to disclosure[709].

g) Decedents[710]:

Pursuant to this provision, PHI can be disclosed by covered entities to funeral directors, coroners, or medical examiners, to perform functions authorized by law.

---

695 45 C.F.R. § 164.512(f)(1)(ii).
696 45 C.F.R. § 164.512(f)(2)(i)(A)-(H). Some PHI, instead, are specifically excluded, unless they fall within the (A) to (H) list (e.g., DNA analysis). 45 C.F.R. § 164.512(f)(2)(ii).
697 45 C.F.R. § 164.512(f)(2).
698 45 C.F.R. § 164.512(f)(3).
699 45 C.F.R. § 164.512(f)(3)(i).
700 45 C.F.R. § 164.512(f)(3)(ii)(A).
701 45 C.F.R. § 164.512(f)(3)(ii)(B).
702 45 C.F.R. § 164.512(f)(3)(ii)(C).
703 45 C.F.R. § 164.512(f)(4).
704 45 C.F.R. § 164.512(f)(5).
705 45 C.F.R. § 164.512(f)(6)(i). However, if the covered health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the relevant provision (45 C.F.R. § 164.512(c)) applies. 45 C.F.R. § 164.512(f)(6)(ii).
706 GOSTIN & HODGE, *supra* note 419, at 1474. *See* SWIRE & STEINFELD, *supra* note 648, at 1529 (describing some situations in which health information might be important to national security).
707 *Id.* at 1474-75.
708 SWIRE & STEINFELD, *supra* note 648, at 1530.
709 GOSTIN & HODGE, *supra* note 419, at 1475. *See also* SWIRE & STEINFELD, *supra* note 648, at 1532.
710 45 C.F.R. § 164.512(g).

h) Cadaveric organ, eye, or tissue donation[711]:

Covered entities are allowed to use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, or tissues.

i) Research purposes[712]:

First of all, it is important to underline that human subject research, when it is federally funded, is mostly subject to the so-called Common Rule[713], but the HIPAA Privacy Rule applies more detailed privacy requirements than those existing under the Common Rule[714].

In the HIPAA framework, research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge"[715]. It is important to distinguish research activities from the set of activities called "health care operations", in that the former require the patient's authorization, whereas the latter are not subject to this kind of restriction[716]. As the rule shows, the distinction is based on "whether the activity is designed to develop or contribute to generalizable knowledge": if so, then it is considered to be research[717]. Research activities are subject to stricter requirements because according to DHHS individuals expect that their information will be used for health care operations but not for research[718].

The research provisions usually apply in two different situations: (1) when a covered health care provider discloses information to a researcher who has requested it; or (2) when a researcher who is a covered entity wishes to use protected health information to carry out research[719]. The Privacy Rule, though, applies to both uses and disclosures[720].

Generally, the individual's authorization is needed for the use or disclosure of health data for research, but the Privacy Rule carves out three exceptions to this general rule[721]. In addition, limited data sets are also permissibly disclosed for research purposes without an authorization if some requirements are met, and it is important to remember that de-identified data can always be freely used and disclosed[722].

---

711 45 C.F.R. § 164.512(h).

712 45 C.F.R. § 164.512(i).

713 Federal Policy for the Protection of Human Subjects, 45 C.F.R. § 46. GOSTIN & HODGE, *supra* note 419, at 1472.

714 GOSTIN & HODGE, *supra* note 419, at 1472 (pointing out that the Common Rule only conditions Institutional Review Board approval of government-sponsored research on the existence of "adequate provisions to protect the privacy of subjects").

715 45 C.F.R. § 164.501.

716 TOVINO, *supra* note 519, at 454.

717 *Id.* Instead, "if the activity relates to conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines and the primary purpose of any studies resulting from such activities is not obtaining generalizable knowledge, then the activity constitutes a health care operation". *Id.*

718 *Id.* at 455 (citing Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,625).

719 *Id.* at 451-52.

720 *Id.* at 453. This represents a difference between HIPAA and many state laws, which tend to regulate disclosures of information to third parties but not internal uses of such information. *Id. See, e.g.*, Texas Hospital Licensing Law (Tex. Health & Safety Code Ann. § 241.152(a)), Texas Medical Practice Act (Tex. Occ. Code Ann. § 159.002(a)-(b)).

721 45 C.F.R. § 164.512(i)(1).

722 TOVINO, *supra* note 519, at 455-56. *See* Chapter III.

The first exception occurs if the covered entity obtains documentation that an alteration or waiver of individuals' authorization for the use or disclosure of PHI about them has been approved by an Institutional Review Board (IRB)[723] or Privacy Board[724]. The documentation must:

- identify the IRB or privacy board, and specify the date of the approval of the alteration or waiver of authorization[725];
- include a statement that such IRB or privacy board has determined that certain criteria (analyzed below) are satisfied[726];
- briefly describe the protected health information for which use or access has been determined to be necessary[727];
- include a statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures[728];
- be signed by the chair or other designated member of the IRB or privacy board[729].

The first waiver criterion regards a determination that the use or disclosure only involves a "minimal risk to the privacy of individuals"[730], based on at least "[a]n adequate plan to protect the identifiers from improper use and disclosure"[731]and "to destroy the identifiers at the earliest opportunity consistent with conduct of the research" (unless retention is appropriate in light of a health or research justification or required by law)[732], and "[a]dequate written assurances that the [PHI] will not be reused or disclosed to any other person or entity"[733]. These criteria are arguably "problematic", as the category of individual privacy rights is "undefined and disturbingly ambiguous" and the rule does not specify what is "minimal" risk, asking reviewers "to assess whether the […] risks […] outweigh the anticipated benefits of the research"[734].

The second criterion requires IRBs or privacy boards to determine that "[t]he research could not practicably be conducted without the waiver or alteration[735]. The Department of HHS has provided an interpretation of this provision, which highlights that "[i]f research could practicably be conducted with authorization, then authorization must be sought"[736]. Many entities do not seem to be aware that "[a]uthorization may not be

---

[723] 45 C.F.R. § 164.512(i)(1)(i)(A).

[724] 45 C.F.R. § 164.512(i)(1)(i)(B). Such Privacy Board must meet a number of requirements. First, it must "[have] members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests". 45 C.F.R. § 164.512(i)(1)(i)(B)(1). Secondly, it must "[include] at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities. 45 C.F.R. § 164.512(i)(1)(i)(B)(2). Third, it must "not have any member participating in a review of any project in which the member has a conflict of interest" 45 C.F.R. § 164.512(i)(1)(i)(B)(3).

[725] 45 C.F.R. § 164.512(i)(2)(i).

[726] 45 C.F.R. § 164.512(i)(2)(ii).

[727] 45 C.F.R. § 164.512(i)(2)(iii).

[728] 45 C.F.R. § 164.512(i)(2)(iv).

[729] 45 C.F.R. § 164.512(i)(2)(v).

[730] 45 C.F.R. § 164.512(i)(2)(ii)(A).

[731] 45 C.F.R. § 164.512(i)(2)(ii)(A)(1).

[732] 45 C.F.R. § 164.512(i)(2)(ii)(A)(2).

[733] 45 C.F.R. § 164.512(i)(2)(ii)(A)(3). Reuse or disclosure to third parties is only allowed "as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart". *Id.*

[734] *See* J. KULYNYCH & D. KORN, *Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule*, 28 *Am. J. L. & Med* 309, 320 (2002).

[735] 45 C.F.R. § 164.512(i)(2)(ii)(B).

[736] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,693.

waived simply for convenience"[737] and routinely request IRB approval in clinical trials[738], which do not meet the criterion because "hav[ing] direct contact with research subjects […] should in virtually all cases [enable them] to seek and obtain […] authorization"[739].

The third criterion is met if the IRB or privacy board determines that "[t]he research could not practicably be conducted without access to and use of the [PHI]"[740]. Therefore, as explained by HHS, if de-identified information can practicably be used for the study, PHI should not be used without authorization[741].

Some commenters maintained that IRBs and privacy boards should not be allowed to waive an individual's right to control uses and disclosures of PHI for research[742], but the Department believed that the safeguards required by the rule represent "the appropriate balance between protecting individuals' privacy interests, while permitting researchers to access protected health information for important, and potentially lifesaving, studies"[743]. Accordingly, this provision has been defined as "a workable framework for protecting individual privacy while also facilitating research", as the requirements "do not significantly thwart health research" while also taking into account individual rights[744]. Nevertheless, a major problem must be pointed out: very often IRBs and privacy boards do not have enough time, information, or skills to carry out the tasks they are entrusted with under these provisions[745], especially considering their potential lack of independence[746].

The second exception to the authorization requirement involves obtaining representations from the researcher that the use or disclosure of the information is only meant for a purpose preparatory to research, such as a research protocol, that the researcher will not remove any PHI from the covered entity, and that the information is necessary for the research[747]. The covered entity may allow the researcher to make such representations in written or oral form[748].

Thirdly, the covered entity can choose to obtain representations from the researcher that the use or disclosure sought is only for research on PHI of decedents which is necessary for the research[749]. In this instance, the covered entity can request documentation of the death of the individual[750]. This is modeled after the Common Rule, which does not include deceased persons within the concept of human subjects[751]. This is not undisputed, however, as, for example the American Medical Association's Code of Ethics provides that "[d]isclosure of medical information postmortem for research and educational purposes is

---

737 *Id.*
738 TOVINO, *supra* note 519, at 485-86.
739 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,693.
740 45 C.F.R. § 164.512(i)(2)(ii)(C).
741 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,698.
742 TOVINO, *supra* note 519, at 483.
743 Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,131.
744 GOSTIN & HODGE, *supra* note 419, at 1473-74.
745 TOVINO, *supra* note 519, at 486. For a deep and insightful analysis of this issue and some proposals, see id. at 486-496.
746 HATCH, *supra* note 432, at 1484 ("Because IRBs are established by research-oriented facilities, the likelihood of patient advocacy is minimal"). See 45 C.F.R. § 690.107 (listing features that IRBs must possess).
747 45 C.F.R. § 164.512(i)(1)(ii). *See also* TOVINO, *supra* note 519, at 497-98.
748 TOVINO, *supra* note 519, at 459 (citing Dep't of Health & Human Servs., Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule 17, NIH Pub. No. 03-5388 (2003)).
749 45 C.F.R. § 164.512(i)(1)(iii).
750 *Id.*
751 TOVINO, *supra* note 519, at 459 (citing Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,701 (Dec. 28, 2000)).

appropriate as long as confidentiality is maintained to the greatest possible degree by removing any individual identifiers"[752].

j) Serious threat to health or safety[753]:

Pursuant to this provision, a covered entity may use or disclose PHI if it in good faith believes it is either "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public"[754] or "for law enforcement authorities to identify or apprehend an individual"[755].

In the first instance, disclosure must be to someone who is "reasonably able to prevent or lessen the threat"[756]. The second prong of this provision refers to when there is "a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim", or "[w]here it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody"[757]. If a patient merely attempts to have the medical provider hide his identity, it does not qualify as such a statement, but, of course, if a patient confesses to participating in the act (e.g., in a terrorist attack), it does qualify, and it allows the entity to report to law enforcement[758]. This exception, however, does not apply if the information is acquired by the covered entity "[i]n the course of treatment to affect the propensity to commit the criminal conduct" or due to a request by the individual to start such treatment[759].

k) Specialized government functions[760]:

This exception refers to a number of government functions in relation to which a covered entity may use or disclose PHI without authorization. For example, this may be allowed with respect to military and veterans activities[761], or to the provision of protective services to the President or others[762]. Also, a covered entity that belongs to the Department of State may use PHI to make medical suitability determinations and disclose their outcomes to the officials[763]. Another reason falling within this exception concerns the disclosure of PHI to correctional institutions or law enforcement officials having lawful custody of the individual to whom the health data refers, in order to protect his or others' health or safety, or to carry out law enforcement or administration activities[764]. Another permissible disclosure of PHI is from a covered entity that is a government program providing public benefits to another[765]. Finally, and most interestingly, this provision also contains an exception related to national security and intelligence activities, allowing the disclosure of PHI "to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National

---

[752] American Medical Association, Code of Ethics E-5.051. *See also* TOVINO, *supra* note 519, at 496-97.
[753] 45 C.F.R. § 164.512(j).
[754] 45 C.F.R. § 164.512(j)(1)(i)(A).
[755] 45 C.F.R. § 164.512(j)(1)(ii).
[756] 45 C.F.R. § 164.512(j)(1)(i)(B). This may include the target of the threat. *Id.*
[757] *Id. See also* SWIRE & STEINFELD, *supra* note 648, at 1530-31.
[758] SWIRE & STEINFELD, *supra* note 648, at 1531.
[759] 45 C.F.R. § 164.512(j)(2).
[760] 45 C.F.R. § 164.512(k).
[761] 45 C.F.R. § 164.512(k)(1).
[762] 45 C.F.R. § 164.512(k)(3).
[763] 45 C.F.R. § 164.512(k)(4).
[764] 45 C.F.R. § 164.512(k)(5).
[765] 45 C.F.R. § 164.512(k)(6).

Security Act"[766]. Remarkably, then, "national security information can be reported by medical professionals even without patient consent", so long as the disclosure is in good faith according to the general approach of the regulations[767].

l) Workers' compensation[768]:

Covered entities can disclose PHI "as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault"[769].

Pursuant to the regulations, a different scenario emerges concerning "limited data sets", i.e. PHI from which some listed identifiers of the individual or of relatives, employers, or household members have been removed[770]. The sole purposes for which a limited data set can be used or disclosed are "research, public health, or health care operations"[771]. A scholar has written that this option "appears to be a nice compromise between the stringent de-identification safe harbor and the authorization requirement", also considering that it minimizes patient concerns with respect to re-identification[772].

A covered entity may use or disclose limited data sets as long as it enters into a data use agreement with the recipient[773], providing "satisfactory assurance […] that [it] will only use or disclose the protected health information for limited purposes"[774]. Such agreement must specify the permitted uses and disclosures[775] – in addition to who the recipient is[776] – and provide that he will: not use or further disclose the data other than as permitted by the data use agreement or as otherwise required by law[777], use appropriate safeguards[778], report to the covered entity any unauthorized use or disclosure[779], ensure that its agents agree to the same restrictions and conditions[780], and not identify the information or contact the individuals[781].

In case the covered entity finds out about a material breach or violation of the data use agreement committed by the limited data set recipient, it needs to take reasonable steps to cure the breach or end the violation[782]. If such steps are not successful, the entity needs to discontinue disclosure of PHI to the recipient and report the problem to the Secretary of HHS[783].

---

766 45 C.F.R. § 164.512(k)(2).

767 SWIRE & STEINFELD, *supra* note 648, at 1530 (citing 45 C.F.R. § 164.512(j)(4)). Thus, "the drafters of the privacy rule had in fact contemplated possible national security implications before September 11". *Id.*

768 45 C.F.R. § 164.512(l).

769 *Id.*

770 45 C.F.R. § 164.514(e). The identifiers that need to be removed are listed at § 164.514(e)(2)(i)-(xvi). Some identifiers are allowed to remain, including years and information relating to the town or city, state, and zip code of the patient, of his or her employer and of his or her household members. TOVINO, *supra* note 519, at 457-58.

771 45 C.F.R. § 164.514(e)(3)(i).

772 TOVINO, *supra* note 519, at 499.

773 45 C.F.R. § 164.514(e)(1).

774 45 C.F.R. § 164.514(e)(4)(i).

775 45 C.F.R. § 164.514(e)(4)(ii)(A).

776 45 C.F.R. § 164.514(e)(4)(ii)(B).

777 45 C.F.R. § 164.514(e)(4)(ii)(C)(1).

778 45 C.F.R. § 164.514(e)(4)(ii)(C)(2).

779 45 C.F.R. § 164.514(e)(4)(ii)(C)(3).

780 45 C.F.R. § 164.514(e)(4)(ii)(C)(4).

781 45 C.F.R. § 164.514(e)(4)(ii)(C)(5).

782 45 C.F.R. § 164.514(e)(4)(iii)(A).

783 45 C.F.R. § 164.514(e)(4)(iii)(A)(1)-(2).

Furthermore, the regulations specify that "[i]f a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law"[784].

4.1.4.6 Prohibited Uses and Disclosures

The HIPAA Privacy Rule lists two situations in which use and disclosure of PHI is prohibited. The first one forbids health plans from using and disclosing genetic information for underwriting purposes[785]. Such purposes include rules for eligibility for benefits, coverage or policy[786], the computation of premium or contribution amounts[787], the application of any pre-existing condition exclusion[788], and any other "activit[y] related to the creation, renewal, or replacement of a contract of health insurance or health benefits"[789]. The rule further clarifies that this does not regard "determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy"[790]. The second forbidden activity is the sale of protected health information, when not authorized in compliance with § 164.508[791] (see paragraph 4.1.4.2).

4.1.5 Individual Rights

The HIPAA privacy regulations vest individuals with several rights, with the purpose of allowing them to "make informed choices about the delivery and financing of their health care"[792].

(a) Access

First of all, individuals have the right to access, inspect and obtain a copy of protected health information about him or herself[793].

The covered entity must act no later than thirty days after receipt of the request[794], and if access is provided it must be in the form and format requested by the individual or, if the individual agrees, it can be in the form of a summary or explanation of the requested information[795].

---

[784] 45 C.F.R. § 164.514(g). Such use or disclosure is "subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information". Id.

[785] 45 C.F.R. § 164.502(a)(5)(i). *See also* ROTHSTEIN, *supra* note 505, at 527.

[786] 45 C.F.R. § 164.502(a)(5)(i)(A)(1).

[787] 45 C.F.R. § 164.502(a)(5)(i)(A)(2).

[788] 45 C.F.R. § 164.502(a)(5)(i)(A)(3).

[789] 45 C.F.R. § 164.502(a)(5)(i)(A)(4).

[790] 45 C.F.R. § 164.502(a)(5)(i)(B).

[791] 45 C.F.R. § 164.502(a)(5)(ii).

[792] GOSTIN & HODGE, *supra* note 419, at 1462.

[793] 45 C.F.R. § 164.524(a)(1). This right refers to a "designated record set", which is: "a group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals". 45 C.F.R. § 164.501. This definition is meant to be "sufficiently flexible to work with the varying practices of covered entities". 65 Fed. Reg. at 82607.

[794] *Id.* § 164.524(b)(2)(i).

[795] *Id.* § 164.524(c)(2).

Exceptions to this right are carved out allowing the covered entity to deny access: some of these grounds for denial are subject to review and some are not. The "narrow, unreviewable reasons for denials"[796] are: psychotherapy notes[797], information likely to be used in a civil, criminal, or administrative proceeding[798], requests by inmates to correctional institutions that might jeopardize the health or safety of the requester or others[799], suspended access to information while it is being used for research to which the individual has previously consented[800], information subject to the Privacy Act[801], information obtained under a promise of confidentiality[802]. In other instances, access can be denied but the individual is allowed to request a review of the grounds for denial[803]. Such situations consist in the determination by a licensed health care professional, and in the exercise of professional judgment, that the access is reasonably likely to endanger the life or safety of the individual or another, or that it is reasonably likely to cause substantial harm to a person to which the information makes reference, or that providing access to the individual's personal representative, who has made request, would cause substantial harm to the individual or another[804].

(b) Amendment

The second right afforded to individuals is that of having the covered entity correct the individual's PHI[805], so that they "can ensure that information about them is as accurate as possible as it travels through the health care system and is used to make decisions […] about them"[806]. Action must be taken within sixty days (extendable for thirty more days)[807]. If the covered entity accepts the amendment it must make the amendment "by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment"[808], as well as inform the individual and other specific persons[809] that the amendment has been carried out. In some situations the amendment may be denied, e.g. if the record was not created by the covered entity, or if it is not accurate and complete[810]. The individual has the right to "submit a written statement"[811] but "there is no final review to clarify which party, the individual or the covered entity, is correct"[812].

(c) Notice of Privacy Practices

Covered entities must provide a notice of their privacy practices, because individuals have "a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered

---

796 GOSTIN & HODGE, *supra* note 419, at 1463; 45 C.F.R. § 164.524(a)(2).
797 45 C.F.R. § 164.524(a)(1)(i).
798 Id. § 164.524(a)(1)(ii).
799 Id. § 164.524(a)(2)(ii).
800 Id. § 164.524(a)(2)(iii).
801 Id. § 164.524(a)(2)(iv).
802 Id. § 164.524(a)(2)(v).
803 Id. § 164.524(a)(3).
804 Id. § 164.524(a)(3)(i)-(iii).
805 Id. § 164.526.
806 65 Fed. Reg. 82736.
807 Id. § 164.526(b)(2).
808 Id. § 164.526(c)(1).
809 Id. § 164.526(c)(2)-(3).
810 Id. § 164.526(a)(2).
811 Id. § 164.524(d)(1)(ii).
812 GOSTIN & HODGE, *supra* note 419, at 1464.

entity's legal duties with respect to protected health information"[813]. Such notice must also include information on how to complain about misuses or violations to the entity or to the Secretary of HHS, as well as how to contact the covered entity[814]. Notices must be in plain language[815], and they must be given within different deadlines depending on the type of covered entity[816]. Despite the "plain language" requirement, most notices are either too long or too complicated, so "that patients likely would have difficulty shopping for a health care provider based on whether the […] notice states that the provider will use a patient's PHI for research activities without authorization"[817].

Furthermore, health care providers must "[p]rovide the notice […] [n]o later than the date of first service delivery […] to [patients] after the compliance date"[818] and must make a good faith attempt to get each patient's written acknowledgment of receipt[819]. Unfortunately, covered providers often put a lot of effort into obtaining such acknowledgments without carrying out equally strong attempts to notify patients of their privacy practices[820]. Also, many patients receive such notices right before receiving treatment and are unwilling to switch to a more privacy-protective provider[821].

(d) Request an Accounting of Disclosures

Another right individuals are afforded by the HIPAA regulations is the right to receive an accounting of disclosures of protected health information made by a covered entity or its business associates[822]. The maximum period is the six years prior to the date on which the accounting is requested[823].

Unfortunately, this requirement is subject to so many exceptions that they "almost swallow the rule"[824], as covered entities do not have to include:

- disclosures to carry out treatment, payment, or health care operations;
- disclosures to individuals of PHI about them;
- disclosures for the covered entity's facility directory or to persons involved in the individual's care or other notification purposes;
- disclosures for national security or intelligence purposes;
- disclosures to correctional institutions or law enforcement officials;
- disclosures that occurred prior to the compliance date for the covered entity;
- disclosures authorized by the individual pursuant to an authorization form that meets all the requirements;
- disclosures that are incidental to a permitted use or disclosure;
- disclosures of a limited data set pursuant to a data use agreement[825].

---

[813] 45 C.F.R. § 164.520(a)(1). This provision has some exceptions, e.g. inmates do not have a right to notice. 45 C.F.R. § 164.520(a)(3).
[814] Id. § 164.520(b)(1)(vi).
[815] Id. § 164.520(b)(1).
[816] Id. § 164.520(c)(1)-(2).
[817] TOVINO, *supra* note 519, at 476.
[818] 45 C.F.R. § 164.520(c)(2)(i).
[819] 45 C.F.R. § 164.520(c)(2)(ii) (except in emergency situations).
[820] TOVINO, *supra* note 519, at 477.
[821] *Id.* at 478.
[822] 45 C.F.R. § 164.528(a)(1).
[823] Id.
[824] TOVINO, *supra* note 519, at 479.
[825] 45 C.F.R. § 164.528(a)(1). Therefore, looking at uses or disclosures for research purposes, if they are made pursuant to an authorization form or are of a limited data set and pursuant to a data use agreement, they need not be listed in the accounting, whereas the uses or disclosures which must be tracked are those preparatory

The accounting includes the name of the person or entity who received the information, the date of the disclosure, a brief description of the information disclosed, and an explanation of the reasons for disclosure if not authorized by the patient[826].

Theoretically, patients will then be able to identify who has received their information and determine whether the covered entity is wrongfully disclosing PHI[827]. However, there are several elements that undermine this goal. First, there is a simplified accounting process for disclosures for research purposes involving PHI relating to fifty or more individuals[828]. Secondly, patients are often unaware of their right to receive an accounting because they can only be informed through the notice of privacy practices and there are often communication problems[829]. Thirdly, it is very complex and burdensome for covered entities to produce an accounting that actually respects the Privacy Rule requirements, insofar as, for instance, tracking not only electronic but also physical disclosures is often difficult[830]. This provision has been "pointed to […] as the most onerous requirement set forth in the Privacy Rule"[831].

(e) Request Additional Privacy Protections

This right is composed of two different rights. Individuals have, first, the right to request covered entities to restrict uses or disclosures of PHI, and secondly, to request them to provide confidential communications of PHI.

Whenever an individual requests that a covered entity restrict the disclosure of the PHI, the entity is not required to agree to such restrictions, except for when "the disclosure is to a health plan for purposes of carrying out payment or health care operations" and "the [PHI] pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full"[832].

As to the second prong of this right, covered health care providers "must accommodate reasonable requests by individuals to receive communications of [PHI] […] by alternative means or at alternative locations"[833], and they cannot require an explanation from the individual as a condition for accommodating the request[834]. Health plans, instead, are only required to accommodate requests "if the individual clearly states that the disclosure […] could endanger [him or her]"[835].

4.1.6 The Administrative Requirements

Covered entities need to implement policies and procedures with respect to PHI in order to comply with the requirements of the HIPAA Privacy Rule. Such policies and

---

for research, or on decedents' information, or based on an IRB or privacy board waiver. TOVINO, *supra* note 519, at 479.

826 45 C.F.R. § 164.528(b)(2).

827 TOVINO, *supra* note 519, at 479-80.

828 45 C.F.R. § 164.520(b)(1)(i). *See* TOVINO, *supra* note 519, at 480.

829 TOVINO, *supra* note 519, at 480-81.

830 *Id.* at 481.

831 *Id.* at 481-82 (citing M. L. DURHAM, *How Research Will Adapt to HIPAA: A View From Within the Healthcare Delivery System*, 28 *Am. J. L. & Med.* 491, 497 (2002)).

832 42 U.S.C. § 17935(a)(1)-(2); 45 C.F.R. § 164.522 (a)(1)(vi).

833 45 C.F.R. § 164.522(b)(1)(i).

834 45 C.F.R. § 164.522(b)(2)(iii).

835 45 C.F.R. § 164.522(b)(1)(ii).

procedures must be reasonably designed, taking into account the size and type of activities that involve PHI[836].

First, in order to efficiently develop and implement such policies and procedures, a covered entity needs to designate a privacy official[837]. Also, a contact person or office must be designated who is responsible for receiving complaints and providing further information on the privacy practices[838]. These two roles may, but do not have to be, covered by the same person. Also, this function can permissibly be combined with other duties[839].

Secondly, a covered entity has a duty to train all the members of its workforce on its enumerated policies and procedures, as necessary and appropriate for them to carry out their tasks[840]. Non-employed contractors who perform "a substantial proportion of their activities" on the covered entity's premises may be, if the entity so chooses, treated as business associates or as part of the workforce[841]. This training must be carried out in a timely fashion and needs to be documented[842]. The content and type of the training can be determined by the entity so that it is "the most effective means of communicating with their workforce"[843]. In some instances it may be sufficient to provide each employee with a copy of the practice's information policies, whereas sometimes the entity needs to set up a more structured program, depending on the size of the workforce and on the economical feasibility[844]. A covered entity must also apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies[845]. The type of sanction, which can also be represented by termination, depends on many factors, including the severity of the violation, its intentionality, and whether it indicates a pattern of improper use or disclosure of PHI[846].

Third, entities need to have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI from any intentional or unintentional use or disclosure that violates the Privacy Rule, as well as to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure[847]. This, too, is meant to be a flexible, "common sense, scalable, standard": covered entities are not required "to guarantee the safety of [PHI] against all assaults", but only need to take the appropriate measures depending on the size of the entity and the type of its activities, also looking at the existing bodies of recommended practices[848].

Fourth, covered entities must set up a process to allow individuals to make complaints about their policies and procedures, and their compliance with them[849]. All

---

836 45 C.F.R. § 164.530(i). Also, such policies and procedures must be documented and maintained in written or electronic form for six years. 45 C.F.R. § 164.530(j).
837 45 C.F.R. § 164.530(a).
838 *Id.*
839 65 Fed. Reg. at 82744.
840 45 C.F.R. §164.530(b). "Workforce" is defined as including "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate". 45 C.F.R. § 160.103.
841 65 Fed. Reg. at 82480.
842 45 C.F.R. § 164.530(b)(2).
843 64 Fed. Reg. at 59989.
844 *See id.*
845 45 C.F.R. § 164.530(e).
846 64 Fed. Reg. at 59991.
847 45 C.F.R. § 164.530(c).
848 65 Fed. Reg. at 82562.
849 45 C.F.R. § 164.530(d).

complaints must be documented[850]. Because individuals can also take their complaints to the Secretary of HHS, covered entities have an incentive to implement a favorable complaint process for individuals[851].

Furthermore, covered entities have a duty to mitigate harmful effects of improper use or disclosure of PHI carried out by members of their workforce or by their business associates[852]. This duty is only triggered when the harmful effect is "known" to the covered entity, and only "to the extent practicable"[853].

The rules also impose duties on covered entities that are meant to protect the chance for individuals to exercise the rights they are provided with. Thus, covered entities need to refrain from intimidating or retaliatory acts against individuals for the exercise of their rights under the Privacy Rule or for filing a complaint with the Secretary, or for participating in an investigation or compliance review, or otherwise opposing unlawful practices[854]. Also, "[a] covered entity may not require individuals to waive their [right to file a complaint with the Secretary] as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits"[855].

4.2 The HIPAA Security Rule

The HIPAA Security Rule only applies to information held in electronic form and is particularly relevant in that it "introduced industry-standard information technology security practices to the health care field"[856]. The specific protections mandated by the Security Rule include administrative, physical, technical, and organizational safeguards.

First of all, the Security Rule mandates some administrative safeguards[857]. Covered entities and business associates need to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations", by assessing the potential risks, implementing measures aimed at reducing those risks, applying sanctions against workforce members who are not complying with the policies, and implementing procedures to review records of information system activity[858]. Furthermore, a security official must be identified who is responsible for developing and implementing such procedures[859]. The members of the entity's workforce must be given appropriate access to electronic PHI via the implementation of a workforce clearance procedure,[860] and must be included in security awareness and training programs[861]. Security incidents and other emergencies must be dealt with in a timely and careful manner through the implementation of procedures to maintain retrievable copies of electronic PHI and restore losses of data[862].

Secondly, covered entities must have in place physical safeguards, in order "to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed"[863]. Similar to

---

850 *Id.*
851 65 Fed. Reg. at 82747.
852 45 C.F.R. § 164.530(f); 65 Fed. Reg. at 82562-63.
853 65 Fed. Reg. at 82748.
854 45 C.F.R. § 164.530(g).
855 45 C.F.R. § 164.530(h); 45 C.F.R. § 160.306.
856 WU, *supra* note 409, at xi.
857 45 C.F.R. § 164.308.
858 45 C.F.R. § 164.308(a)(1).
859 45 C.F.R. § 164.308(a)(2).
860 45 C.F.R. § 164.308(a)(3).
861 45 C.F.R. § 164.308(a)(5).
862 45 C.F.R. § 164.308(a)(6)-(7).
863 45 C.F.R. § 164.310(a)(1).

what is required from the administrative side, there must be procedures to restore data in case of disasters and emergencies[864], as well as policies to safeguard the facilities from unauthorized physical access, tampering, and theft[865].

Third, technical safeguards must be implemented for the purposes of allowing access only to persons or software programs that have been granted access rights, of examining activities involving electronic PHI, of protecting information from improper alteration or destruction, and verifying person or entity authentication[866].

Finally, covered entities must comply with some organizational requirements regarding contracts with business associates[867] and the disclosure of electronic PHI by a group health plan to the plan sponsor[868]. In both cases, the aim is ensuring that the business associate and the plan sponsor implement appropriate safeguards.

4.3 Breach Notification Requirements

A "breach" occurs whenever PHI is acquired, accessed, used, or disclosed, in a manner not permitted under the rules and which compromises the security or privacy of the information[869]. In order for an event to constitute a breach, it must be intentional: if the acquisition, access, or use is carried out by a workforce member or person acting under the authority of a covered entity or of a business associate, and it is unintentional and in good faith, it is excluded from the definition of breach[870]. Similarly, the definition also does not include inadvertent disclosures by an authorized person to another when the information is not further used or disclosed in a forbidden manner[871].

Whenever an event falls within the definition, it is presumed to be a breach unless the covered entity or business associate is able to demonstrate that there is a "low probability that the protected health information has been compromised" [872]. Such demonstration must be "based on a risk assessment" of several factors, which must include at a minimum: the nature and extent of the PHI involved[873], the unauthorized person who used the PHI or to whom it was disclosed[874], whether the PHI was actually acquired or viewed[875], and the extent to which the risk to the PHI has been mitigated[876].

Different kinds of duties are imposed on covered entities and business associates depending on the size of the breach and other factors. In the event of an unauthorized use or disclosure, the burden of proof is borne by the covered entity or business associate, who needs to demonstrate that all notifications were made as required or that no breach occurred[877].

---

[864] 45 C.F.R. § 164.310(a)(2)(i).
[865] 45 C.F.R. § 164.310(a)(2)(ii).
[866] 45 C.F.R. § 164.312.
[867] 45 C.F.R. § 164.314(a).
[868] 45 C.F.R. § 164.314(b).
[869] 45 C.F.R. § 164.402 (definition of "Breach").
[870] 45 C.F.R. § 164.402 (definition of "Breach", subsection (1)(i)).
[871] 45 C.F.R. § 164.402 (definition of "Breach", subsection (1)(ii)).
[872] 45 C.F.R. § 164.402 (definition of "Breach", subsection (2)).
[873] 45 C.F.R. § 164.402 (definition of "Breach", subsection (2)(i)). This includes "the types of identifiers and the likelihood of re-identification, see Chapter III).
[874] 45 C.F.R. § 164.402 (definition of "Breach", subsection (2)(ii)).
[875] 45 C.F.R. § 164.402 (definition of "Breach", subsection (2)(iii)).
[876] 45 C.F.R. § 164.402 (definition of "Breach", subsection (2)(iv)).
[877] 45 C.F.R. § 164.414.

After discovering a breach of unsecured protected health information[878], a covered entity shall "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach"[879]. This notification must occur "without unreasonable delay and in no case later than 60 calendar days after" the discovery[880], but a delay is allowed "[i]f a law enforcement official states that the notification would impede a criminal investigation or cause damage to national security"[881]. The notification must be written in plain language[882], and it shall describe what happened and what kind of unsecured PHI was involved, as well as the measures that the individuals should take and that the entity is already taking to mitigate the harm[883]. The method of notification that the rule encourages is a written notification (either by first class-mail or electronic mail, if it has been agreed to)[884]. Only in instances where the contact information is insufficient or out-of-date and written notification is impossible, does the covered entity need to provide "a substitute form of notice reasonably calculated to reach the individual"[885]. In urgent situations where there is "possible imminent misuse of unsecured protected health information", the notification may be additionally provided by telephone or other appropriate means[886].

If the breach involves more than 500 residents of a State or jurisdiction, the covered entity also needs to notify the media, "without unreasonable delay and in no case later than 60 days after discovery of a breach"[887].

Furthermore, breach notification must also be provided to the Secretary of HHS[888]. If 500 or more individuals are involved, this must happen at the same time as the notification to the individual, otherwise it is enough to send a yearly report of all breaches discovered during the preceding calendar year[889]. Indeed, if the breach involves the PHI of 500 individuals or more, it is included in the so-called Wall of Shame, i.e., a report kept by the Office of Civil Rights within the HHS[890]. According to a recent report, "low-tech breaches [are] the most common form of data loss in the health sector – surpassing the more publicized hacking events"[891]

Business associates who discover a breach must notify the covered entity, including the identification of each individual whose information has been, or is reasonably believed

---

878 "Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5". 45 C.F.R. § 164.402 (definition of "Unsecured protected health information"). Furthermore, a breach is treated as discovered "as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity". 45 C.F.R. § 164.404(a)(2).

879 45 C.F.R. § 164.404(a)(1).

880 45 C.F.R. § 164.404(b).

881 45 C.F.R. § 164.412.

882 45 C.F.R. § 164.404(c)(2).

883 45 C.F.R. § 164.404(c)(1).

884 45 C.F.R. § 164.404(d)(1).

885 45 C.F.R. § 164.404(d)(2).

886 45 C.F.R. § 164.404(d)(3).

887 45 C.F.R. § 164.406.

888 45 C.F.R. § 164.408(a).

889 45 C.F.R. § 164.408(b)-(c).

890 U.S. Dep't Health & Hum. Services, Health Information Privacy: Breaches Affecting 500 or More Individuals, available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

891 Bryan Cave LLP Global Data Privacy and Security Team, *The Causes of Healthcare Breaches At A Glance* (2015), available at: http://bryancavedatamatters.com/the-causes-of-healthcare-breaches-at-a-glance/.

by the business associate to have been, accessed, acquired used or disclosed, and provide any other available information relevant to the breach[892].

4.4 Enforcement and Penalties

Some scholars have heavily criticized the HIPAA enforcement regime as "the overbroad law and threat of sanctions spawned an inevitably overbroad regulatory privacy regime and effectively convinced patients and providers that the act of sharing PHI is morally problematic"[893]. At the same time, Terry noted that "[t]he federal standards […] do not provide an aggrieved patient with enforcement through a private right of action", but "rather they provide for a compliance mechanism with regulatory agency oversight and the potential for civil or criminal penalties"[894]. In his view, "[t]he message is that any privacy-confidentiality "rights" belong to the healthcare system and not to patients"[895].

The Privacy Rule is enforced both through civil and criminal penalties. The Office of Civil Rights (OCR), which is a division of HHS, handles complaints, performs audits of covered entities, engages in activities to encourage compliance, and imposes civil penalties[896]. Civil enforcement is also carried out through a state attorney general who has reason to believe that one or more of the residents of the State have been adversely affected by a violation of the rule[897]. The rules, however, emphasize the importance of using self-regulatory means to ensure compliance, which include "demonstrated compliance, or a completed corrective action plan or other agreement"[898].

A number of factors are considered in determining the amount of the penalty, including the nature and extent of the violation, the nature and extent of the harm, the history of prior compliance, and the financial condition of the entity[899].

Civil penalties can only be applied as long as no one of the following criteria is met. First, if there is an overlap of jurisdiction with the Department of Justice (which prosecutes criminal violations) criminal enforcement prevails[900]. Secondly, penalties may be waived if the person or entity "did not know, and by exercising reasonable diligence would not have known" that a violation had been committed[901]. Third, the HHS Secretary can also excuse the violation if "the failure to comply was due to reasonable cause and not to willful neglect, and the failure to comply is corrected"[902]. Furthermore, regardless of these three criteria, the Secretary may waive the penalty to the extent that it would be excessive relative to the compliance failure involved[903].

---

892 45 C.F.R. § 164.410.
893 WILKES, *supra* note 425, at 1223.
894 TERRY, *supra* note 414, at 13.
895 *Id.*
896 45 C.F.R. § 160.404; G. FLEMING, *HIPAA-Cratic or HIPAA-Critical: U.S. Privacy Protections Should Be Guaranteed By Covered Entities Working Abroad*, 98 *Minnesota Law Review* 2375, 2380 (2014). *See* Bryan Cave LLP Global Data Privacy and Security Team, *Healthcare Data Breach Enforcements and Fines At A Glance* (2015), available at: http://bryancavedatamatters.com/healthcare-data-breach-enforcements-and-fines-at-a-glance/.
897 *See* Bryan Cave LLP Global Data Privacy and Security Team, *Healthcare Data Breach State-Level Enforcements and Fines At A Glance* (2015), available at: http://www.bryancavedatamatters.com/state-level-enforcement-and-fines-for-health-data-breaches-at-a-glance/ (noticing that few attorney generals so far have brought actions to enforce HIPAA on behalf of their state citizens).
898 45 C.F.R. § 160.312(a)(1). *See* SOMA ET AL., *supra* note 411, p. 122.
899 45 C.F.R. § 160.408.
900 45 C.F.R. § 160.410(a).
901 45 C.F.R. § 160.410(b).
902 45 C.F.R. § 160.410(c).
903 45 C.F.R. § 160.412.

In 2009, the OCR started keeping a record of PHI breaches affecting 500 people or more, creating the so-called "Wall of Shame"[904]. As much as this was meant to incentivize covered entities to focus on PHI confidentiality, some have noted that the outcome has merely been to motivate companies toward compliance interest and avoiding fees rather than the attempt to protect patient data[905].

As to criminal violations, they can result in a fine of up to $50,000 and/or imprisonment (maximum one year). In case the crime is committed using false pretenses, the fine can increase to $100,000 and/or maximum five years in prison. If the crime is committed for personal gain, or to inflict malicious harm, the penalty amounts to up to $250,000 or imprisonment for up to ten years, or both[906].

4.5 Application of HIPAA Abroad: an Open Issue

A very important yet unresolved issue concerns whether HIPAA requirements apply to U.S.-based institutions when they are engaged in international clinical trials[907]. We have seen that HIPAA recognizes privacy as a fundamental right but "it is still unclear whether this right must be recognized by U.S. organizations when they work outside of the country"[908]. However, some clues are arguably provided by HIPAA's text: first, it only excludes foreign nationals who receive health care from the Department of Defense or from another federal agency, and secondly, it tends to focus on whether the entity is covered or on whether the information falls within the definition of PHI rather than on the nationality of research participants[909]. Therefore, it looks like the requirements apply to all identifiable health information that is handled by a covered entity, which would include researchers abroad[910]. Furthermore, "[e]xpanding HIPAA to cover international research would achieve [the] goal" of "guaranteeing protection of private information in research in all cases"[911]. Hence, it would be desirable for the HHS to issue guidance documents establishing the applicability of HIPAA to covered entities engaged in international researching[912].

5. Comparative Conclusions

Health data protection throughout the world features a degree of complexity and of technicality that makes it seem impossible to spot any sort of pattern or to conduct a comprehensive analysis. Nevertheless, a more careful glance can lead to insightful reflections on the way health data protection is pursued on either side of the Atlantic Ocean.

Interestingly, the protection of individual rights was not the leading concern that brought on the implementation of the EU Directive and HIPAA. As it has often happened in the history of European Union law (we can think, for instance, of the right to work as related to the freedom of movement and establishment), the safeguard of human rights has

---

904 U.S. Dep't Health & Hum. Services, *supra* note 890.
905 WILKES, *supra* note 425, at 1231.
906 42 U.S.C. § 1320d-6(b). *See* SOMA ET AL., *supra* note 411, at 121.
907 FLEMING, *supra* note 896, at 2377.
908 *Id.* at 2378.
909 *Id.* at 2381-82.
910 *Id.* at 2382.
911 *Id.* at 2405 (highlighting that "[p]rivacy may be more difficult to achieve, but there remains a moral imperative to enforce privacy in health as a basic human right").
912 *Id.* at 2406-07.

long been an ancillary goal when compared to the implementation of a free internal market, which was the initial dream of the drafters of the Directive. The attempt to achieve greater harmonization also plays a crucial role in the reform process leading to the General Data Protection Regulation. Similarly, the trigger for the adoption of the Health Insurance Portability and Accountability Act in the United States was in allowing employees to easily change employers while retaining health insurance coverage. Easier and smoother transactions seem to have been the main underlying goal. Data were mostly seen in light of their flow rather than of their connection with each and every individual. Yet, both scenarios have been defined by an ever-growing importance of the protection of individual rights, be it through the explicit recognition of a fundamental right to data protection, or through the concrete application of the rules. The fact that the individual was not at the center of the lawmaking process in the field of health data protection, however, can shed light on some of the shortcomings and gaps of the legislation. It is all the more unsettling if we consider that health data deal with human weaknesses, a realm that we all struggle to accept and that we would not want others to enter.

The European Union and the United States are two multi-level systems that feature extremely different approaches to data protection, especially with respect to legislative technique. The European Union goes in the direction of greater harmonization by implementing one act for the whole data protection field (Directive 95/46/EC and the upcoming Regulation). Conversely, federal US data protection law adopted a piecemeal approach, as different acts apply depending on the type of record, and only establishes a minimum level of protection, thereby allowing states to keep more stringent requirements. Despite these patent differences, it is possible to detect some trajectories that both systems follow in order to grant protection to health data, as well as some common general principles. For instance, the HIPAA minimum disclosure rule closely resembles the European proportionality principle[913].

Defining personal data and health data is an endeavor that all data protection legal frameworks engage in. Medical data are defined as data that have a link with the individual's health status. This link does not need to be very strong. The recognition of health as a comprehensive status – which does not just have to do with present illnesses but also with psychological situations, genetic data, and in general with the present, past and future wellbeing of the person – has led to considering even potential links sufficient to trigger health data protection.

The importance of protecting health data is highlighted both in the EU Directive and in HIPAA by establishing a general ban on its processing, followed by exceptions. This does not amount to much more than an expressive mode (which the Italian law does not employ), as the exceptions are fairly broad, but it conveys the importance of surrounding this type of data with strict rules. The data subject's consent represents the first instance in which processing of data is allowed, but it is also a tricky one. As much as the laws around the globe attempt to make this consent a free and thoroughly informed one, in the field of health data individuals inherently experience a power imbalance, which impairs their ability to make decisions. Is it possible to have rules on the provision of consent and authorization that take into account all the different implications of the processing of health data, and that at the same time allow companies to transfer data and researchers to contribute to the public good? This is the struggle that legislators on both sides of the Ocean are engaged in. Very often, though, consent is reduced to complex forms and burdensome formal requirements, and both data subjects and data controllers are

[913] DUMORTIER & VERHENNEMAN, *supra* note 125, at 34.

ultimately deprived of the understanding of what is at stake. The Directive seems to be aware of this risk by entrusting Member States with envisioning cases in which not even consent is able to lift the ban.

Without the individual's consent, the processing of health data is permitted in a number of different cases. The United States legislation carves out many, very specific (e.g., face-to-face marketing communications) and extremely broad exceptions, so as to not look like exceptions after all, whereas the European legislation looks more cautious. For example, the Italian Data Protection Code requires the data subject's consent even for the processing of data for therapeutic activities. Also, data subjects are granted individual rights such as the right to access and to rectify information, but sometimes they are accompanied by such broad exceptions as to reduce them to hollow shells.

The analysis of all the different provisions in Europe and in the United States leads to the realization that the main problem is to effectively safeguard health data and uphold the value of the human person while designing workable rules and allowing for smooth transactions. To this end, it is not enough to create bright-line rules that generate incentives merely to comply with the law rather than to provide effective protection: rather, requesting data controllers to regularly perform an assessment of risks looks like a much more desirable approach.

Chapter II • E-Health and Electronic Health Records in the European Union and in the United States

1. Preliminary Considerations

Among the defining characteristics of our modern era is the way in which new technologies have permeated the different realms of daily life. In no place is this more evident than in the area of e-Health, where we encounter the intersection of the provision of healthcare services and technology. The e-Health phenomenon is a broad category that encompasses many different innovations, including telemedicine and electronic health records (EHRs)[1]. Indeed, "[t]echnological progress has extended the degree of effectiveness and sophistication of medical intervention resulting in a rise in social expectations and, consequently, in higher claims by patients with new requirements such as: an ever more pressing need for health, a growing expectation towards the system, and a greater degree of information (computer-health literacy)"[2]. Because health care and information are inextricably intertwined, as the physician-patient relationship largely depends on an exchange of information[3], the advent of technological innovation within health care has brought about different ways to share such information.

The driving force behind these developments has been the pursuit of a more efficient and less costly health care system. Unfortunately, this pursuit has created some tricky incentives which tend to conceal and undermine some important stakeholder interests. While the reduction of transaction costs and the implementation of smoother flows of information between health care providers are both very praiseworthy goals, the overriding concern in developing an e-Health model has been to facilitate smooth transfers

---

[1] Telemedicine consists in the provision of health care services at a distance using interactive technological tools. It is important to bear in mind that it "is not an alternative treatment that replaces the traditional doctor-patient relationship", but "[r]ather it is a tool that is complementary to it, enhancing the delivery of health services and reducing inherent limitations, primarily due to distance". P. GUARDA, *Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context*, Trento Law and Technology Research Group, Research Paper n. 23 (July 2015), available at: https://iris.unitn.it/retrieve/handle/11572/109729/14864/Guarda_LawTechRP_23_2.pdf, at 19. For more information on e-Health and telemedicine, see F. ABET, *Il ruolo delle tecnologie per una sanità moderna: la telemedicina*, in *Informatica & Documentazione*, 2007, 51; E. BRENNA, *La valutazione economica delle tecnologie in sanità con particolare riferimento all'area della telemedicina*, in *Sanità pubbl.*, 2001, 89; L. BUCCOLIERO, C. CACCIA, G. NASI, *E-he@lth. Percorsi di implementazione dei sistemi informativi in sanità*, Milano 2005; C. CACCIA, *Management dei sistemi informativi in sanità*, Milano, 2008; G. CANGELOSI, *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in *Dir. famiglia*, 2007; B.J. CRIGGER, *e-Medicine: Policy to Shape the Future of Health Care*, 36 *The Hastings Center Report* 12 (2006); L.A. FLIER, *Health information technology in the era of care delivery reform. To what end?*, in *JAMA*, 2012, 307, 24, 2593; U. IZZO, *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, in *Danno e resp.*, 8-9, 807-18 (2000); R. LATIFI (ED.), *Current principles and practices of telemedicine and e-health*, Amsterdam 2008; M. MORUZZI, *Internet e Sanità. Organizzazioni e management al tempo della rete*, Milano 2008; A. NARDONE, M. TRIASSI, *Profili organizzativi e giuridici della telemedicina nel quadro delle risorse tecnologiche in sanità*, in *Sanità pubblica e privata*, 2003, 27; L. NICOLAS, *EHealth, health networks and electronic health record: towards a culture of sharing and trust*, 33 *Rev Med Brux.*, 2012, 4, 416; N.P. TERRY, *A Medical Ghost in the E-Health Machine*, 14 *Health Matrix* 225-29 (2004); A. SINHA, *An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century*, in *Medical Anthropology Quarterly*, New Series, vol. 14, n. 3 (Sep. 2000); B. STANBERRY, *The legal and ethical aspects of telemedicine: data protection, security and European law*, 4 *Journal of Telemedicine and Telecare*, 18 (1998); S. WALLACE ET AL., *The legal and risk management conundrum of telemedicine, in 5 Journal of Telemedicine and Telecare*, 1999, 8.

[2] GUARDA (2015), *supra* note 1, at 6.

[3] *See* IZZO, *supra* note 1, at 807-08.

of data, which creates some cause for alarm. This requires us to pay particular attention to avoiding workable solutions that do not fully respect individual rights and public health interests. How has this affected the implementation of e-Health systems? Have the privacy concerns been adequately taken into account? These are some of the questions this chapter seeks to answer by focusing on the phenomenon of electronic health records, which best embodies the different concerns we would like to tackle. Despite the several advantages of EHR systems, including the reduction of errors and expenditures along with the improvement of health care services, they also create risks to privacy and human dignity. Tiered, modular solutions that do not rely on bright-line rules are the ones that best take into account privacy and dignity interests, while also being effective in promoting efficiency and transparency.

To begin, this Chapter will illustrate the lights and shadows of the EHR phenomenon, with a focus on the issue of informed consent, which has often proved to be unable to fulfill its promises. Then, we will address the implementation of electronic health records in Europe and in the United States. The inquiry into the European framework has been enriched by an analysis of the Italian experience, which is a particularly interesting scenario given the state-of-the-art EHR systems that have been implemented and the adoption of specific legislation. Finally, the Chapter offers a glance at the topics of mobile health apps and cloud computing, by providing an overview of the relevant legal issues and focusing on the concerns these two phenomena share with electronic health records.

2. E-Health: How Technology Meets Health Care

E-Health is a phenomenon concerning "the application of information and communication technologies across the whole range of functions that affect the health care sector" [4]. This encompasses various categories of applications, including clinical information systems, telemedicine, and electronic health records. We can identify four "waves" in the history of this phenomenon. Historically, e-Health "first emerged in the guise of "telemedicine", [which] has delivered […] medical services to rural and other underserved communities for three decades"[5]. Then, "the second wave of e-health […] focused our attention on innovative structures for health care delivery that were designed to supplement or even compete with traditional health care", as it was basically rooted in the e-commerce phenomenon and business-to-consumer models and included for instance health information websites[6]. Recently, the third wave shifted to business-to-business services, while the latest fourth wave "sees technologically-mediated care less as a goal in and of itself […], but as a method of solving severe and pressing issues in traditional health

[4] S. CALLENS, *The EU legal framework on e-health*, in E. MOSSIALOS, G. PERMANAND, R. BAETEN, T. HERVEY (EDS.), *Health Systems Governance in Europe – The Role of EU Law and Policy*, Cambridge University Press 2010, at 561. E-Health has been described as "cover[ing] the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals; it can also include health information networks, electronic health records, telemedicine services, and personal wearable and portable communicable systems for monitoring and supporting patients". EUROPEAN COMMISSION, *eHealth Task Force Report 2007. European Lead Market Initiative for Europe*, Brussels 2007, at 10. Interestingly, it has been stated that the basic concept of E-Health is that "these technologies let computers do what they do best – collect and disseminate data – while letting doctors do the doctoring". K.M. BRISCH AND C.E. HAUPT, *Information Technology Meets Healthcare: The Present and Future of German and European E-Health Initiatives*, 12 *DePaul J. Health Care L.* 105, 105 (2009) (citing J.B. MARTIN, *Op-Ed., Digital Doctoring*, Boston Globe, March 29, 2007). *See also* G. EYSENBACH, *What is e-health? [editorial]*, in *Journal of Medical Internet Research*, vol. 3, n. 2, 2001, e(20).

[5] N.P. TERRY, *E-Health: Perspective and Promise*, 46 *St. Louis U. L.J.* 1, 1 (2002).

[6] *Id.* at 1-2.

care: spiraling health care costs and medical error"[7].

Clearly, health care systems are facing new, complex challenges with a transnational scope[8]. This is amplified by a growing demand for health care services due to the progressively aging population in developed countries and higher average income levels, as well as an evolution of patient expectations and of the health care provision system[9]. As a consequence, the development of e-Health has generally been endorsed by governments as a public goal. For instance, in April 2004 the European Commission adopted an E-Health Action Plan[10], as the Commission considered e-health as "an instrument for restructured, citizen-centered health care systems, which, at the same time, respects the diversity of Europe's multicultural, multilingual health care traditions"[11]. The overall goal was "enabling higher-quality, effective health care that is safe, empowering and accessible for patients and cost-effective for governments"[12]. This plan "would build on a variety of common policies and initiatives and create concerted efforts providing an environment fostering the integration of related policy on the Community level"[13]. Then, in 2009, the European Commission published its Digital Agenda as part of the Europe 2020 Strategy[14], which established the goal of defining a set of patient data for interoperable patient records and gave patients secure access to their digital health records[15]. The new "eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century"[16] also stresses the importance of creating a fully mature eHealth system in Europe. Meanwhile, the United States has also undergone a push towards e-Health initiatives, despite the fact that "United States health lawyers view e-health as an essentially private business model"[17]: former President Bush announced in 2004 that most Americans should have electronic health records by 2014, a goal that was again stressed by President Obama. Everywhere in the world the transformation of health care has become a priority due to "various major challenges […] such as rising costs, shortages of many different kinds of health-related staff, demographic changes, medical errors, a growing elderly population that potentially needs prolonged medical care, the increasing management costs of chronic diseases and fragmented […]

---

[7] *Id.* at 2.

[8] P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, Università degli Studi di Trento, 2011, at 9.

[9] *See* P. GUARDA, R. DUCATO, *Profili giuridici dei Personal Health Records: l'autogestione dei dati sanitari da parte del paziente tra privacy e tutela della salute*, 3 *Rivista Critica del Diritto Privato* 389, 393-94 (2014).

[10] European Commission, *'e-Health – making healthcare better for European citizens: an action plan for a European e-Health Area'*, COM(2004)356 final, 30 April 2004 [hereinafter e-Health Action Plan 2004].

[11] CALLENS, *supra* note 4, at 573-74.

[12] *Id.* at 574 (citing EUROPEAN COMMISSION AND MEMBER STATES, '*eHealth Conference 2007 Final Declaration*', 17 April 2007).

[13] BRISCH & HAUPT, *supra* note 4, at 110 (citing e-Health Action Plan 2004, at 4).

[14] European Commission, *A digital agenda for Europe*, 26 August 2010, COM(2010)245; European Commission, *Europe 2020—A strategy for smart, sustainable and inclusive growth*, COM (2010) 2020.

[15] *See also* European Commission, *White paper - Together for Health: A Strategic Approach for the EU 2008-2013*, COM(2007) 630 final, Brussels, October 23, 2007; European Commission, Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems, C(2008) 3282, 2008/594/EC, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008H0594&from=EN [hereinafter European Commission Recommendation on cross-border interoperability of EHR systems]; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*, COM(2008) 689, Brussels, November 4, 2008.

[16] European Commission, *Communication "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century"*, COM (2012) 736 final.

[17] TERRY, *supra* note 5, at 3.

services and solutions"[18].

Using technology in the health care sector is therefore "a natural progression for the digital agenda", as well as a part of the broader transformation of society, which is increasingly characterized by "information flows"[19]. However, it also creates several challenges linked to "remodeling a sector that has traditionally operated through direct face-to-face human contact"[20]. Patient information can no longer be accessed only by the health care practitioners directly involved with the patient[21]. This creates important issues with respect to patient trust: "it is necessary for the patient to trust that the healthcare system will uphold the long-held principle of confidentiality"[22]. Lack of trust may generate reluctance on behalf of the patient to disclose accurate information or to go to the doctor at all, which is likely to result in a harmful outcome[23]. The widespread application of e-Health solutions needs to face the privacy concerns related to "the need to constantly access identifiable information, relative to large group of subjects, ideally for the overall population"[24]. The importance of "the degree and completeness of the information flow that supports the actions and the decisions between the different providers" stems from the fact that "[m]edical practice has evolved" and "must demonstrably be effective and safe", as "health care professionals [are] no longer confined to respect an 'obligation of means' but are practicing to reach outcomes"'[25]. In addition, the number of health care providers involved is much larger, as "the need for collaboration between care professionals has passed the walls of hospitals"[26]. The phenomenon of e-Health needs to deal with these new challenges.

3. Electronic Health Records: the Issues

Electronic health record systems are a powerful tool for health care professionals and patients, so much so that they not only deeply affect our daily life, but also bring about relevant changes in the legal framework and in society at large[27]. Thus, we have chosen to analyze this phenomenon in depth, among all the different e-Health tools.

3.1 Definitions

The concept of electronic health record really encompasses many different tools, reflecting differences in complexity and structure, as well as many attempts to provide

---

[18] C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY, *Assessing Legal, Ethical and Governance Challenges in eHealth*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 4. *See also* GUARDA, *supra* note 8, at 9-10.

[19] GUARDA, *supra* note 8, at 11.

[20] P. DUQUENOY, N. M. MEKAWIE AND M. SPRINGETT, *Patients, Trust and Ethics in Information Privacy in eHealth*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 275.

[21] *Id.* at 276. *See also* GUARDA, *supra* note 8, at 7.

[22] DUQUENOY ET AL., *supra* note 20, at 281.

[23] *Id.* at 283.

[24] C. T. DI IORIO & F. CARINCI, *Privacy and Health Care Information Systems: Where Is The Balance?*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 78.

[25] P. STACCINI, C. DANIEL, T. DART, AND O. BOUHADDOU, *Sharing Data and Medical Records*, in A. VENOT, A. BURGUN AND C. QUANTIN (EDS.), *Medical Informatics, e-Health. Fundamentals and Applications*, Springer 2014, at 316.

[26] *Id.* at 316-17.

[27] GUARDA, *supra* note 8, at 167.

accurate definitions[28]. The two models that we can examine here are Electronic Health Records and Personal Health Records.

Electronic health records have been defined by the Article 29 Working Party as "comprehensive medical record[s] or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes"[29]. Unlike traditional health records, EHRs aim at collecting in one place all the health data concerning a patient – 'from the cradle to the grave' – and sharing it among a plurality of actors[30]. Coherently, another definition, which has been provided by the National Alliance for Health Information Technology, clarifies that it is "an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed and consulted by authorized clinicians and staff across more than one health care organization" [31]. The difference between EHR and the earlier models is that the patient is no longer seen as the object of the healthcare process but rather as the active subject[32], who can "participate more effectively in [his or her] care"[33].

The Personal Health Record (PHR) is featured by an approach aimed at storing and processing only those data that are relevant to the patient[34]. PHRs "are created upon request and consent of the individuals involved, recognized as the owners", and "information is disclosed only to those authorized by the owners"[35]. A patient can actively interact with his PHR and create new data: this means that this data creation can occur without any qualified subject acting as intermediary[36]. However, due to the "skepticism about the reliability of patient-maintained PHRs", the trend "has more recently emphasized technologies that allow patients to access their providers' record systems, communicate

---

[28] *Id.* at 27. For an analysis of the different models proposed by the Medical Record Institute (Automated Medical Record, Computerised Medical Record, Electronic Medical Record, Electronic Patient Record, Electronic Health Record, Personal Health Record), see *id.* at 28-30. For further insights on electronic health records and personal health records, see R. GARTEE, *Electronic Health Records. Understanding and Using Computerized Medical Records*, Upper Saddle River - New Jersey, 2007; M.A. HALL, *Property, Privacy and the Pursuit of Integrated Electronic Medical Records*, Wake Forest Univ. Legal Studies Paper No. 1334963; J.G. HODGE ET AL., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 *JAMA* 1466 (1999); S. HOFFMAN & A. PODGURSKI, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 *Berkeley Tech. L.J.* 1523 (2009); S. HOFFMAN & A. PODGURSKI, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, Working Paper 06-15, September 2006; N.P. TERRY, *Electronic health records: International, structural and legal perspectives*, 12 *Journal of Legal Medicine* No. 1 (2004); J. WALKER, E.J. BIEBER, F. RICHARDS (eds.), *Implementing an electronic health record system*, New York, N.Y., 2006.

[29] Article 29 WP Working Document 2007 on EHR, at 4. For a more specific analysis of the EHR features, see GUARDA, *supra* note 8, at 34-37.

[30] V. PEIGNÉ, *Il Fascicolo Sanitario Elettronico, Verso Una "Trasparenza Sanitaria" Della Persona – Electronic Health Records: Towards An "Health Transparency" Of The Individual*, 6 *Riv. It. Medicina Legale* 1519 (2011).

[31] J. DUMORTIER AND G. VERHENNEMAN, *Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 26-27. Another definition has been provided by the International Organization for Standardization, which considers EHR as a "repository of information regarding the health status of a subject of care, in computer-processing form, stored and transmitted securely, and accessible by multiple authorized users". U. IZZO AND R. DUCATO, *The Privacy of Minors within Patient-Centered e-Health Systems*, Trento Law and Technology Research Group, Research Paper n. 21, June 2014, at 4.

[32] GUARDA, *supra* note 8, at 30-31.

[33] WALKER, BIEBER, RICHARDS (eds.), *supra* note 28, at 153.

[34] GUARDA, *supra* note 8, at 31.

[35] STACCINI ET AL., *supra* note 25, at 324.

[36] GUARDA, *supra* note 8, at 32.

interactively with providers, or upload information directly into their providers' records"[37]. Interestingly, many consumers declare that they "are concerned about the privacy and security of their health information, but most of those using PHRs are not worried about privacy implications"[38]. Nevertheless, a system of patient interaction with provider EHRs "raises a host of issues of data privacy, confidentiality and security", in particular with respect to patient awareness that the data entered may then be used and disclosed by providers, to "determining that the person actually interacting with the EHR is the patient him or herself", and to "making sure that an authorized person is accessing only those portions of the record that the patient wants to have accessed by that person"[39].

3.2 Electronic Health Records and Public Policy

Very often EHR systems are supported and funded by governments aiming at creating a more efficient health care system. Among the government-implemented systems, we can see that some are organized on a regional basis, some on a national basis, and some employ a blended model[40]. Public funding is also a solution to the market failures perturbing this field: "[m]uch of the savings from EHR will accrue to payers […] rather than health care providers actually investing in the technology"[41]. Together with this "misaligned incentives" problem, the "network effects" phenomenon has contributed, too, since "[t]he marginal value for an individual provider to seek out a network-ready EHR is very low when so few […] systems have been deployed"[42]. As a well-known health care entrepreneur and author provocatively suggested, and without anticipating that something similar would occur, "[t]he federal government can and should write the huge check and be done with it"[43]. In fact, the incentive programs designed in the United States are an attempt to answer the market failures problem[44].

In order to further the public goals, governments can adopt one of two solutions: they can either "build a public infrastructure for the exchange of records and extrapolation of data that will protect individual privacy" or "develop a regulatory framework of privacy and security requirements by which private industry may act"[45].

The introduction of EHR systems has led to the "addition of a new layer of regulation": in Europe it was often included in laws on national eHealth services, whereas the US adopted a broader approach by putting in place a stimulus package, conditioned on showing that EHRs are used in a "meaningful" way[46].

3.3 Electronic Health Records: the Lights

Electronic health record systems aim toward two large groups of goals. The first set

---

[37] L.P. FRANCIS, *When Patients Interact with EHRs: Problems of Privacy and Confidentiality*, 12 *Hous. J. Health Law & Policy* 171, 174 (2012).
[38] STACCINI ET AL., *supra* note 25, at 324.
[39] FRANCIS, *supra* note 37, at 182.
[40] PEIGNÉ, *supra* note 30.
[41] N.P. TERRY, *Certification and Meaningful Use: Reframing Adoption of Electronic Health Record as a Quality Imperative*, 8 *Ind. Health L. Rev.* 45, 47 (2011).
[42] *Id.* at 48.
[43] J.D. KLEINKE, *Dot-Gov: Market Failure and the Creation of a National Health Information Technology System*, 24 *Health Aff.* 1246, 1258 (2005).
[44] *See* Paragraph 7.1.
[45] K. BOMASH, *Privacy and Public Health in the Information Age: Electronic Health Records and the Minnesota Health Records Act*, 10 *Minn. J.L. Sci. & Tech.* 117, 123-24 (2009).
[46] DUMORTIER AND VERHENNEMAN, *supra* note 31, at 36.

of objectives relates to increased efficiency, cost reduction and ease of transactions, whereas the second group concerns the improvement of individual health care and public health through transparency and data sharing. It is hard to determine whether one side has prevailed over the other, but it is important to highlight that prioritizing efficiency may lead to legal frameworks that do not adequately take into account privacy concerns.

3.3.1 Efficiency and Savings

The efficiency-driven goals concern the reduction of medical errors and, as a consequence, the reduction of costs, which is particularly necessary "[a]s the pressure to reduce ballooning healthcare expenditures continues to rise" [47]. The technological innovation has triggered "a positive interaction" between ICT (Information and Communication Technology) and health care[48]. For instance, an accurate record of the patient's medical history avoids duplicative efforts: "if a patient seeks a second opinion after one physician's diagnosis, the second physician can easily determine which tests have already been performed and obtain the results of those tests"[49]. Also, it can "[reduce] care variability by use of data to define and disseminate best practices, therefore helping to deliver more effective care to a broader patient base"[50]. An analysis in 2005 predicted that if 90% of hospitals and doctors in the United States adopted health information technology over fifteen years there could be a saving of almost $77 billion a year[51], provided that "all, or nearly all, healthcare organizations participate in sharing EHRs"[52]. Therefore, EHRs are considered to be "an appropriate means to "improve the cost efficiency of medical treatments and thus prevent further rapid growth of health care budget deficits"[53].

The switch to electronic health records has been considered an "economic imperative" meant to "maintain health and at the same time maintain the momentum of our economy"[54]. Some commentators have aptly said that "[t]he advent of the [EHR] has been accompanied by some buzzwords in these times of crisis: efficiency, savings and quality" [55]. As discussed above, the focus on economic growth creates the risk of disregarding other values at stake: "progress towards these laudable goals has, so far, reflected institutional interests and priorities" and, according to some commentators, "has been an example of "insider baseball" that has focused primarily on architecture and

---

[47] J. HILLER, M.S. MCMULLEN, W. M. CHUMNEY, D.L. BAUMER, *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*, 17 *B.U. J. Sci. & Tech. L.* 1, 3 (2011). *See also* M.B. BUNTIN ET AL., *The Benefits Of Health Information Technology: A Review Of The Recent Literature Shows Predominantly Positive Results*, in 30 He*alth Affairs*, 2011, 464; B. CHAUDHRY ET AL., *Systematic Review: Impact of Health Information Technology on Quality, Efficiency and Costs of Medical Care*, in 144 *Ann. Intern. Med.*, 2006, 742; D. THOMPSON ET AL., *Reducing Clinical Costs with an EHR*, in 64 *Healthcare Financial Management*, 2010, 106; S. WU, B. CHAUDHRY, J. WANG, M. MAGLIONE, W. MOJICA, E. ROTH, *Systematic Review: Impact of Health Information Technology on Quality, Efficiency and Costs of Medical Care*, in *Annals of Internal Medicine*, 144, 10, 2006, 742.

[48] GUARDA (2015), *supra* note 1, at 7.

[49] A. GRADY, *Electronic Health Records: How The United States Can Learn From The French Dossier Medical Personnel*, 30 *Wis. Int'l L.J.* 374, 377 (2013).

[50] HILLER ET AL., *supra* note 47, at 6.

[51] THE ECONOMIST, *Medicine goes digital. A special report on health care and technology*, April 18, 2009, available at: http://www.economist.com/sites/default/files/special-reports-pdfs/13447102.pdf, at 3.

[52] HILLER ET AL., *supra* note 47, at 5.

[53] Article 29 WP Working Document 2007 on EHR, at 5.

[54] N.P. TERRY & L. FRANCIS, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 *U. Ill. L. Rev.* 681, 734-35 (2007).

[55] IZZO & DUCATO, *supra* note 31, at 6.

technical standards"[56]. An efficiency-driven mindset has often led to considering privacy and security concerns as "barriers" to electronic health record implementation[57], instead of seeing them as useful resources to build up a system that is accurately taking into account all the different interests at stake. Indeed, "[w]hether framed in terms of data protection laws, a duty of confidentiality, a right to respect for private life, medical ethics, or professional responsibility, those who are able to access private health information about individuals are bound by a variety of obligations", but they "should not be seen as obstacles […] but rather aspects of the fair and legal treatment of a patient who is first and foremost a private individual"[58].

3.3.2 Better Health Care and Public Health

As to the second group of objectives, the need to share health data is part of a broader transformation of the provision of health care services, featured by a multiplication of the number of actors involved and an ever-growing patient mobility[59]. This scenario makes it crucially important to have an accurate and comprehensive record of the patient's medical history, as well as an improvement of "the overall interaction between parties inside and out of the [health care] system"[60]. It is very easy to notice that "[t]he more accurate is the collection of data, as long as they are accessible and correctly transposed, the greater will be the goals that the system will be able to achieve"[61]. Electronic health records should support "the appropriate treatment of patients by providing health professionals with a better knowledge of a patient's history and previous interventions by other medical practitioners"[62]. Coordinating the efforts of the health care providers leads to better health care, both from the perspective of the individual patient and from the perspective of public health.

Looking at individual health, an "accurate and efficient flow of patient medical information between providers" has been considered to "improve preventative treatment and the continuity, coordination, and quality of care"[63], even by reducing medical errors[64]. This can happen, first, because EHRs can "help with the filtering, organization, and provision of access to information that physicians […] need"[65]. According to many studies, "EHR databases are a cost-effective way to reduce medical errors due to disorganized and inaccessible patient data, thus improving medical care"[66]. Secondly, they are a useful tool to document all kinds of necessary data, such as evaluations and diagnoses, the history of the different steps of the treatment and ongoing assessment, and questions and problem lists[67]. Because e-Health projects allow the aggregation of the pieces of information on previous

---

[56] TERRY & FRANCIS, *supra* note 54, at 735.
[57] *See*, e.g., GRADY, *supra* note 49, at 388 ("Data privacy and security concerns have been one of the major barriers to the adoption of EHRs").
[58] E. WICKS, *Electronic Health Records and Privacy Interests: The English Experience*, in C. GEORGE, D. WHITEHOUSE, P. DUQUENOY (eds.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013, at 76.
[59] PEIGNÉ, *supra* note 30.
[60] S. R. GERING, Electronic Health Records: How to Avoid Digital Disaster, 16 *Mich. St. U. J. Med. & L.* 297, 300 (2012).
[61] IZZO & DUCATO, *supra* note 31, at 5.
[62] CALLENS, *supra* note 4, at 576 (citing e-Health Action Plan 2004, *supra* note 10, at 8).
[63] GRADY, *supra* note 49, at 378.
[64] *See* HILLER ET AL., *supra* note 47, at 4.
[65] J. KLOSEK, *Exploring The Barriers to The More Widespread Adoption of Electronic Health Records*, 25 *Notre Dame J. L. Ethics & Public Policy* 429, 432 (2011).
[66] GRADY, *supra* note 49, at 376-77.
[67] *Id.*

treatments and ideas, they enhance the chance to make steps toward better health conditions[68]. Moreover, EHRs are searchable and "can be scanned for drug interactions or for consistent patterns of symptoms"[69]. Thirdly, templates and checklist prompts "can help to ensure that medical professionals ask key questions and consider all relevant diagnoses"[70], even though some risks are lurking behind this apparently innocuous aspect, as we will discuss in the following paragraphs.

At the same time, within the public health care sector, EHRs can "furnish the necessary data for quality control, statistics and planning"[71], as "a national database of population health measures will improve public health reporting"[72]. It has been noted that the implementation of an EHR network "would aid public health in all three of its core functions: assessment, assurance, and policy promotion"[73]. First of all, it "would allow for better and faster assessment of diseases that strike the general population" and "for non-industry assessment of competing treatments and faster development of evidence-based physician treatment guidelines"[74]. Also, it "may improve assurance that [a] disease can be contained" and "has public health benefits for emergency and disaster planning"[75]. Thirdly, it "would aid in policy promotion because it could provide more accurate data regarding the incidence and prevalence of disease, the effectiveness of alternative treatments for those diseases, and the treatment costs"[76]. These important goals are pursued through easier access and more legible information: information contained in an EHR is more easily accessible than that on a traditional record and is constantly up to date as well as more legible (it is a well known stereotype that doctors "have terrible handwriting")[77].

Therefore, it looks like the overarching goal is the convergence of the privacy of the individual and the interest to public health: they are not to be conceived as mutually exclusive but rather as two indispensable pieces of the same puzzle[78].

3.4 Electronic Health Records: the Shadows

Electronic health records offer "[t]he opportunity to reduce costs and provide safer, more effective healthcare"[79], but their full implementation has encountered several hurdles, such as financial barriers due to the very high initial costs[80], and technological barriers linked to the necessity of extremely advanced tools[81]. It has also generated relevant risks[82]. Common justifications for EHRs, such as faster access by health staff and by patients themselves, usually start from a number of assumptions: it is assumed that data will be reliable and easy to access disregarding the risk of incompleteness or lack of accuracy, it is

---

[68] GUARDA, *supra* note 8, at 13.
[69] TERRY & FRANCIS, *supra* note 54, at 683.
[70] *Id.*
[71] Article 29 WP Working Document 2007 on EHR, at 5.
[72] GRADY, *supra* note 49, at 377. *See also* GUARDA, *supra* note 8, at 229.
[73] BOMASH, supra note 45, at 120.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] TURK, *supra* note 623, at 568.
[78] *See* GUARDA, *supra* note 8, at 230.
[79] HILLER ET AL., *supra* note 47, at 4.
[80] *See* GRADY, *supra* note 49, at 377; J.D. SZEREJKO, *Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security*, 47 *Conn. L. Rev.* 1103, 1106-07 (2015); GERING, *supra* note 60, at at 311-12.
[81] *See* GERING, *supra* note 60, at 395-96.
[82] *See also* TERRY & FRANCIS, *supra* note 54, at 683.

assumed that only authorized staff will access data only when necessary for treatment, overlooking security concerns linked to technological and human weakness, and it is assumed that a patient wishes to have greater access to his medical data[83]. However, those risks represent "a significant obstacle to public acceptance of EHRs"[84], which is related to the fact that they "transgress the traditional boundaries of the individual patient's direct relationship with a health care professional or institution"[85], traditionally occurring through oral and written contact[86]. In order for electronic health record systems to be successful, though, they need patient trust, as the "unwillingness [to disclose critical information] would prove detrimental to the quality of […] healthcare and thus to their health"[87]. Indeed, "the public perception of an EHR as a governmental "big brother" is increasingly likely" and this undermines the chances of success[88].

The number of risks to deal with makes it necessary to adopt a modular approach in order to fully take into account all the degrees of complexity[89]. This must be implemented at two different levels: first, with respect to the right of self-determination, and secondly, with respect to the different e-health mechanisms, which should be able to evolve and be modified without impacting the rest of the system[90].

3.4.1 Risks to Patient Privacy and Security

Probably "the most complex set of risks is to patient privacy and security"[91], as EHRs will "decrease the privacy of individuals in the sensitive area of personal health information and treatment"[92]. Somewhat connected to such risks is the possibility of "the aggregation of one's personal information from a variety of authorized sources"[93].

Some have argued that "[a] combination of technical and legal improvement in EHRs could make the loss of privacy associated with EHRs de minimis"[94] and that "[t]he EU has come closer to this position, encouraging the adoption of EHRs and confirming the application of privacy protections at the same time". Whereas the EU adopts a more "proactive" approach, the US still "lacks a strong framework for healthcare privacy"[95].

First of all, inadequately designed legal systems, defective safeguards, or negligent technical system design can cause data breaches and losses of PHI privacy[96], which "eliminate the trust necessary for a patient-physician relationship"[97], especially if combined with a failure to timely report them[98]. Data breaches can also occur due to the loss or theft of mobile electronic devices: as one commentator aptly says, "the ability to store copious

---

[83] WICKS, *supra* note 58, at 61.
[84] HILLER ET AL., *supra* note 47, at 6.
[85] CALLENS, *supra* note 4, at 578.
[86] *See* GUARDA & DUCATO, *supra* note 9, at 395-96.
[87] E. RIVKIN-HAAS, *Electronic Medical Records and the Challenge to Privacy: How the United States and Canada Are Responding*, 34 *Hastings International & Comparative Law Review* 177 (2011).
[88] TERRY & FRANCIS, *supra* note 54, at 684.
[89] GUARDA, *supra* note 8, at 38.
[90] *Id.* at 38-39.
[91] HILLER ET AL., *supra* note 47, at 6.
[92] *Id.* at 4.
[93] RIVKIN-HAAS, *supra* note 87, at 193.
[94] HILLER ET AL., *supra* note 47, at 1.
[95] *Id.* at 1-2.
[96] *Id.* at 4. *See also* TURK, *supra* note 623, at 569. For some example of health data breaches, see GERING, *supra* note 60, at 310.
[97] GERING, *supra* note 60, at 309.
[98] *See id.* at 310.

amounts of data electronically in one device can be a gift and a curse"[99]. Just like in society at large, technology makes us personally more powerful and more vulnerable at the same time, as evidenced through the cyber attack risks born in the last decades[100].

Furthermore, the data contained in EHRs "are used increasingly for purposes other than treatment, and health care actors are becoming more global", so in Europe "there are more opportunities to process health data among several Member States and/or third parties"[101].

Enhanced access does not necessarily enhance record quality, as "the best medical records require concerns about consent, security, accuracy and public confidence to be adequately tackled"[102], and also creates several risks. Thus, with respect to access by health care professionals, "there needs to be a delicate balance between a doctor's use of technology in conjunction with their ability to strategically think"[103]. Otherwise, there is the risk that "[d]octors […] resort to simply checking the boxes provided instead of taking the time to write detailed information about a specific patient", thereby waiving many of the promised gains[104]. Indeed, the templates used by electronic systems "can give the provider a roadmap to remember what to document" but "can cause issues when a physician moves down the form filling in sections just to fill them in without reason or need"[105].

EHRs are also meant to make data "more readily available to a wider circle of recipients"[106]. Indeed, "electronic health information in an EHR system – apart from being accessible to health care professionals – might generally attract the interest of third parties such as insurance companies and law enforcement agencies"[107]. This "chang[es] the whole scale of possible misuse of medical information about individuals"[108], as the traditional confidentiality model no longer holds up "in the corporate healthcare context"[109].

Another very relevant risk regards medical identity theft, which is "the theft of personally identifiable health information in order to gain access to health treatment or to fraudulently file for reimbursement for false medical treatment"[110]. The two most common types of medical identity theft occur "when an internal employee steals a patient's information" or when "an individual uses another's identity to receive medical services or goods"[111]. The implementation of EHRs "will exponentially increase the number of patient records obtainable by [identity] thieves, also making notification to victims more difficult"[112]. The same "great technological innovations that facilitate saving lives also provide criminals with tools for their respective trade"[113].

---

99 SZEREJKO, *supra* note 80, at 1127-28. *See also* KLOSEK, *supra* note 65, at 436.
100 *See* E. SCHMIDT AND J. COHEN, *The New Digital Age: Reshaping the Future of People, Nations and Business*, Knopf 2013.
101 CALLENS, *supra* note 4, at 577.
102 WICKS, *supra* note 58, at 62.
103 GERING, *supra* note 60, at 315.
104 TURK, *supra* note 623, at 569.
105 GERING, *supra* note 60, at 312.
106 CALLENS, *supra* note 4, at 577.
107 Article 29 WP Working Document 2007 on EHR, at 5
108 *Id.*
109 RIVKIN-HAAS, *supra* note 87, at 181.
110 HILLER ET AL., *supra* note 47, at 7-8.
111 *Id.* at 8. *See also* KLOSEK, *supra* note 65, at 437.
112 HILLER ET AL., *supra* note 47, at 8. *See also* C. CIAMPI, *La Sicurezza dei Dati Personali Sanitari*, in *Rivista elettronica di Diritto, Economia, Management*, n. 3, 2014, at 29-33.
113 SZEREJKO, *supra* note 80, at 1106.

3.4.2 Turning the Person Into a Stack of Data?

The creation of a sanitary record that potentially includes the whole medical history of a patient can fall within the broader tendency of our digital era to create personal profiles. Social networks are the brightest example of this trend, which leads to a more and more detailed online record of each individual. At the same time, we can see how our society favors "transparency" over "secrecy" in order to better monitor individuals, for purposes of national security or public health[114]. We should be aware of the risks lurking behind this tendency, especially when we are dealing with sensitive data. The "simultaneous evolution of health services research, statistical methods, and information technology has created new opportunities to use health information for public health monitoring, surveillance and policy"[115].

As much as public health and security are laudable goals, EHRs should not be turned into a way to reduce the human person to a mere stack of data[116]. It is easy to imagine how EHRs could be a useful source of information for border controls or, worse, practices leaning towards eugenics[117]. Indeed, this is only one of the aspects of excessive transparency that we need to be very cautious about in our era[118]. In order to avoid harms to human dignity, it is necessary to highlight the importance of the proportionality and minimization principles, established by Article 6.1 of Directive 95/46, by Section 3 of the Italian Data Protection Code, and to a lesser extent by HIPAA, via the minimum necessary standard. The importance of this principle can only be borne in mind if we are constantly aware that – as the Data Protection Directive aptly notes – "data-processing systems are designed to serve man"[119], and we do not fall prey to the temptation of thinking that "health privacy laws must focus not on people, nor records, but on health data"[120].

Another similar risk that has been highlighted by some scholars is that these health care technologies "[seek] to minimize the role of the individual autonomous physician (and the correlative autonomous patient)" because they "replace autonomy and choice with systems that identify while simultaneously commodifying patients (e.g., by positively identifying them with bar codes) and reduce discretion in treatment" by relying on guidelines and templates[121]. This approach potentially "depersonalizes medicine"[122]. As much as we should not give too broad of a role to patient self-determination (see paragraph 4), we should refrain from "preferring an instrumental rationale that is almost totally focused on institutions and compliance"[123], and we should look at the provision of health care services as an intrinsically human, complex and nuanced experience. The implementation of digital health care systems creates a risk of "dehumanization" of the patient-physician relationship[124].

---

114 PEIGNÉ, *supra* note 30.

115 DI IORIO & CARINCI, *supra* note 24, at 78. See *id.* at 79-80 for a discussion of some applications of health care information to serve the public interest.

116 PEIGNÉ, *supra* note 30.

117 *See id.*

118 *See, e.g.,* D. EGGERS, *The Circle* (2013) (a dystopian novel showing what transparency conceived as a value per se can lead to).

119 Data Protection Directive, Recital 2.

120 RIVKIN-HAAS, *supra* note 87, at 194.

121 TERRY & FRANCIS, *supra* note 54, at 700.

122 GERING, *supra* note 60, at 312.

123 TERRY & FRANCIS, *supra* note 54, at 700

124 GUARDA (2015), *supra* note 1, at 10. "Today, computer technology fits into the relationship between physician and patient: this relationship is mediated by digital tools even though the parties continue to interact physically". *Id.* at 11. For more insights on the need for the delivery of health care to be "human",

4. Electronic Health Records: Consent, Freedom and Self-determination

A consequence of modern society's reliance on information technology has been the creation of new digital spaces that allow for greater personalization and customization. Health information technology is no exception to this phenomenon, especially if we look at Personal Health Records (PHRs): indeed, it "is gradually creating new virtual spaces for patient participation in the management of their clinical data and is restructuring the process of care around the patient"[125]. The so-called "patient empowerment" trend is defined as "a philosophy of health care that proceeds from the perspective that optimal outcomes of health care interventions are achieved when patients become active participants in the health care process"[126]. Within this approach, "patients and clinicians jointly set goals, select interventions, and assess outcomes according to mutually-defined parameters"[127]. The patient's choices are then respected inasmuch as the legal instrument of consent is conceived in a specific and modular way[128], which depends both on the legal framework and on the technical measures. The implementation of adequate technological structures is clearly crucial to the achievement of such a goal.

Therefore, a deep and crucially important issue has defined the process of designing EHR systems: what is the role of individual choice? What is the degree of autonomy that the data subject should have with respect to the creation of the record, its content and its use? The answers have been varying widely. Interestingly, patient empowerment has also been viewed as a way to increase social acceptance of this tool and build up trust[129]. We will now try to analyze some of the choices patients are given in the EHR world, "choices that range from opting out completely, through redacting specific data or restricting occasions of disclosure, to reviewing the data that is included in the system"[130].

4.1 The Role of Consent in EHRs

Interestingly, "the U.S. and EU have diametrically opposed starting points for what health information may be collected"[131]. The US framework is "based on the assumption that health information will be collected from the individual" and focuses "on the subsequent protection, use, and sharing of that information", whereas the EU features "detailed considerations about whether the information may be collected and how to protect patients in the original collection process" [132]. As a consequence, it can be argued that "patients in the U.S. have no real choice as to whether to participate in the system",

---

see, e.g., E. SGRECCIA, *Non archiviare l'impegno per l'umanizzazione della medicina*, *Medicina e Morale*, 1986, fasc. 2, 267-270.

125 IZZO & DUCATO, *supra* note 31, at 5.

126 P. BRENNAN, C. SAFRAN, *Report of conference track 3: patient empowerment*, 69 *International Journal of Medical Informatics* 301 (2003). *See also* L. BOS, A. MARSH, D. CARROLL, S. GUPTA, M. REES, *Patient 2.0 Empowerment*, in H. ARABNIA, A. MARS (EDS.), *Proceedings of the 2008 International Conference on Semantic Web & Web Services* SWWS08 (2008); P. SUTER, W.N. SUTER, D. JOHNSTON, *Theory-based telehealth and patient empowerment*, 14 *Popul. Health. Manag.* 87 (2011); M. HOUSEH, E. BORYCKI, A. KUSHNIRUK, *Empowering patients through social media: the benefits and challenges*, 20 *Health Informatics J.* 50 (2014); S. RODOTÀ, *Libertà, opportunità, democrazia, informazione, Relazione introduttiva al Convegno "Internet e privacy – quali regole?"*, May 8 1998.

127 BRENNAN & SAFRAN, *supra* note 126, at 301.

128 *See* GUARDA & DUCATO, *supra* note 9, at 395.

129 PEIGNÉ, *supra* note 30.

130 TERRY & FRANCIS, *supra* note 54, at 725.

131 HILLER ET AL., *supra* note 47, at 32.

132 *Id.* at 31.

given the number of exceptions to when a patient's consent is needed, while in the EU "protections should be implemented to prevent coercion of a patient into participation"[133]. The only way to implement EHRs in the EU is the public interest exception, which "requires an explicit legal basis that is tailored to the circumstances and that always allows the right of the patient to either limit sharing or withdraw completely from the system"[134].

In France, in Italy, and in the United Kingdom the creation of an EHR is linked to the person's autonomy[135]. Whereas in France the person's will is necessary for an EHR to be created, in the UK the person only has an opt-out right to oppose to it, which accomplishes the dual goal of taking the individual's will into account and having only a minority of citizens opting out[136]. In Italy, the EHR is created by default and remains an empty tool if the citizen does not provide consent to the insertion of data[137]. This attention to individual preference is meant to enhance social acceptability of this tool, which could hardly be reached if it was imposed from the public authority[138]. Also, this focus on individual freedom generates a person-centered approach to the flow of health data and underlines how the issues related to EHRs concern both individual and collective interests[139]. This increases the likelihood that the patient himself will consent to the creation of an EHR system which embodies both the individual and the public good[140]. Interestingly, research reveals that the most common factor influencing the decision to create an EHR is personal experience, which is inherently subjective and therefore can lean either way[141].

Individual choice is relevant to the content of the EHR, too. In some models the patient can shape his profile and choose which pieces of information he wants to include in his record[142]. This can be grounded in a respect for the patient-physician relationship: the patient discloses as much information as he wants, depending on his trust in the physician, and the implementation of an EHR system should not erase the chance to make these choices[143]. This may negatively affect the accuracy and comprehensiveness of the record. Physicians and other health care providers should then be aware that the EHR may not be exhaustive and does not take away the need for them to get information personally from

---

133 *Id.*

134 *Id.* at 33. For a better understanding, see the chart at 33-34.

135 PEIGNÉ, *supra* note 30. *See Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services – Final report and recommendations*, July 23, 2014, at 33, available at: http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf [hereinafter Report on EHRs in the EU Member States].

136 PEIGNÉ, *supra* note 30. *See also* WICKS, *supra* note 58, at 63.

137 GUARDA & DUCATO, supra note 9, at 410.

138 PEIGNÉ, *supra* note 30.

139 *Id.*

140 *Id.*

141 WICKS, *supra* note 58, at 63 ("So, for those patients who have previously had a bad experience due to a loss or misuse of health data, or have suffered, or are likely to suffer, an episode that requires quick access to accurate health data (particularly perhaps if this occurs at a time when the patient lacks capacity due to a lack of consciousness), the potential benefits of the Summary Care Record easily outweigh any potential drawbacks. Personal experience can also lead to the opposite conclusion, however. […] Those who had been the victim of mistaken identity (in the NHS or outside it), an incorrect medical diagnosis, or identity fraud (such as stolen credit card) tended to be opposed to [the Summary Care Record]. For these patients, the dangers of permitting personal data to be uploaded onto the Internet outweigh any potential benefits. These patients are all too aware that mistakes can occur, and that information is not always secure, and thus are not willing to take the risk with their sensitive health data" (citations omitted)).

142 PEIGNÉ, *supra* note 30.

143 *Id.*

the patient[144].

Also, in some systems the person is able to designate the recipients of the EHR, since his or her consent is needed in order to allow health care providers to have access[145]. For instance, the English model requires "an opt-in from the patient at the point at which a health professional seeks to view the record"[146].

4.2 The Issues with Informed Consent

There is, however, another side to the coin. Any analysis of the importance of individual choice in the field of electronic health records must also account for the inherent problems of informed consent and choice here. As we will see, informed consent mechanisms as currently designed today are ultimately inadequate to take into account all the different interests at stake, and new, creative solutions should be envisioned.

Informed consent for treatment is a doctrine "premised on the concept that not only do individuals have a right to decide what happens to their bodies, but that individual goals, not simply medical goals, should drive treatment choices"[147]. Nowadays, though, "[p]atients are regarded as consumers of healthcare", and "[l]ess attention is paid to whether information sharing and informed consent can live up to the goals we currently set for them"[148]. Especially interesting is "the development of e-Health substitutes for traditional clinical encounters", such as e-Health apps[149] (see paragraph 8.1). It is already farfetched to think that patients are fully capable of understanding their own medical information, as many different biases affect how the patient assesses the pros and cons of a medical intervention[150]. The "use of new technologies as both supplements and substitutes for informed consent" is all the more disconcerting as it "may further obfuscate the nuances of information disclosure and potentially increase the effect of any biases"[151]. On the other hand, using Information and Communications Technology (ICT) in health care can also represent a new chance of meaningful interaction between physicians and patients that would allow the threshold of informed consent to be conceived as higher than obtaining the patient's signature[152].

Some commentators have noted that "[l]egal mechanisms such as informed consent and privacy-confidentiality that operationalize patient interaction with medical services" and give the patients the opportunity to waive some rights "tend to pay only lip service to the underlying autonomy"[153]. The main problem of informed consent mechanisms is that they tend "to focus on the narrow issue of "consent" rather than the disclosure of information that increases patient choice and participation"[154]. For instance, "some staff

---

144 *Id.*

145 *Id.* (referring to the French, Italian and UK systems).

146 WICKS, *supra* note 58, at 63.

147 J. BERG, *The E-Health Revolution and the Necessary Evolution of Informed Consent*, 11 *Indiana Health Law Review* 589, 590 (2014). *See also* C. CASONATO, *Il consenso informato. Profili di diritto comparato*, in C. CASONATO, T.E. FROSINI, T. GROPPI (eds.), *Diritto pubblico comparato ed europeo*, 2009, 1052.

148 *Id.*

149 *Id.* at 600.

150 *Id.* at 606. See also P. SCHWARTZ, *Questioning the Quantitative Imperative: Decision Aids, Prevention, and the Ethics of Disclosure*, 41 *Hastings Ctr. Rep.* 30 (2011).

151 BERG, *supra* note 147, at 607.

152 *See* G. PREITE, *L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente*, 3 *Rivista Elettronica di Diritto, Economia, Management* 106, 112 (2014).

153 TERRY & FRANCIS, *supra* note 54, at 725.

154 *Id.*

have developed so-called 'workarounds' to avoid [the consent] requirement"[155]. Also, "[i]ndividuals are unable to protect themselves or make informed decisions about whether to share information if they are neither aware that the information is being collected nor aware of how the information will be used once collected"[156]. Drawing a comparison between the United States and the EU, we can see that the first "emphasizes that information must be given to individuals in a covered entity's privacy notices"[157], whereas the latter focuses more "on actual patient understanding of information collection and sharing, depending on individual circumstances", thus establishing more specific requirements[158].

In addition, other factors prevent choices from being completely free. Sometimes the price for opting out is too high and "there is no genuine choice" because "patient "consent" to information sharing is often a nonnegotiable precondition to treatment"[159]. Furthermore, there can be problems related to patients' "limited understanding of key technical and organisational issues pertinent to eHealth", especially with respect to older people[160]. This can lead to "a level of resistance to involvement in eHealth due perhaps to fears about loss of privacy or the perceived inability of authorities to protect privacy"[161]. Also, "in many cases, access and secondary uses of personal information may exceed the scope of what patients, upon disclosure, believe they have consented to"[162]. This shows the importance of considering the degree of patient control over secondary uses of health information as "technology allows for secondary uses far beyond those that patients (or even doctors) anticipate upon disclosure and for which they may not have consented if they had known of them"[163]. It would be burdensome on many uses to require consent every time, also considering the "selection bias" created by informed consent when EHR data is used for research[164], but it would be "dangerous to entirely sacrifice individual autonomy in the decision process"[165]. Unauthorized secondary use of patient data somehow "resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information"[166]. Nevertheless, the traditional confidentiality model does not fit the need for "protecting a person's interests in knowing when personal information will be collected and for what purposes" or remedying "inadequate controls over storage or security of information", or "prevent[ing] discrimination on the basis of a person's health status"[167]. The concerns that we often express in terms of privacy "really

---

155 WICKS, *supra* note 58, at 65 (referring to the English experience).
156 HILLER ET AL., *supra* note 47, at 32.
157 *Id. See* Chapter I, Paragraph 4.1.5.
158 HILLER ET AL., *supra* note 47, at 32.
159 TERRY & FRANCIS, *supra* note 54, at 725.
160 DUQUENOY ET AL., *supra* note 20, at 288.
161 *Id.* (making a comparison with other sectors, such as eCommerce and eGovernment, in which "the issue of privacy has prompted greater efforts to reassure the public so that the potential benefits of the Internet may be more fully exploited"). For an interesting analysis of this issue, see U. IZZO & P. GUARDA, *Sanità Elettronica, Tutela Dei Dati Personali E Digital Divide Generazionale / E-Health, Data Protection And Generational Digital Divide*, Trento Law and Technology Research Group - Research Paper Series (2010), available at: http://eprints.biblio.unitn.it/archive/00001921/ (dealing specifically with possibility of nominating a trusted person who could act as a proxy in the context of EHRs).
162 RIVKIN-HAAS, *supra* note 87, at 178.
163 *Id.* at 182.
164 S. HOFFMAN AND A. PODGURSKI, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 *S. M. U. L. Rev.* 85, 114-19 (2012).
165 RIVKIN-HAAS, *supra* note 87, at 182.
166 D. J. SOLOVE, *A Taxonomy of Privacy*, 154 *U. Pa. L. Rev.* 477, 522 (2006).
167 R. S. MAGNUSSON, *The Changing Legal and Conceptual Shape of Health Care Privacy*, 32 *J. L. Med. & Ethics* 680, 682 (2004).

reflect individuals' desires to maintain control over personal data"[168].

The identification of ways to enhance patient participation and choice without completely losing sight of the underlying interests at stake is a real challenge, which is made even harder by some factors that tend to undermine the patient's freedom. Generally speaking, the provision of health care is a field where the individual is in a position of weakness. This is made even more evident when health data can bear on his or her chance to get a job or sign an insurance contract. Therefore, it is necessary to avoid economic exploitation of health data[169]: the implementation of EHR systems has individual and public health protection as its primary goals, and legal rules should make sure that commercial interests do not undermine these objectives[170]. Indeed, an uninhibited flow of health data for commercial reasons is more likely to lead to stigmatizing or discriminating results[171]. This is why a scholar maintains there should be a general ban on divulging health data from an EHR, as well as a stronger awareness of the risks inherent in the disclosure of health data[172].

Together with the afore-mentioned risks, there are other reasons why self-determination pursued through patient empowerment should not be interpreted as excessively broad. Not only should we adequately take into account the public health interest as well[173], but also we should be aware of the risk of overlooking some fundamental features of the physician-patient relationship. Indeed, this relationship always includes an asymmetry: the physician is the mentor, and the patient is led through the path of health treatment by someone who has spent years toward gaining professional training and expertise[174]. Thus, as much as patients are more and more informed and willing to participate in their own care, they always need a guide: while building PHR architectures allows patients to add data and actively participate, it is necessary to understand how "what is truly inhuman is not the new relationship which could be created through technology, but thinking that the individual could become entrusted with final decisions that need a qualified guide to be taken"[175]. Therefore, the technical structures building up PHRs must be able to "express the legal and social values featuring the ineluctably human physician-patient relationship"[176].

4.3 Using Electronic Health Record Data for Research: Enhancing Individual Freedom Through Accountability

The issues concerning secondary uses of electronic health record data offer an interesting chance to see how tiered, complex and modular solutions are those which best protect individual privacy without sacrificing efficiency.

Two scholars in the United States wrote a paper in 2012 on the balance between privacy, autonomy, and scientific needs in using EHRs for research[177]. Hoffman and Podgurski notice that "[c]omputerization of health information poses new risks of privacy breaches" and creates the risk of other "dignitary harms" such as "group stigmatization due

---

168 RIVKIN-HAAS, *supra* note 87, at 181.
169 *See* IZZO, *supra* note 1, at 810.
170 PEIGNÉ, *supra* note 30.
171 *Id.*
172 *Id.*
173 GUARDA, *supra* note 8, at 230.
174 GUARDA & DUCATO, *supra* note 9, at 419.
175 Id.
176 Id.
177 HOFFMAN & PODGURSKI, *supra* note 164.

to research findings, inability to control whether one's records will be used for objectionable purposes, and a lack of opportunity to share in profits acquired by data users"[178]. They developed a proposal that takes into account these risks as well as the need for researchers to use accurate and up-to-date data. What Hoffman & Podgurski propose is a distinction between interventional and record-based studies: the use of interventional studies for research purposes should depend on consent, whereas the rules on the use of record-based studies should focus on the common good[179]. The underlying argument is that "[w]hen human beings are not subject to any physical or psychological testing in research, and only their records are scrutinized, the value of the common good should prevail over individual interests" and [s]ociety's interests in achieving medical advances should outweigh the individual risks of privacy breaches and non-privacy-related dignitary injuries when all reasonable efforts are made to prevent such harms[180]. Looking at past research abuses (e.g. the Nazi concentration camp experiments), they point out that "electronic-database queries […] present a drastically diminished risk of gross abuses that will inflict acute physical or mental pain"[181].

Therefore, Hoffman and Podgurski make the case that within record-based studies the data subject should not be protected by the requirement of informed consent but rather by other kinds of safeguards. Informed consent seems inadequate for three main reasons[182]. First of all, the process can be extremely burdensome and costly[183]. Secondly, obtaining consent can distort research results by introducing selection bias, therefore we should not "routinely [grant] data subjects a choice concerning inclusion of their records in research"[184]. Thirdly, "while informed consent provides subjects with a choice, it does not provide them with any added protection against privacy breaches"[185].

Hoffman and Podgurski suggest that we should switch from the current "consent-centered ethical framework" to a new conceptual framework where a distinction is operated between research involving only record review and research with clinical testing[186]. In order to balance the individual interests of the data subjects with the common good, measures other than consent must be adopted in order to make record-based research without consent ethically justified[187].

One viable option is the adoption of identity concealment techniques. The article proposes two different techniques: the first one is the creation of "large databases exclusively for research that would include only EHRs that have been de-identified"[188], whereas the second approach is a "secure statistical analysis of distributed databases, which

---

178 *Id.* at 89. *See also id.* at 107-08 on group stigmatization (it "may occur if researchers find that individuals with particular ancestry are more vulnerable to a specific illness than other groups or have better outcomes with treatment that is different from standard therapy"); *id.* at 108 on moral objections (e.g., "[a] patient who opposes abortion may find it abhorrent to have her medical file play a role in [a research on fetal abnormalities that can be discovered in-utero], even if it is merely subejct to an automated query as part of a large database of de-identified files [but] without an informed consent process, she will be given no choice in the matter"); *id.* at 108-09 on the lack of share in commercial profits.

179 *Id.* at 124.

180 *Id.* at 124-25.

181 *Id.* at 90. *See also id.* at 109-11.

182 *Id.* at 90.

183 *Id.* at 90. The article shows the shortcomings and risks for the different ways of seeking consent. *Id.* at 119-23.

184 *Id.* at 114. *See id.* at 114-19.

185 *Id.* at 90.

186 *Id.* at 124.

187 *Id.* at 90.

188 *Id.* at 90-91. *See id.* at 128-31.

allows researchers to query the EHR databases of medical facilities or trusted aggregators, but enables them to receive only summary statistics in response"[189].

Another safeguard the article recommends is additional oversight, performed by an ethics board[190]. This "tiered review process" is meant to "apply some degree of scrutiny to all research projects"[191], because "all record-based studies [should] undergo approval by an ethics board with expertise in non-interventional research and in information security"[192]. We consider this recommendation particularly insightful inasmuch as it envisions a way to take into account privacy interests that is different from traditional consent and that is a more attentive balance of the interests at stake. Within this proposal, the processing of health data for research does not rely on automated operations but rather is grounded on decisions taken by human beings, who can be held accountable. This allows all the subjects involved in the processing to be constantly aware of the sensitivity of the data they are dealing with. The degree of scrutiny that ethics board should apply depends on the depth of the re-identification risk and on the severity of the potential harm[193]. This risk-based approach is really the kind of approach that should be adopted in this field[194]. Furthermore, the article aptly advises that even research protocols that only involve de-identified data should be subject to this additional scrutiny[195]. As we will see in Chapter III, anonymization techniques usually cannot rule out de-identification risks, especially if the data set needs to include enough information for it to be useful for research. Also, if de-identified information is used in research without the subjects' consent, they "will likely not have opportunities to opt out of studies that could conceivably lead to stigmatization of groups with which they strongly identify"[196]. Another feature of this proposal that deserves our appreciation is that it deems it "essential for ethics boards to conduct continuing review of all research studies"[197]: due to the quick changes in technology and in the circumstances, risk assessment can never be a one-shot operation. Additionally, there should be an oversight by HHS, which "should be authorized to conduct unannounced audits of all research projects, including those using de-identified data"[198].

The third recommendation concerns replacing consent in record-based research studies with enhanced notification and education, which, "like consent, can demonstrate

---

189 *Id.* at 91. *See id.* at 131-33.

190 *Id.* at 91.

191 *Id.* at 133. *See also* Institute of Medicine (IOM), Committee on Health Research & the Privacy of Health Information: The HIPAA Privacy Rule (S.J. NASS ET AL., eds.), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* 247 (2009), available at: http://www.aisp.upenn.edu/wp-content/uploads/2015/03/BeyondHIPAAPrivacyRule_EnhancingPrivacy_ImprovingHealthThroughResearch_2009.pdf (proposing a similar approach whereby researchers who want to use direct identifiers for their studies and who do not want to seek consent would ask for approval from an ethics oversight board). Hoffman and Podgurski argue that the IOM's proposal "does not go far enough" because it does "not take into account the multiplication of risk that occurs when de-identified health information is promulgated to more and more research groups, each of which is a point of potential vulnerability to security and privacy violations" and does not consider "the highly changeable nature of security threats". HOFFMAN & PODGURSKI, *supra* note 164, at 134.

192 *Id.* at 135.

193 *Id.* at 135.

194 *See id.* at 135. Studies using identifiers (including limited data sets) should undergo a thorough approval process, whereas studies which use de-identified data should undergo a streamlined process coupled with the promise by the researchers that they will not attempt to re-identify data, will not disseminate the records outside the research team, and will not use data for purposes outside the scope of the research. *Id.*

195 *Id.* at 91.

196 *Id.* at 107-08.

197 *Id.* at 136.

198 *Id.*

researchers' respect for human subjects and promote a sense of autonomy"[199]. As to notice, the article proposes "expanding the HIPAA Privacy Rule notice requirement to apply to all research uses"[200], whereas the current rules require notice only with respect to identifiable data[201]. At the same time, education campaigns should be launched by HHS and research institutions in order to gain public trust[202]. This measure, too, enhances awareness and replaces consent with an approach even more respectful of human freedom. Indeed, under this approach human autonomy is more respected by arming data subjects with knowledge rather than settling for a so-called "check the box". Hoffman and Podgurski argue that notice and education "can empower data subjects in other ways", such as acting through the democratic process[203]. Furthermore, they argue that "[t]ransparency and accountability on the part of researchers should prevent data subjects from suffering serious research abuses and should inspire enthusiasm about biomedical research"[204], also in light of the fact that history shows that "abuses occurred when data subjects were vulnerable because of ignorance, poverty, or imprisonment"[205].

We have analyzed this proposal in depth because of the importance of secondary uses of health data, but especially because of the nuanced, complex approach it adopts. This kind of perspective focuses on risk assessment rather than reliance on black-or-white rules, and ultimately enhances the importance of human judgment.

5. Electronic Health Records in Europe

The EU legal framework has been said to have "made more significant progress towards the dual goals of effective implementation of EHRs and the protection of individual privacy through enabling patient control"[206]. This is largely due to the fact that within the EU standard, which "begins with the presumption of privacy for sensitive health records", "the patient should always have the right to prohibit transfer of health information that is in an electronic system" and "foreign recipient of EHRs must agree to abide by the basic rules of EU protection of personally identifying health records"[207]. EHR systems must then prove themselves to meet such standards, which "could serve to calm consumer concerns"[208].

A major problem in the implementation of EHRs in the European Union is the fact that legal frameworks and traditions vary widely among the Member States[209], but "[i]t has become increasingly clear that the eHealth keyword *interoperability* does not only concern technological and semantic standards, but also legal, ethical, social, cultural and organizational aspects"[210]. Some European countries "have set detailed requirements as to the content of EHRs", whereas "others do not specify what should be this content"[211]. However, this "does not seem to constitute an obstacle for interoperability between EHR

---

[199] *Id.* at 91.
[200] *Id.* at 139.
[201] *Id.* at 141.
[202] *Id.* at 140-41.
[203] *Id.* at 139.
[204] *Id.* at 91.
[205] *Id.* at 141.
[206] HILLER ET AL., *supra* note 47, at 36.
[207] *Id.* at 38.
[208] *Id.*
[209] *See* E. RYNNING, *Public Trust and Privacy in Shared Electronic Health Records*, 14 *European Journal of Health Law* 105, 109 (2007).
[210] *Id.* at 107.
[211] Report on EHRs in the EU Member States, at 7.

systems"[212].

5.1 The Article 29 Working Party Working Document on Electronic Health Records: the Legal Framework and the Guidelines

In 2007, the Article 29 Working Party wrote a report that "provides an interpretation of the application of privacy principles to electronic health records" recommending the adoption of legal protections[213]. This guidance was very useful insofar as "many health care players do not always seem to know how to comply with the Data Protection Directive"[214].

The report begins by stressing that "data processing systems are designed to serve man"[215], and goes on to list the relevant provisions with respect to the fundamental right to the protection of personal data[216]. Indeed, data controllers in the context of EHR systems must fall within the general framework and comply with the data protection principles of use limitation, data quality, and retention, as well as with the information requirements, the data subject's right of access, and the security related obligations[217]. Furthermore, the report highlights that data contained in EHRs must be considered "sensitive personal data" pursuant to the Directive, and thus be subject to the general prohibition on processing with the exceptions we have analyzed[218]. This offers the chance for us to consider again the provisions set out by the Directive looking more specifically at the realm of EHRs.

The first exception to the general ban is the consent of the data subject[219]. The Article 29 Working Party stresses that "[a]ny consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as free", because if the data subject "has not had the opportunity to make a genuine choice or has been presented with a *fait accompli*" his consent is not valid[220]. The report provides some more guidance: the processing of personal data in an EHR system usually cannot be legitimized through consent, as "[r]eliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment"[221]. Consent must not only be free, but also specific and informed. Consent cannot be considered specific if there is "a 'general agreement' of the data subject e.g. to the collection of his medical data for an EHR and to subsequent transfers of these medical data of the past and of the future to health professionals involved in treatment", and it is only "informed" if it is "based upon an appreciation and understanding of the facts and implications" of the action, as the individual is given "accurate and full information of all relevant issues" including "an awareness of the consequences of not consenting to the processing in question"[222]. Even if it is complicated to obtain consent, especially where direct contact between the data controller and the data subjects is impossible, the data controller must be able to prove that he has obtained the explicit consent and that it "was given on the basis of sufficiently precise information"[223].

---

[212] *Id.*
[213] HILLER ET AL., *supra* note 47, at 21. *See also* CALLENS, *supra* note 4, at 576-77.
[214] CALLENS, *supra* note 4, at 576.
[215] Data Protection Directive, Recital 2.
[216] Article 29 WP Working Document 2007 on EHR, at 6. *See* Chapter I, Paragraph 2.2.
[217] Article 29 WP Working Document 2007 on EHR, at 6-7.
[218] *Id.* at 7-8.
[219] Data Protection Directive, Article 8(2)(a). *See* Chapter I, Paragraph 2.4.2.
[220] Article 29 WP Working Document 2007 on EHR, at 8.
[221] *Id.* at 8-9.
[222] *Id.* at 9.
[223] *Id.*

Under Article 8(2)(c)[224], the processing of health data can also be justified if it is necessary to protect the vital interest of the data subject or of another person: in the medical context, this regards "life-saving treatment[s] in a situation where the data subject is not able to express his intentions"[225]. The Article 29 Working Party clarifies this with an example: if a data subject loses consciousness after an accident and cannot give his consent to the disclosure of allergies, a health professional could access the data in an EHR in order to retrieve relevant information[226].

Article 8(3) allows for the processing of health data under three conditions[227]. First, the processing must be for the specific purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services"[228]. Thus, "further processing which is not required for the direct provision of such services, such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims" is not covered[229]. Secondly, the processing must be "required" for such specific purposes, which "means in an EHR context that any inclusion of personal data in an EHR would have to be fully justified": mere usefulness is not sufficient[230]. The third condition is that the processing is performed "by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy"[231].

The Working Party stresses that this exception must be interpreted in a restrictive way and that "[w]here the processing of personal data in an EHR goes in any way beyond these purposes or does not meet the said conditions, then Article 8(3) cannot serve as the sole legal basis for the processing"[232]. Anyways, even if all the conditions are met, the "new risk scenario" created by EHRs "calls for new, additional safeguards as counterbalance"[233]. The increased chances of patient data interception make the traditional legal standard of confidentiality insufficient, because "the obligation of medical professionals to confidentiality […] may no longer be fully applicable in an EHR environment, as one of the purposes of EHR is to grant access to medical documentation for the sake of treatment to such professionals who have not been party to the previous treatment documented in a medical file"[234].

Another exception is represented by Article 8(4), which allows Member States to establish further derogations in a "special legal basis" and "justified by reasons of substantial public interest"[235]. According to the Article 29 Working Party, the arguments for implementing EHR systems may be considered "substantial public interest", as some Member States feature a constitutional right to health protection[236].

After clarifying the data protection framework, the report offers some guidelines on a suitable legal framework for EHRs, looking at the "topics where special safeguards […]

---

224 Data Protection Directive, Article 8(2)(c). *See* Chapter I, Paragraph 2.4.2.
225 Article 29 WP Working Document 2007 on EHR, at 9.
226 *Id.* at 9-10.
227 *Id.* at 10. Data Protection Directive, Article 8(3).
228 Data Protection Directive, Article 8(3). *See* Chapter I, Paragraph 2.4.2.
229 Article 29 WP Working Document 2007 on EHR, at 10.
230 *Id.*
231 Data Protection Directive, Article 8(3). *See* Chapter I, Paragraph 2.4.2.
232 Article 29 WP Working Document 2007 on EHR, at 11.
233 *Id.*
234 *Id.* at 11-12.
235 *Id.* at 12.
236 *Id.* at 13.

seem particularly necessary"[237].

The first safeguard is the respect for a patient's self-determination concerning when and how data are used: an agreement as a safeguard does not need to meet all the requirement for consent, as "it could – depending on the situation – also be offered in form of an opt-out/ a right to refuse"[238]. Also, since different types of health data have a varying damage potential, there should be different degrees of the right to exercise self determination, through "an incremental system of opt-in requirements […] and opt-out possibilities for less intrusive data"[239]. Generally speaking, a patient should always have the possibility to prevent disclosure of his health data by a health professional to another[240].

Secondly, "[r]eliable identification of patients in EHR systems is of crucial importance", as well as forbidding access to unauthorized persons[241]. Uniquely identifying and properly authenticating users is extremely important insofar as "one of the main advantages of EHR systems is their availability for access by electronic communication irrespective of time and location"[242].

As a third safeguard, the Working Party deals with authorization for accessing EHR in order to read and make entries in it[243]. The essential principle must be that only health care professionals or authorized personnel who are in a relationship of actual and current treatment with the patient can access the record[244]. The Working Party further advises the implementation of "modular access rights", i.e. "forming categories of medical data in an EHR system with the consequence that access is limited to specific categories of health care professionals/institutions"[245]. Modular, complex frameworks are generally a better fit for data protection than black-or-white distinctions, as we have discussed. Furthermore, the report takes the stand that a patient should be able to prevent access to his EHR[246].

The fourth guideline the report provides concerns the use of electronic health records for purposes other than those mentioned in Article 8(3): it should in principle be prohibited to enhance citizens' trust in the confidentiality of the system[247]. This would exclude access by medical practitioners acting as experts for third parties like insurance companies[248]. The Working Party further advises that "[s]pecial measures should be taken to prevent that patients are illegally induced to disclose their EHR data", through "[e]ducation of the patient" as well as technical measures[249].

According to the report, an exception to this general prohibition could be carved out for the processing of EHR data for medical scientific research and government statistics, provided that there is compliance with the Directive[250]. Otherwise, further uses of EHR data should be allowed only if it is in anonymized or pseudonymized data[251]. As to the legal rules concerning the processing of personal health data for purposes other than treatment, such as research and quality review, "[b]etter and more specific provisions […] are needed,

---

237 *Id.*
238 *Id.* at 13-14.
239 *Id.* at 14.
240 *Id.*
241 *Id.*
242 *Id.* at 15.
243 *Id.*
244 *Id.*
245 *Id.*
246 *Id.*
247 *Id.* at 16.
248 *Id.*
249 *Id.*
250 *Id.*
251 *Id. See* Chapter III.

as the use of such data takes place increasingly within a globalized context of health care actors"[252]. As "globalization in health care has become a reality", the situation "requires more harmonized rules for health data processing, particularly as the exchange of data between European e-health actors will not be limited to the treatment of patients", but also "for evaluation, research or statistical purposes"[253].

With respect to the data stored in an EHR, the Working Party identifies several issues. A major issue is deciding which categories of data should be stored and for how long, as "[c]ompleteness of a health file is practically impossible and also not desirable", as "[o]nly relevant information should be entered into an EHR"[254]. Also, the Working Party suggests that it might be useful to implement different data modules with different access requirements, as each category may require a different degree of confidentiality[255].

The Working Party also provides some guidelines regarding data security: access should only be possible to authorized persons in order for the system to be acceptable[256]. Thus, the ideal EHR legal framework should require the implementation of technical and organizational measures in order to avoid loss and unauthorized processing and guarantee integrity[257]. Privacy enhancing technologies (PETs) should be used as much as possible, and security measures should be designed in a user friendly way[258]. More specifically, the Working Party clarifies the necessity of:

- developing a reliable and effective system of identification and authentication;
- documenting all processing steps which have taken place, especially access requests;
- securing the content of the system via effective backup and recovery mechanisms;
- preventing unauthorized access to or alteration of data;
- giving clear instructions to all authorized employees;
- clearly distinguishing functions and competences concerning the categories of persons involved with the system and establishing liabilities;
- regularly performing internal and external data protection auditing[259].

Another recommendation by the Working Party is enhanced transparency about the content and functioning of the system, in order to generate trust[260]. To this end, the system "must also guarantee that the possible infringements of privacy […] are adequately balanced by liability for damages caused e.g. by incorrect or unauthorized use of EHR data"[261]. Member States must then conduct careful assessments to identify the most significant liability issues[262].

At the same time, "effective control mechanisms for evaluating the existing safeguards are necessary"[263]. First, disputes about the correct use of EHR data should be dealt with via a special arbitration procedure[264]. Secondly, access requests should be handled by a single special institution, in order to fully enable data subjects to exercise their access rights[265].

---

252 CALLENS, *supra* note 4, at 578.
253 *Id.* at 578-79.
254 Article 29 WP Working Document 2007 on EHR, at 18.
255 *Id.*
256 *Id.* at 19.
257 *Id.*
258 *Id.*
259 *Id.* at 20.
260 *Id.*
261 *Id.*
262 *Id.*
263 *Id.* at 21.
264 *Id.*
265 *Id.*

Thirdly, data subjects should always be informed as to when and why data is accessed, and a special mechanism must be designed[266]. Last, there must be "[r]egular internal and external data protection auditing of access protocols"[267].

5.2 EHR Organizational Structures and Models

The Article 29 Working Party identified three possible organizational alternatives for storing data in an EHR[268]. Despite the Commission's focus on interoperability, there are strong national peculiarities[269], which the Working Party splits into three categories: decentralized storage, centralized storage, and storage under the control of the data subject[270]. While not requiring that any one model be adopted, the report "identifies privacy considerations for each type"[271]. We can still look at the Article 29 Working Party's opinion to get a general framework despite the fact that it was written in 2007.

5.2.1 Decentralized Model

The first model is the decentralized storage model, where the individual health records are kept on the IT systems of every health care provider and institution and where they are connected through a repository[272]. Via this national switch point, the health care provider can access other health records[273]. Because of the complexity of such a system, countries opting for the first model have typically established a new legal framework "simultaneously with the roll-out of government initiated eHealth infrastructures such as eHealth platforms, National Switch Points and Reference Directories"[274]. For example, in Belgium, an "eHealth Platform" was created in 2008 to establish a "secure electronic exchange of patient information, provid[ing] care and electronic prescriptions between all relevant healthcare actors": it is a public institution, managed by representatives of the stakeholders in the healthcare sector[275]. It does not change the division of tasks, nor does it store information in a central way[276]. Rather, it just provides basic services, such as "integrated user and access management, orchestration of electronic processes and a portal environment including a management system", as well as a reference directory[277]. Another example we can look at is Germany, where doctors who prefer to store the data electronically must observe special rules of the medical professional code and recommendations of the German medical assembly, including "actions to protect the data against unauthorized modification, destruction or utilization and the use of digital signatures and qualified digital time stamps"[278]. Furthermore, in Germany health data can be filed via an electronic health card and the Health Professional Card, in principle

---

266 *Id.*
267 *Id.*
268 Article 29 WP Working Document 2007 on EHR, at 17.
269 DUMORTIER & VERHENNEMAN, *supra* note 31, at 26. For an overview of the different European initiative, see STACCINI ET AL., *supra* note 25, at 326-34.
270 Article 29 WP Working Document 2007 on EHR, at 17.
271 HILLER ET AL., *supra* note 47, at 35.
272 DUMORTIER & VERHENNEMAN, *supra* note 31, at 37.
273 *Id.*
274 *Id.* at 50.
275 *Id.*
276 *Id.*
277 *Id.*
278 *Id.* at 38 (citing Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, published in 105 Deutsches Ärzteblatt (DtÄBl.) 19, p. A1026 of May, 9th 2008).

controlled by the patient, who in his storage area (Patientenfach) can add information[279].

5.2.2 Centralized Model

The second structure is the centralized storage model, featuring "a uniform system of storage, to which medical professionals have to transfer their documentation"[280]. The main advantage would be "higher technical security and availability", as "[t]here will be a single controller for the whole system separate from the healthcare professionals/institutions who forwarded their documentation […] to the central system"[281]. However, there is a "higher potential of misuse": "[s]pecial arrangements and security measures […] could be foreseen in order to balance the security risks", but "liability for the confidentiality of the system is taken out of the hands of medical professionals which might influence the amount of trust invested by the patients into such a system"[282]. This model has been particularly employed in Scandinavian countries, which "prefer to centrally store a national electronic health record for each individual because it simplifies planning, monitoring and managing healthcare"[283]. In Finland, the Act on Electronic Handling and Archiving of Electronic Healthcare Records[284] required the Social Insurance Institution KELA to provide services for handling electronic patient information[285]. The Act makes it mandatory to incorporate all public health care units into the electronic archiving system, as the government "judged that structurally uniform entry, storage and transfer of data make data easier to be retrieved and easier to reuse" and decided to "enable patients to view data and participate in their medical treatment", which will "increase their confidence in the system"[286].

5.2.3 France: Storage Under the Control of the Data Subject

The third alternative is storage under the control of the data subject, who is then "master of his own medical records"[287]. This is "the best solution in terms of self determination", but features some problems with respect to "accuracy and completeness"[288]. This patient-centred model is the French approach. The Dossier Médical Personnel (DMP) was introduced in France within the Health Insurance Reform Act in August 2004[289] "because of sharp increases in medical costs as well as a growing awareness of the lack of coordination between hospitals and private physicians"[290]. The DMP was financed by the French government, "in anticipation of the amount of money the DMP [would] save in health care expenditures, as well as advertising and partnership arrangements"[291]. This tool "consists of a storage system of health data for esach beneficiary of the compulsory health insurance system"[292]. We can call the French

---

[279] *Id.*
[280] Article 29 WP Working Document 2007 on EHR, at 17.
[281] *Id.*
[282] *Id.*
[283] DUMORTIER & VERHENNEMAN, *supra* note 31, at 51.
[284] Finland – Client Data Act 2007/159.
[285] DUMORTIER & VERHENNEMAN, *supra* note 31, at 39.
[286] *Id.*
[287] Article 29 WP Working Document 2007 on EHR, at 17.
[288] *Id.*
[289] France, Healthcare Insurance Act no. 2004-810 of 13 August 2004.
[290] GRADY, *supra* note 49, at 386.
[291] *Id.* at 394.
[292] GUARDA (2015), *supra* note 1, at 35.

approach "patient-centered", as under the initial regulations the patient could choose a service provider to host his electronic health record and request his healthcare provider to update it[293]. Thus, the electronic health record was created by a certified host chosen by the patient, and legal rules[294] were established for the certification of host providers[295]. Healthcare professionals were bound by the patient's choice for a certain provider and need to report elements to the record. This policy proved to be ineffective in practice, so in 2009 it was decided to centralize the Dossier and host the files centrally[296]. This would be carried out through the creation of a specific national agency called ASIP Santé, which "defines the DMP as a national and secured [personal electronic health record] accessible on the Internet by patients and healthcare professionals"[297]. The approach continues to be patient-centered, though, because "[i]t is still the patient who decides on the creation of the record, who manages the record and who administers the access thereto"[298]. Indeed, "[t]he DMP is a public service freely accessible to all the beneficiaries of the national health insurance" and "not mandatory"[299]. The implementation of this project in France is still incomplete, since despite the initial goal of having 5 million dossiers by 2013, there were only about 420,000 in January 2014[300]. Very recently, a new project has been launched introducing the Dossier Médical Partagé (i.e., shared), created only with the express consent of the person ("*créé sous réserve du consentement exprès de la personne*")[301]. The goal is allowing the health care professionals and patients to have access to all the health information at any time[302]. The project looks quite similar to the Italian framework, described below.

5.2.4 England and Other Projects

Another experience we can look at is the English one[303]. The Department of Health gave birth to a National Programme for IT in 2002, aiming at providing comprehensive electronic patient records[304] within the so-called NHS Care Record Service. The projects "are divided into five geographical areas to limit the risk of an industrialist or a system failure"[305]. There were some delays in the implementation, however, due to technical

---

293 DUMORTIER & VERHENNEMAN, *supra* note 31, at 40.

294 France, Healthcare Insurance Act no. 2004-810 of 13 August 2004, Article R. 1111-9.

295 DUMORTIER & VERHENNEMAN, *supra* note 31, at 40.

296 *Id.* at 40-41 (citing eSante´ France, "The DMP: a project that is structuring the development of e-health in France", http:// esante.gouv.fr (last accessed 9 April 2012); CNIL, "La CNIL authorise le de´ploiement du dossier me´dical personnel sur l'ensemple du territoire", http://www.cnil.fr; France2, "Le Dossier me´dical personnel lance´ jeudi", 15 December 2010, http://info.france2.fr/france/le-dossier-medical-personnel-lance-jeudi-66405648.html).

297 STACCINI ET AL., *supra* note 25, at 331.

298 DUMORTIER & VERHENNEMAN, *supra* note 31, at 41. *See also* GUARDA, *supra* note 8, at 67-70.

299 STACCINI ET AL., *supra* note 25, at 331.

300 V. MASSON, *Le dossiér medical personnel fait peau neuve*, Le Figaro, October 16, 2015, available at: http://www.lefigaro.fr/conjoncture/2015/10/16/20002-20151016ARTFIG00097-le-dossier-medical-personnel-fait-peau-neuve.php.

301 *See* V. GRANIER, *Un avant-projet de décret sur le futur DMP soumis à concertation*, January 6, 2016, available at: http://www.ticsante.com/print_story.php?story=2795; C. POPPE, *JuriS-feuilleton – Le projet de loi, épisode 13: Le dossier médical partagé (DMP)*, December 14, 2015, available at: http://www.jurisante.fr/?p=3963.

302 POPPE, *supra* note 301.

303 *See* C.N. MCCUBBIN, *Legal and Ethico-legal Issues in E-healthcare Research Projects in the UK*, 62 *Social Science & Medicine* 2768 (2006); T. SALEEM, *Implementation of HER/EPR in England: a model for developing countries*, in *Journal of Health Informatics in Developing Countries*, 2009 vol. 3, n. 1, 9.

304 WICKS, *supra* note 58, at 60.

305 STACCINI ET AL., *supra* note 25, at 328.

difficulties as well as to citizen concerns about security and consent[306]. A strategy for a reform was published with a white paper in 2010[307]. The first stage of this ambitious plan, which "benefit[s] from the largest public IT budget allocated by a government"[308], is the Summary Care Record, i.e. an electronic summary of key medical data, taken from the patient's electronic record already held by his general practitioner[309]. Initially, the content is limited to basic information but is later supposed to include diagnoses and other types of information[310]. The patient can choose whether he wants to create a Summary Care Record, whether he wants it to be accessible to other health professionals, and what information can be included[311]. Together with the Summary Care Record, the English plan includes HealthSpace[312], which is a personal health organizer "through which patients can store their own health data and connect to their Summary Care Record"[313].

After the first attempt, England has initiated a new project for the integration of health records with the policy paper "Personalised health and care 2020: a framework for action", published on November 13, 2014[314].

Also, we can mention some projects born in Europe, such as the epSOS Project (Smart Open Services for European Patients), started in July 2008 and aiming at realizing an electronic service of exchange of health data[315]. Twelve EU Member States have joined this project, which attempts to build up a practical solution allowing the secure exchange of personal data among the different national e-Health systems[316].

5.3 The e-Commerce Directive

When a health care actor utilizing eHealth is considered to be providing information society services, it must comply with the so-called e-Commerce Directive[317]. This Directive applies to information society services, i.e., any service normally provided for remuneration, at a distance, by electronic means, for the processing and storage of data, and at the individual request of a recipient of a service. Under the Directive, eHealth actors acting as an information society service must provide the recipient of the service and competent authorities with easily, directly and permanently accessible information on the service providers and, where their activity is subject to an authorization scheme, the particulars of the relevant supervisory authority, any professional body or similar institution with which they are registered, as well as which professional titles they have obtained, which Member State has granted these titles, which applicable professional rules in the Member State of establishment are applicable and what means exist to access them[318]. Under Article 4 of the e-Commerce Directive, "Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made

---

306 WICKS, *supra* note 58, at 60-61.
307 *Id.* at 61. The White Paper is available at www.dh.gov.uk/en/Healthcare/ LiberatingtheNHS/index.htm.
308 STACCINI ET AL., *supra* note 25, at 329.
309 WICKS, *supra* note 58, at 61.
310 *Id.*
311 GUARDA, *supra* note 8, at 73.
312 *See* www.healthspace.nhs.uk.
313 WICKS, *supra* note 58, at 61.
314 ENGLAND, DEPARTMENT OF HEALTH, *Policy Paper – Personalised health and care 2020: a framework for action*, November 13, 2014, available at: https://www.gov.uk/government/publications/personalised-health-and-care-2020/using-data-and-technology-to-transform-outcomes-for-patients-and-citizens.
315 GUARDA, *supra* note 8, at 23. *See* http://www.epsos.eu/epsos-home.html.
316 *Id.* at 24.
317 E-Commerce Directive (2000/31/EC).
318 CALLENS, *supra* note 4, at 567.

subject to prior authorisation or any other requirement having equivalent effect"[319].

5.4 Cross-border Interoperability and International Data Transfers

Cross-border transfers of data are a major issue, especially if we consider that an interconnected market is one of the main goals of the European Union. This creates an increasing need for interoperability between the different national EHR systems, which "should make access easier, and enhance the quality and safety of patient care throughout the Community by providing patients and health professionals with relevant and up-to-date information while ensuring the highest standards of protection of personal data and confidentiality"[320]. The European Commission has issued a recommendation on this topic, as it considered "[l]ack of interoperability of electronic health record systems" as "one of the major obstacles for realising the social and economic benefits of eHealth in the Community"[321]. The achievement of greater interoperability does not necessarily require harmonization of Member State laws and regulations[322], but obviously this is the direction we are moving toward with the new GDPR. The Recommendation invited Member States "to undertake actions at five levels, namely the overall political, the organisational, the technical, the semantic and the level of education and awareness raising"[323]. Obviously, the pursuit of greater interoperability should not be at the expense of privacy protection[324], as "interoperable [EHR] systems increase the risk that personal data concerning health could be accidentally exposed or easily distributed to unauthorised parties" [325]. Thus, the Recommendation states that "Member States should lay down a comprehensive legal framework for interoperable [EHR] systems" that "should recognise and address the sensitive nature of personal data concerning health and provide for specific and suitable safeguards so as to protect the fundamental right to protection of personal data of the individual concerned"[326].

The issue of the interoperability of EHR systems among the different EU Member States leads us to consider what happens when data are transferred to other countries. The Commission has the power to determine whether "a third country ensures an adequate level of protection […] by reason of its domestic law or of the international commitments it has entered into"[327]. If such a decision is made[328], personal data can flow to such country with no need for any further safeguard.

The most famous instance of such a decision regards the Safe Harbor Principles,

---

[319] E-Commerce Directive, Article 4(1) (followed by the clarification that "[p]aragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services", id., Article 4(2)).

[320] European Commission Recommendation on cross-border interoperability of EHR systems, Recital 3.

[321] *Id.*, Recital 4.

[322] *Id.*, Recital 3.

[323] *Id.*, Paragraph 4(a). *See id.*, Paragraph 5 (political level); Paragraph 6 (organizational level); Paragraph 7 (technical level); Paragraph 8 (semantic level); Paragraph 17 (education and awareness raising level).

[324] *Id.*, Paragraph 10.

[325] *Id.*, Paragraph 12.

[326] *Id.*, Paragraph 14.

[327] Data Protection Directive, Art. 25(6).

[328] This decision entails: a proposal from the Commission, an opinion by Member States' data protection authorities and the European Data Protection Supervisor in the framework of the Article 29 Working Party, an approval from the "Article 31 Committee" (composed of representatives of Member States) under the comitology "examination procedure", and the adoption of the decision by the College of Commissioners.

concerning the transfer of personal data from the EU to the U.S, which is "an essential element of the transatlantic relationship" considering that "[t]he EU and the United States are each other's most important trading partners"[329]. In 2000, the European Commission adopted a decision recognizing the Principles as providing adequate protection[330]. A decade and a half later, however, in a landmark ruling, this decision was declared invalid by the Court of Justice on October 6, 2015[331].

The Safe Harbor Principles were issued by the U.S. Department of Commerce, which developed such principles "in consultation with industry and the general public to facilitate trade and commerce between the United States and the European Union"[332]. The 2000 decision by the Commission "allow[ed] free transfer of personal information from EU Member States to companies in the US which have signed up to the Principles in circumstances where the transfer would otherwise not meet the EU standards for adequate level of data protection given the substantial differences in privacy regimes between the two sides of Atlantic" [333]. Indeed, the functioning of this arrangement "relie[d] on commitment and self-certification of adhering companies", who could freely choose to sign up and would then be bound by the obligations[334]. Essentially, whenever a company wanted to adhere to the Safe Harbor Principles, it had to "identify in its publicly available privacy policy that it adheres to the Principles and actually does comply with the Principles", and "self-certify i.e., declare to the US Department of Commerce that it is in compliance with the Principles"[335]. Since this mechanism was "based on the voluntary adherence of companies, on [their] self-certification […] and on enforcement of the self-certification commitments by public authorities", clearly "any lack of transparency and any shortcomings in enforcement [could] undermine the foundations on which the […] scheme [was] constructed"[336]. After the revelations on the US surveillance programs, the "divergent responses of data protection authorities […] demonstrate[d] the real risk of the fragmentation of the Safe Harbour scheme and raise[d] questions as to the extent to which it [was] enforced"[337]. These shortcomings were the ones that led to the ruling by the Court of Justice.

On October 6, 2015, as we previously hinted at, the Court of Justice of the European Union, in an effort to "reaffirm the importance of the fundamental right to protection of personal data"[338], invalidated the adequacy decision concerning the Safe Harbor Principles. The Court "clarified that legislation permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as

---

[329] European Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) COM(2015) 566 final (November 6, 2015) [hereinafter European Commission Communication on the Schrems decision], at 2.

[330] Commission Decision 2000/520/EC pursuant to European Parliament and Council Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 No. L215/7.

[331] Judgment of 6 October 2015 in Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, EU:C:2015:650.

[332] CALLENS, *supra* note 4, at 565.

[333] European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, (November 27, 2013), at 2.

[334] *Id.*

[335] *Id.* at 3.

[336] *Id.* at 5.

[337] *Id.*

[338] European Commission Communication on the Schrems decision, at 2.

compromising the essence of the fundamental right to respect for private life"[339]. Furthermore, the ruling also highlighted that, even in the presence of an adequacy decision, the Member States' DPAs "remain empowered and obliged to examine, with complete independence, whether data transfers to a third country comply with the requirements laid down" by the Directive and by the Charter of Fundamental Rights[340].

While there were several discussions as to whether we would ever have a "Safe Harbor 2.0", as "the Commission consider[ed] that a renewed and sound framework for transfers of personal data to the United States remain[ed] a key priority"[341], the Commission has endeavored to clarify under which conditions transatlantic data transfers can continue. The viable options are mainly represented by Standard Contractual Clauses (SCCs) and, for transfers between the different entities of a multinational corporate group, Binding Corporate Rules (BCRs)[342]. These alternative methods, if compared to adequacy decisions, "have both a more limited scope (as they apply only to specific data flows) and a broader coverage (as they are not necessarily confined to a specific country)"[343]. With respect to contractual clauses, the Commission "has approved, in accordance with Article 26(4) of the Directive, four sets of SCCs considered as fulfilling the requirements of Article 26(2)" and that "[lay] down the respective obligations of data exporters and importers"[344]. These model clauses also require that EU data subjects are allowed to "invoke before a DPA and/or a court of the Member State in which the data exporter is established the rights they derive from the contractual clauses as a third party beneficiary"[345]. Whenever a Member State has a system of notification and/or pre-authorization for the use of the SCCs, "the national DPA has to compare the clauses actually contained in the contract […] with the SCCs and verify that no change has been made"[346]. As to intra-group transfers, a multinational company can adopt BCRs, which allow a free flow of personal data among the various entities of a corporate group[347]. The Article 29 Working Party "has spelled out the substantive […] and procedural […] requirements for BCRs based on EU data protection standards"[348]. Similarly to the SCCs, BCRs are both "binding on the members of the corporate group" and "enforceable in the EU" as they allow individuals to lodge a complaint before a DPA or bring an action before a Member State court as third-party beneficiary[349].

Outside of these mechanisms, data transfers to third countries are possible within the derogations set out in Article 26(1) of the Directive, namely the data subject's unambiguous

---

339 *Id.* at 3.
340 *Id.*
341 *Id.* at 15.
342 *Id.* at 4. *See* Statement of the Article 29 Working Party, October 16, 2015, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.
343 European Commission Communication on the Schrems decision, at 5.
344 *Id.* at 6. Two of these sets regard transfers between controllers, whereas the other two relate to transfers between a controller and a processor. *Id.*
345 *Id.*
346 *Id.* at 6-7. Under the proposed GDPR, if SCCs or BCRs have been "adopted by the Commission or in accordance with the envisaged consistency mechanism", there shall be no need for any further authorization. *Id.* at 7, fn. 13.
347 *Id.* at 7.
348 *Id.* at 8. *See* European Union Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (WP 153), 24 June 2008.
349 European Commission Communication on the Schrems decision, at 8.

consent or the pursuit of other goals[350]. These other goals include the compliance with a contractual obligation, important public interest grounds, and the protection of the vital interests of the data subject[351].

On February 2, 2016 the European Commission and the United States agreed on a new framework for transatlantic data flows, called the "EU-US Privacy Shield"[352]. This new agreement is supposed to reflect the requirements set out in the Schrems decision, as it "will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities"[353]. Furthermore, the United States committed to subjecting the possibilities for public authorities to access personal data to clear limitations and oversight[354]. A new Ombudsperson will be created to deal with complaints on access by national intelligence authorities[355].

It is still yet to be clarified whether this agreement meets the requirements set out by the Court of Justice of the EU, especially because no formal text was accompanying the announcement. The Article 29 Working Party made a comment and "welcomes the fact of the conclusion of the negotiation", while "look[ing] forward to receiv[ing] the relevant documents in order to […] assess whether [the arrangement] can answer the wider concerns raised by Schrems judgment as regards international transfers of personal data"[356]. Indeed, the Working Party "stands read to analyse the results of the negotiations in the light of the European essential guarantees", in order to assess "if its concerns regarding the U.S. legal framework can be alleviated"[357].

Looking at intelligence activities, the Article 29 Working Party has specified four essential guarantees, in light of which it will assess the new Privacy Shield:

(a) processing must be based on clear, precise and accessible rules, so that any reasonably informed person is able to foresee the consequences of a data transfer;

(b) there is a need to demonstrate necessity and proportionality with regard to the legitimate goals pursued, by striking a balance between the objective (usually national security) and individual rights;

(c) there should be an independent oversight mechanism, which may be performed by a judge or another independent body as long as it guarantees effectiveness and impartiality;

---

350 *Id.* at 8-9. *See* Data Protection Directive, Art. 26(1); European Union Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), 25 November 2005.

351 *Id.* at 9.

352 European Commission – Press release, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Strasbourg, 2 February 2016, available at: http://europa.eu/rapid/press-release_IP-16-216_en.htm. The new agreement was expected to be signed by January 2016. *See* D. KELLEHER, *A new Safe Harbor? Yes, it's possible* (Jan. 12, 2016), available at: https://iapp.org/news/a/173906/.

353 *Id.*

354 *Id.*

355 *Id.*

356 European Union Article 29 Data Protection Working Party, *Statement of the Article 29 Working Party on the consequences of the Schrems Judgment*, Brussels, 3 February 2016, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

357 *Id.*

(d) the individual should be given the necessary remedies and should be able to defend her rights before an independent body[358].

Clearly, agreement on the Privacy Shield "follows closely on the heels of the US Senate Judiciary Committee's passage of the Judicial Redress Act (H.R. 1428) on Jan. 28, 2016"[359]. This bill would provide EU citizens with the right to bring a civil action in the US against a US government agency with respect to the protection of their personal data[360]. The Schrems decision was largely based on the inadequate protection provided to EU citizens' data from access by the US government.

The text of the agreement is expected to be released by the end of February 2016, and the Working Party will hold an extraordinary plenary session in March, in order to achieve a finalization by the end of April. This is a particularly stimulating and interesting time for privacy law, as this kind of event obliges everyone – not just policymakers – to reflect and be creative in the design of new solutions and the abandonment of old, commonplace standards. Also, the Schrems decision increases the importance of finding principles that are common to both sides of the Atlantic Ocean.

6. Electronic Health Records in Italy

6.1 E-Health in Italy

The design of a legal framework for the Fascicolo Sanitario Elettronico (FSE), i.e., the Italian electronic health record, has sped up in the last few years, likely in part because of the savings this architecture is supposed to bring about[361]. Nevertheless, some studies have shown that Italy invests a significantly smaller amount of resources in the implementation of ICT in health care than other countries do[362].

The Italian government identified the general health goals for the country in a "National Plan 2003-2005", with a specific focus on health data[363]. This was followed by an E-Health Permanent Roundtable ("Tavolo di lavoro permanente per la sanità elettronica"), initiated in October 2004. Several institutions took part in this project (Regions, Autonomous Provinces and the central government), which was aimed at coordinating the implementation of the E-Health Plan (Piano Sanità Elettronica)[364]. In 2008, the Industrial Plan for the Innovation of the Public Administration (Piano industriale per l'Innovazione della P.A.) included the implementation of electronic health records by 2009[365]. The "E-Government Plan" (Piano di e-government) of 2012 also created a number of innovation projects attempting to enhancing the efficiency of the administrative system[366].

---

358 *Id.*

359 BRYAN CAVE LLP GLOBAL DATA PRIVACY AND SECURITY TEAM, *Privacy Shield: Safe Harbor 2.0?*, February 3, 2016, available at: https://www.bryancave.com/en/thought-leadership/privacy-shield-safe-harbor-2-0.html.

360 *Id.*

361 *See* IZZO & DUCATO, *supra* note 31, at 6.

362 C. CACCIA, *Sanità digitale: quale futuro. Considerazioni per una speranza di successo*, *Rivista elettronica di Diritto, Economia, Management,* n. 3, 2014, at 20. *See also* A. ORTALI, *Utilizzo dell'ICT (Information Communication Technology) in sanità*, *Rivista elettronica di Diritto, Economia, Management*, n. 3, 2014, at 102-04.

363 GUARDA, *supra* note 8, at 24.

364 *Id.* at 24-25.

365 *Id.* at 25.

366 *Id. See* http://www.e2012.gov.it/egov2012/.

6.2 Fascicolo Sanitario Elettronico

6.2.1 History

The Italian EHR architecture is called "Fascicolo Sanitario Elettronico" and it has been the subject of several pieces of legislation in the last few years. Before then, the legal framework for e-Health in Italy had been largely left to the work of the Italian Data Protection Authority (Garante), who had published its "Guidelines" in 2009[367] pursuant to its task of enhancing awareness of privacy protection laws[368], as well as to Guidelines by the Ministry of Health (Ministero della Salute) [369] generated by an "Interinstitutional" Roundtable involving the Ministero and representatives of Regions, of the Garante and of other institutions. These Guidelines defined the main features of the FSE and sketched a common legal framework[370].

In 2012, the FSE was dealt with by the Decree-Law no. 179 of 2012[371], which provided that the Agenzia per l'Italia Digitale (AgID) (Agency for a Digital Italy)[372] would send guidelines to the Regions and Autonomous Provinces. The deadlines sketched in this project were not completely met, but the path towards a common legal framework for the FSE went on with the Decree-law no. 69 of 2013[373]. The roadmap required ministerial decrees to establish a framework for the AgID to assess the regional projects[374]. Very recently, a long-awaited Decree of the President of the Council of Ministers was published, providing a general framework[375]. The DPCM ends with the creation of a "Tavolo tecnico di monitoraggio e indirizzo", which aims at monitoring FSE systems and proposes annual goals in order to achieve full implementation[376].

6.2.2 Definitions, Purposes and Rights

The FSE has been defined by Decree-law no. 179 of 2012 as "the set of data and digital documents relating to health and socio-medical information generated by past and present clinical events about the patient"[377]. It is "a structured collection of all information

---

[367] Garante per la protezione dei dati personali, Guidelines on the Electronic Health Record and the Health File, July 16, 2009 (published in Italy's Official Journal no. 178, dated 3 August 2009), available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821 [hereinafter Garante – FSE Guidelines 2009]; Garante per la protezione dei dati personali, Guidelines on Online Examination Records, November 19, 2009 (published in Italy's Official Journal no. 288, dated December 11, 2009), available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634292.

[368] *See* GUARDA, *supra* note 8, at 176-77.

[369] Italy – Ministry of Health, *Il Fascicolo Sanitario Elettronico – Linee guida nazionali*, November 11, 2010, available at: http://www.salute.gov.it/imgs/C_17_pubblicazioni_1465_allegato.pdf.

[370] GUARDA, *supra* note 8, at 26. *See also* G. PASCUZZI, *Il diritto dell'era digitale*, II ed., Bologna, 2010, at 84-89.

[371] Decree-law of October 18, 2012, no. 179 (converted into law by L. of December 17, 2012, no. 221 and published in Italy's Official Journal no. 294, dated December 18, 2012).

[372] This agency was established within the Presidency of the Council of Ministers with the decree-law of June 22, 2012, no. 83 (converted into law by L. of August 7, 2012, no. 134, published in Italy's Official Journal no. 189, dated August 11, 2012).

[373] Decree-law of June 21, 2013, no. 69 (converted into law by L. of August 9, 2013, no. 98, published in Italy's Official Journal no. 194, dated August 20, 2013).

[374] Decree-law no. 179 of 2012, Art. 12.7.

[375] Decree of the President of the Council of Ministers of September 29, 2015, no. 179 (published in Italy's Official Journal no. 263 dated November 11, 2015) [hereinafter FSE DPCM].

[376] FSE DPCM, Art. 26.

[377] Decree-law no. 179 of 2012, Art. 12.

relating both to the health of an individual […] and to social-healthcare services"[378]. The 2009 Guidelines by the Garante specify that the FSE is "a set of medical data relating, as a rule, to a given individual and contained in several inter-linked electronic records that can be shared by various public and private health care bodies"[379]. The Garante has not chosen a specific architecture but rather has focused on offering a conceptual and legal framework related to the goal[380].

The creation of FSE within the Italian legal framework is only allowed for some specific purposes: "a) prevention, diagnosis, treatment and rehabilitation; b) study and scientific research in the medical, biomedical and epidemiological field; c) health planning, verification of the quality of care and evaluation of health care"[381]. Interestingly, the Garante Guidelines did not include research within the allowed goals[382].

As we have seen, Section 3 of the Italian Data Protection Code establishes the so-called principle of data minimization, which requires the data controller to adopt organizational measures suitable to rule out, to the largest extent possible, the chance of using identifiable data through using anonymous data or allowing the identification of the data subject only if absolutely necessary under certain conditions[383]. This represents a general principle for the use of technology: the processing of identifiable data must be excluded when the specific goals can be achieved by using anonymous data[384]. This is based on the understanding that privacy can only be protected if the system is designed so as to allow its protection[385]. This principle emphasizes the importance of accurate designing and programming in the implementation of EHR systems[386].

The FSE is meant to be a means of communication among the different actors of the patient's treatment who fill in the information, but this can only happen with the informed consent of the patient, "who can decide which data – if any – can populate the FSE"[387]. Indeed, the patient "plays […] a proactive role": not only does he provide his consent, which is needed in order to insert data, but also he can access online services and upload data[388]. Pursuant to the decree-law no. 179/2012 and to the DPCM, the FSE is created by default by Regions or Autonomous Provinces. This is different from what had been established by the Garante in the Guidelines, according to which the FSE could only be created with the consent of the data subject[389]. However, without consent, which allows to add data, the FSE remains an empty box[390].

Article 6 lists the necessary elements that the information provided to the patients pursuant to Section 13 of the Data Protection Code must include[391]. First and foremost, it must specify that a FSE will be created for specific goals, and that the data that will be included in it will concern his or her present and possibly past health situation[392]. In addition, the information must include warnings about the provision of consent. We can

---

[378] IZZO & DUCATO, *supra* note 31, at 4.
[379] Garante – FSE Guidelines 2009, Paragraph 2.
[380] GUARDA, *supra* note 8, at 227, 33.
[381] Decree-law no. 179 of 2012, Art. 12.2
[382] GUARDA & DUCATO, *supra* note 9, at 399.
[383] GUARDA, *supra* note 8, at 185.
[384] *Id.* at 187.
[385] *Id.*
[386] *Id.* at 188.
[387] IZZO & DUCATO, *supra* note 31, at 4-5. Decree-law no. 179 of 2012, Art. 12.3 and 12.3-bis.
[388] Decree-law no. 179 of 2012, Art. 12.2 and 12.3-bis.
[389] GUARDA & DUCATO, *supra* note 9, at 410.
[390] *Id.*
[391] FSE DPCM, Art. 6.1.
[392] *Id.*

distinguish two different instances – consent to the data processing in order to create a FSE, and consent to access the data in the FSE for health treatment[393]. The patient must be informed that data can only be inserted in the FSE and accessed[394] with a specific consent, and that failure to provide such consent does not bear on the services provided by the National Health Service[395]. Furthermore, other necessary pieces of information concern the fact that the FSE can be accessed without consent if it is necessary to safeguard a third party's health or the public health, pursuant to Section 76 of the Data Protection Code and the General Authorization issued by the Garante[396]. Lastly, the patient must be informed as to the subjects who can access the FSE and as to the identity of the data controller and how to contact him or her[397].

Consent of the patient to the insertion of data in the FSE must be "free and informed", and can be revoked without consequences pertaining to the provision of services by the National Health Service[398]. If it is revoked, there is still the possibility to correct previously added data[399]. As to access to the data and documents within the FSE for the goals of "prevention, diagnosis, treatment and rehabilitation", it can only occur after the patient has viewed the information and expressed his consent[400]. This consent also implies consent toward giving health professionals access in instances of emergency as described by Article 14, and if it is revoked, formerly authorized health professionals can no longer access the data[401].

The patient has the right to access his FSE[402], and he can ask that the data and documents be obscured and be only viewable by him and the data controllers who produced them, in such a way that this decision is not made known to the health professionals and other authorized subjects[403]. Furthermore, the patient can obtain rectification or updating of his data[404].

6.2.3 Content

We can now turn to the content of the FSE. According to the new regulation, the FSE comprises a minimum core of data and documents as well as certain additional data and documents[405]. The core documents include: the identifying and administrative data regarding the patient[406], examination records, emergency room documents, the patient summary (see below), the pharmaceutical dossier, and the consent or denial to organ and tissue donation[407]. The addition of other documents is left to the Regions' autonomy[408].

The aforementioned "patient summary" ("profilo sanitario sintetico") is a document summarizing the clinical history of the patient, with the goal of enhancing continuity of

393 GUARDA & DUCATO, supra note 9, at 410.
394 FSE DPCM, Art. 6.2 e).
395 *Id.*, Art. 6.2 d).
396 *Id.*, Art. 6.2 g).
397 *Id.*, Art. 6.2 f), h) and i).
398 *Id.*, Art. 7.1 and 7.7.
399 *Id.*, Art. 7.7.
400 *Id.*, Art. 7.2.
401 *Id.*, Art. 7.8 and 7.9.
402 *Id.*, Art. 9.
403 *Id.*, Art. 8.1 and 8.2.
404 *Id.*, Art. 8.3.
405 *Id.*, Art. 2.1.
406 *See id.*, Art. 21.
407 *Id.*, Art. 2.2.
408 *Id.*, Art. 2.3.

care for allowing a quick overview of the situation[409].

Article 5 of the DPCM lists some particularly sensitive data, which can only be viewed with the explicit consent of the patient: she can decide to undergo certain treatments, such as abortion, in an anonymous way, and she can choose that her FSE does not include data such as those regarding HIV, alcohol, drugs, or pregnancy[410].

6.2.3.1 The "taccuino personale dell'assistito": the Italian PHR

The so-called "taccuino" ("notebook") is a form of Personal Health Record: because it allows the patient to access his data, fill in new data and view who accessed them, it represents a fundamental recognition of the patient empowerment principle[411]. The new Decree deals with the "taccuino" in Article 4, where it is defined as "a reserved section of the FSE in which the patient can insert data and personal documents relating to his or her care paths, even carried out in healthcare facilities outside the national health system"[412]. It is further specified that "the data and the documents inserted in the [taccuino] are non-certified information, and must be distinguishable from the data inserted by the subject listed in Article 12", i.e., health care professionals[413]. This is a conceptual, rather than architectural, choice: the concept of PHR stems from the possibilities created by technology rather than by a specific project made by the legislator, who follows rather than leads the developments of e-Health[414]. The "taccuino" is the first form of PHR recognized in Italy, preceded only by a project implemented in the Autonomous Province of Trento[415].

There are some issues with respect to the "taccuino", namely concerning data ownership and control, the interpretation of consent, and the value of the data inserted by the patient[416]. According to the DPCM, with respect to data processing for "prevention, diagnosis, treatment and rehabilitation"[417], the data controllers are "the subjects of the National Health System and of the regional services that handle the treatment of the patient, with which the data and the documents inserted in the FSE have been drafted"[418]. These data are to be treated pursuant to the fundamental principles, such as that of

---

409 *Id.*, Art. 3.1-2.

410 *Id.*, Art. 5.

411 GUARDA & DUCATO, *supra* note 9, at 390-91.

412 FSE DPCM, Art. 4.1 ("Il taccuino personale dell'assistito è una sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura, anche effettuati presso strutture al di fuori del SSN").

413 *Id.*, Art. 4.2 ("I dati e i documenti inseriti nel taccuino personale dell'assistito sono informazioni non certificate dal SSN e devono essere distinguibili da quelli inseriti dai soggetti di cui all'articolo 12").

414 GUARDA & DUCATO, supra note 9, at 405-06.

415 The "TreC – Cartella Clinica del Cittadino" project aims at promoting e-care services supporting the citizen as well as healthcare facilities. It includes a "libretto sanitario elettronico", allowing direct access by the patient to the FSE, and a "Diario della salute" (Health Journal), where the patient can add information. *See* https://trec.trentinosalute.net. GUARDA & DUCATO, supra note 9, at 406, fn. 46. *See* GUARDA, *supra* note 8, at 61-65.

416 GUARDA & DUCATO, supra note 9, at 407.

417 Decree-law no. 179 of 2012, Art. 12.2 a).

418 FSE DPCM, Art. 10 ("Per i trattamenti dei dati effettuati per le finalità di cui alla lettera a) del comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, i soggetti del SSN e dei servizi socio-sanitari regionali che prendono in cura l'assistito, presso cui sono stati redatti i dati e i documenti sanitari che alimentano il FSE, sono titolari del trattamento secondo quanto previsto dall'articolo 28 del Codice in material di protezione dei dati personali").

necessity[419]. Similarly, for the goals of "study and scientific research in the medical, biomedical and epidemiological field"[420], the data controllers are the Regions, the Autonomous Provinces and the Ministry of Health[421], and the data must be de-identified[422]. Despite these clarifications, the introduction of a PHR system causes the power of the data controller to be more and more blurred, which led to the creation of the concept of "joint data controller" in the new proposed General Data Protection Regulation[423]. With the introduction of the "taccuino", the patient is no longer just a "data subject", but rather can actively participate to the data flow[424]. This leads to the second relevant issue, i.e., consent. In order to add data to the "taccuino", the patient must have given his informed consent pursuant to Article 7.1 of the DPCM, since the "taccuino" is a section of the FSE[425]. Furthermore, the patient can decide with whom he wants to share the data he fills in the "taccuino", which looks like a "health secret diary" that the patient can unlock and show to selected subjects[426]. The third crucial issue is that of the value of the data added by the patient, which falls into the broader topic of the evolution of trust in the provision of health care. Indeed, the physicians might not trust the data included in the "taccuino", especially in light of possible liability[427].

6.2.4 Data Processing

6.2.4.1 Data Processing for the Purpose of Health Treatment

Part II of the DPCM deals with data processing for treatment, i.e. for the purposes of "prevention, diagnosis, treatment and rehabilitation"[428]: data controllers are the subjects of the national and regional health services who treat the patient and at whose facilities the data are created[429]. The data and documents within the FSE must be processed pursuant to the general principles, such as that of necessity[430], and they can be further elaborated in order to help diagnosis and prevention as long as no new data are created[431]. If the data subject asks to block access to some data or documents (obscurement), they cannot be used[432].

The subjects who can add data to the FSE are health care professionals and any subject operating within the National Health Service, as well as the patient himself with

---

419 FSE DPCM, Art.11.1 ("Per le finalità di cui all'articolo 10, sono trattati tutti i dati e documenti di cui all'articolo 2, presenti nel FSE, coerentemente con i principi di indispensabilità, necessità, pertinenza e non eccedenza").
420 Decree-law no. 179 of 2012, Art. 12.2 b).
421 FSE DPCM, Art.13.1 ("Per i trattamenti dei dati effettuati per le finalità di cui alla lettera b), del comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, le regioni e province autonomi e il Ministero della salute, nei limiti delle rispettive competenze attribuite dalla legge, sono titolari del trattamento secondo quanto previsto dall'articolo 28 del Codice in materia di protezione dei dati personali").
422 FSE DPCM, Art.16.1.
423 GUARDA & DUCATO, *supra* note 9, at 408-09.
424 Id. at 409.
425 Id. at 410.
426 Id. at 411.
427 Id. at 412. For an analysis of this issue, see *id.* at 412-17.
428 *See* Decree-law no. 179 of 2012, Art. 12.2 a).
429 FSE DPCM, Art. 10.
430 *Id.*, Art. 11.1.
431 *Id.*, Art. 11.2.
432 *Id.*, Art. 11.3.

respect to the "taccuino"[433].

Access to the FSE for health care purposes is only allowed if the patient has expressed explicit consent, the data which need to be processed are only those relevant to the ongoing treatment, and the subjects are authorized and effectively involved in the treatment[434]. Regions and Autonomous Provinces implementing a FSE system can choose to provide for a notification service, allowing the patient to be notified as to any access to his FSE[435]. Another instance in which the information contained in the FSE can be accessed concerns emergency cases, where pursuant to Section 82 of the Data Protection Code[436] information and consent can be provided afterwards. Previously, the Guidelines by the Garante had only mentioned emergency cases with respect to cross-border data transfer, and other types of processing were dealt with by applying other general provisions[437].

6.2.4.2 Data Processing for Research Purposes

The Regions and Autonomous Provinces and the Ministry of Health are considered data controllers whenever data is processed for the purposes of "study and scientific research in the medical, biomedical and epidemiological field"[438]. Interestingly, the data need to be stripped of directly identifying data (see Chapter III), and the DPCM lists the data which are expressly excluded from treatment for research purposes[439]. Such data include, among others, name, birthdate, ID documents, and address[440].

6.2.4.3 Data Processing for Governmental Purposes

When the data and documents within the FSE are processed for the purposes of "health planning, verification of the quality of care and evaluation of health care", data controllers are the Regions and Autonomous Provinces, the Ministry of Health and the Ministry of work and social policies[441]. Similar to what happens when data are processed for purposes of research, they must be de-identified, and there is a list of data which must be excluded[442]. Also, the DPCM specifies that the Ministry of work and social policies processes the data in individual form, but deprived of any reference that may allow for a direct link to the patient, and including such measures as ensuring that information about the same patient is linkable over time but not directly traceable to the individual[443].

6.2.5 Technical Rules and Security Measures

The DPCM mandates the adoption of electronic tools which are able to maintain confidentiality and integrity of the data[444]. Furthermore, suitable protections must be set up

---

433 *Id.*, Art. 12.
434 *Id.*, Art. 13.2.
435 *Id.*, Art. 13.3.
436 *Id.*, Art. 14.
437 C. FILAURO, *Telemedicina, cartella clinica elettronica e tutela della* privacy, *Danno e resp.* 5, 2011, at 483.
438 FSE DPCM, Art. 15. *See* Decree-law no. 179 of 2012, Art. 12.2 b).
439 FSE DPCM, Art. 16.
440 *Id.*, Art. 16.2.
441 *Id.*, Art. 18.
442 *Id.*, Art. 19.
443 *Id.*, Art. 20.3.
444 *Id.*, Art. 23.1.

against unauthorized access and theft[445]. To this end, FSE systems must have authentication and authorization mechanisms[446], methods for tracking each access to the system[447], and procedures of anonymization of directly identifying elements[448]. Interestingly, pursuant to the DPCM, the structure and the organization of the data within the FSE must reflect not only the differences among the types of data which are relevant for different purposes, but also the different authorization levels[449].

Every time a data breach or loss or unauthorized disclosure occurs, the data controller must notify the Garante within a week, describing the data involved and the consequences of the incident[450].

Another interesting feature is interoperability: each Region or Autonomous Province must make sure that, at the very least, research and recovery of the data are possible[451]. Indeed, this aims at the creation of a holistic approach, which has so far not been possible: the Italian experience has largely been featured by some local virtuous systems, but it is clear that we need to move toward a more comprehensive national approach[452].

6.3 "Dossier sanitario": the 2015 Guidelines by the Garante

Another pertinent document is the Guidelines on the "Dossier Sanitario" published by the Garante in 2015[453]. To begin with, we need to understand the difference between FSE and "Dossier sanitario". As we have seen, the first is formed by the whole clinical history of the patient, including data created by different health care facilities, whereas the "dossier sanitario" collects only the clinical history of a patient occurring within the same health care facility, i.e., with respect to the same data controller. The Garante noticed many risks with respect to accuracy of the data and allowing access only to authorized subjects, often due to the failure to attentively plan the infrastructure[454]. The mere digitization of health records cannot be carried out without the awareness that the system will then be able to manage the entire clinical history of the patient and without implementing suitable measures to guarantee accuracy and integrity of the data[455].

The insertion of data in a "dossier sanitario" implies a further processing of data, because the health care professional can view not only the information provided by the patient within that clinical event, but also the data concerning past events within that same facility[456]. Therefore, the patient must be adequately informed pursuant to Section 13 of the Data Protection Code: the information must make the patient aware that the data

---

445 *Id.*, Art. 23.4.
446 *Id.*, Art. 23.5 a).
447 *Id.*, Art. 23.5 e).
448 *Id.*, Art. 23.5 g).
449 *Id.*, Art. 23.6.
450 *Id.*, Art. 23.9.
451 *Id.*, Art. 25.1.
452 GUARDA, *supra* note 3, at 37-38.
453 Garante per la protezione dei dati personali, Guidelines on the "Dossier sanitario", June 4, 2015, available at: http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+Allegato+A.pdf [hereinafter Garante – DS Guidelines 2015]. *See also* Garante per la protezione dei dati personali, Dossier sanitario: prescrizioni per il sistema informativo delle prestazioni sanitarie erogate da un'Azienda sanitaria, October 22, 2015, available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4449114 (where the Garante recently published some guidelines with respect to a specific case).
454 Garante – DS Guidelines 2015, at 4.
455 *Id.*
456 *Id.* at 6.

controller aims at collecting a comprehensive record of his clinical history in order to enhance the health care treatment[457]. Also, the patient must be aware that not providing his consent does not bear on the provision of health care services, whereas providing his consent grants access to his data even in cases where it is necessary to safeguard a third party's health or the public health[458]. The "dossier sanitario" can also be accessed by professionals who act independently but within the health care facility infrastructures[459]. Because of the potentially long list of authorized subjects, the information must also include the criteria bearing on the authorization[460].

As we have said, the consent to the "dossier sanitario" is completely free, can be revoked and failure to provide it cannot bear on the chance to access health care treatments[461]. After consent is provided, the "dossier sanitario" will be accessible by any health care professional who deals with the subject's care, without the need for the patient to express his consent every time[462], including instances of emergency where the subject is unable to speak[463].

The data subject can exercise several rights with respect to the "dossier sanitario". He has the right to know the criteria used to process data, as well as the identity of the data controller and of the authorized subjects[464]. Also, he can ask for an amendment to or update of his data[465]. Another right the patient is provided with is that of obscuring certain data or documents, similar to what happens with respect to the FSE[466]. These data or documents remain available to the professionals who produced them[467]. Therefore, the Garante highlights that the "dossier sanitario" is necessarily incomplete[468], due to the chance of obscurement as well as to the fact that it only includes data with respect to clinical events occurring within one particular health care facility[469]. The data subject must be adequately informed of the consequences of obscuring data with respect to the inability of health care professionals to have an exhaustive overview of his record[470]. The patient also has the right to view who accessed his "dossier sanitario" by requesting it[471]. The data controller must answer the request within 15 days (or, in some cases, 30 days)[472].

Most interestingly, the Garante acknowledges that the information included in the "dossier sanitario" can have a relevant economic value and states that it is crucial to avoid access by unauthorized subjects aiming at economic exploitation of such sensitive data[473]. Therefore, the "dossier sanitario" can only be accessed by health care personnel participating in the process of care[474]. This needs to be guaranteed by implementing

457 *Id.* at 7.
458 *Id.*
459 *Id.* at 8.
460 *Id.* at 9.
461 *Id.* at 11-12.
462 *Id.* at 14.
463 *Id.* at 15.
464 *Id.* at 19.
465 *Id.*
466 *Id.* at 20.
467 *Id.* at 21.
468 *Id.* at 20.
469 *Id.* at 20-21.
470 *Id.* at 21-22.
471 *Id.* at 23.
472 *Id.* at 23-24.
473 *Id.* at 25.
474 *Id.*

authentication mechanisms which take into account all the different hypotheses[475]. The data controller must not only establish the criteria to identify the authorized subjects, but also specify the "depth of access"[476]. Depending on the circumstances, access should be given only to certain specific documents and data[477]. For instance, administrative personnel should only be allowed to access the data necessary to carry out administrative tasks[478]. These measures aim at ensuring a "modular" access to the "dossier sanitario", so that data can only be accessed when it is necessary to fulfill a specific and relevant goal[479].

The Garante Guidelines also underline the importance of implementing adequate security measures[480]. First of all, the data controller must adopt suitable authentication and authorization systems[481], in order to provide the necessary technical support to the "modular" approach we have just discussed. Secondly, the technical infrastructure must allow tracking of the instances of access and of the operations and processing performed, including mere inquiry[482]. Thirdly, systems of audit log must be implemented that can spot anomalies with specific alerts[483]. This aims at keeping the data processing performed via the "dossier sanitario" under constant control by the data controller in order to assess the adequacy of the security measures both from the organizational and technical point of view[484]. The auditing must be entrusted to a different personnel unit and must be adequately recorded[485]. The fourth security measure the Garante describes concerns data separation and coding: health data must be separated from other personal data, and particularly sensitive data must be coded, also by partially encrypting them[486].

The last topic the Guidelines deal with regards data breaches. Pursuant to Section 154.1 c) of the Data Protection Code, the data controllers must notify to the Garante a data breach within 48 hours[487]. Also, adequate procedures must be set up to timely notify the data subject of any instances unauthorized access to his file[488]. The Garante also suggests that the data controllers should create a data protection officer[489].

7. Electronic Health Records in the United States

The push for the creation of a national EHR database is rooted in the fragmentation of the U.S. health care system, governed by a piecemeal legislation at the national, state, community, and individual practice level[490]. Given the need for a way to enhance the safety,

---

475 *Id.* at 26.
476 *Id.* at 27.
477 *Id.*
478 *Id.* at 27-28.
479 *Id.* at 28.
480 *Id.* at 31.
481 *Id.*
482 *Id.* at 32-33.
483 *Id.* at 33.
484 *Id.* at 33-34.
485 *Id.* at 34.
486 *Id.*
487 *Id.* at 35.
488 *Id.*
489 *Id.* at 36.
490 GRADY, *supra* note 49, at 380-81. *See* A. SHIH ET AL., *Commonwealth Fund, Organizing the U.S. Health Care Delivery System For High Performance* ix (2008). Indeed, until the 2000s, EHR projects in the United States were not many, as their advantages were not fully perceived and the costs looked too burdensome. The first projects only concerned organizations with strongly integrated systems who could fully take advantage of this kind of plan. Two examples are the Veterans Health Administration VistA architecture and the Kaiser Permanente's HealthConnect system. GUARDA, *supra* note 8, at 75. *See also* Executive Office of the President

efficiency, and quality of health care, President Bush passed an executive order in 2004 initiating a ten-year plan for the implementation of a national electronic health record system[491], "designed to share information privately and securely among and between health care providers when authorized by patients"[492]. Subsequently, the Obama administration established a 27 billion dollar investment to promote health information technology in the American Recovery and Reinvestment Act (ARRA) of 2009[493], which includes the Health Information Technology for Economic and Clinical Health Act (HITECH) [494]. Nevertheless, "the implementation of EHRs at the national and regional level has been mostly piecemeal, with different agencies and health care organizations developing electronic databases of patient information as part of their own programs"[495]. Arguably, [i]n order for a national [system] to be successful, the United States must adopt a uniform national privacy law"[496]. Indeed, the potential underlying EHR technology could be fully developed if HIPAA did not allow for any exceptions to the preemption provision, since "any health care provider would have access to an individual's entire health record from his birth to his most recent encounter with the health care system" with no need for patient consent, as it is not required for disclosures of PHI for treatment purposes[497]. Thus, HIPAA has been said to "[pose] a challenge to the development of a national EHR system […] because of the ways it may conflict with state privacy laws, thus impeding progress toward the national goal of interoperability"[498]. On the other hand, others have noted that the security standard system established by HIPAA can represent a valid framework to handle medical data, especially due to its flexibility, which leaves such a degree of leeway as to make data controllers fully aware of the risks and more able to adopt the solutions that best fit the circumstances[499].

Looking at the degree of patient control, the US system seems to give patients "little choice in the electronic recording of sensitive medical information if they want to be treated, and minimal control over the sharing of that information"[500]. Furthermore, it has been argued that "the U.S. framework, while making progress in the protection of health information, lacks the historical presumption of privacy [that the EU features] and thereby may not earn consumer confidence as easily"[501], also due to a lack of transparency and clarity[502].

– President's Council of Advisors on Science and Technology, *Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: the Path Forward,* December 2010, available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf. *See also* C. CHEN, T. GARRIDO, D. CHOCK, G. OKAWA, L. LIANG, *The Kaiser Permanente Electronic Health Record: Transforming And Streamlining Modalities of Care*, 28 *Health Affairs*, 2009, 2 , 323.

491 Exec. Order No. 13,335, 69 Fed. Reg. 24059, 24059 (April 30, 2004). *See* GRADY, *supra* note 49, at 382; HILLER ET AL., *supra* note 47, at 3.

492 The White House, *Transforming Health Care: The President's Health Information Technology Plan*, April 2004, available at: http://georgewbush-whitehouse.archives.gov/infocus/technology/economic:policy200404/chap3.html.

493 American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

494 Health Information Technology for Economic and Clinical Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

495 GRADY, *supra* note 49, at 382.

496 *Id.* at 396.

497 *Id.* at 397. *See* Chapter I, Paragraph 4.1.4.5.

498 GRADY, *supra* note 49, at 390.

499 GUARDA, *supra* note 8, at 87.

500 HILLER ET AL., *supra* note 47, at 1.

501 *Id.* at 38-39.

502 GUARDA, *supra* note 8, at 90.

7.1 The EHR Incentive Program

The HITECH Act established incentive programs to encourage the adoption of electronic health records by Medicare and Medicaid providers[503], "by providing carrots for those professionals and hospitals that shoulder the onerous burdens associated with implementing and using this technology"[504]. This was done in order to try to "reduce or eliminate the market failures that have impeded the adoption of" EHRs[505]. Under these programs, incentives are awarded to eligible entities demonstrating "meaningful use" of certified EHR technology[506].

The HITECH Act also created the Office of the National Coordinator (ONC) for Health Information Technology, within the Department of Health and Human Services[507]. Among its responsibilities is the review of the meaningful use requirements established by the Health Information Technology Standards Committee[508], entrusted with the task of providing a basic framework for every EHR system[509]. Also, the Health Information Technology Policy Committee is responsible for making policy recommendations to the ONC and "setting forth official standards as to how providers should document and exchange patients' [PHI]"[510].

In order to meet the "meaningful use" requirement, providers "have to show CMS that they are using their EHRs in ways that can positively affect the care of their patients"[511]. The Medicare EHR Incentive Program consists of three stages, and "each stage will have its own set of requirements to meet in order to demonstrate meaningful use"[512]. The three stages must be met over the five consecutive years following the first one[513]: Stage One is aimed at generating PHI in EHR format, Stage Two focuses on the exchange of data, and Stage Three revolves around the improvement of health care with such data[514]. More specifically, within Stage One eligible professionals have to meet the measures for 15 "core objectives" and 5 "menu objectives" and report on "clinical quality

---

503 A. WRIGHT, J. FEBLOWITZ, L. SAMAL, A. B. MCCOY, D.F. SITTIG, *The Medicare Electronic Health Record Incentive Program: Provider Perofrmance on Core and Menu Measures*, 49 *Health Services Research 325* (2014). *See EHR Incentive Programs*, CMS.gov, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentive Programs/. *See also* D. BLUMENTHAL AND M. TAVENNER, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 *New England Journal of Medicine* 501 (2010); L. MARCOTTE, J. SEIDMAN, K. TRUDEL, D. M. BERWICK, D. BLUMENTHAL, F. MOSTASHARI, AND S. H. JAIN, *Achieving Meaningful Use of Health Information Technology: A Guide for Physicians to the EHR Incentive Programs*, *Archives of Internal Medicine* 172 (9):731–6 (2012).

504 SZEREJKO, *supra* note 80, at 1109.

505 TERRY, *supra* note 41, at 45.

506 GRADY, *supra* note 49, at 394. Centers for Medicare & Medicaid Services, Office of Public Affairs, *CMS EHR Meaningful Use Overview*, available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html. *See also* S. HOFFMAN & A. PODGURSKI, *Meaningful Use and Certification of Health Information Technology: What About Safety?*, Faculty Publications. Paper 3 (2011), available at: http://scholarlycommons.law.case.edu/faculty_publications/3; A. WRIGHT, S. HENKIN, J. FEBLOWITZ, A.B. MCCOY, D.W. BATES, D. F. SITTIG, *Early Results of the Meaningful Use Program for Electronic Health Records*, in *New England Journal of Medicine*, 368, 8, 2013, 779.

507 42 U.S.C. § 300jj-11(a) (2012).

508 SZEREJKO, *supra* note 80, at 1110. *See* 42 U.S.C. § 300jj-13 (2012).

509 SZEREJKO, *supra* note 80, at 1110.

510 *Id.* at 1110-11.

511 Centers for Medicare & Medicaid Services, *An Introduction to the Medicare EHR Incentive Program for Eligible Professionals*, available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf, at 7.

512 *Id.* at 8.

513 SZEREJKO, *supra* note 80, at 1112.

514 *Id.* at 1113. For a broader explanation of the three different stages, see *id.* at 1114-17.

measures"[515].

These requirements are meant to "serve as a call to action for health care providers insofar as they delineate how clinicians should use EHR technology's best features to their full potential"[516]. Indeed, the "deceptively simple requirement" of 'meaningful use' "has become both the regulatory core and the talisman for the next decade's implementation of health information technology"[517]. Starting in 2015, Medicare-eligible professionals who are not able to prove meaningful use will receive a one-percent Medicare payment reduction for that calendar year, increasing by a percentage point for every subsequent year[518]. The "incentive payment schedule and the increasingly harsh penalties for non-compliance" are meant "to make meaningful use of EHRs by all U.S. health care providers a reality", because "in theory, the […] scheme enforces compliance for the large majority of health care providers who receive reimbursement payments under Medicare and Medicaid"[519]. Health care privacy expert N.P. Terry has argued that "the inclusion in HITECH of the elegant phrase "meaningful use" together with the emerging political reality of broader health care reform under the Obama administration discloses a considerably broadened agenda", as this concept seems to "[transcend] any expected accountability-for-stimulus-funds model" and to be rather aimed at achieving "health care that is patient-centered, evidence-based, prevention-oriented, efficient, and equitable"[520].

As mentioned, EHR technology must be certified, i.e., EHR software must be tested and certified by an ONC Authorized Testing and Certification Body before the provider can qualify for the incentive payments[521]. Also, "failure to comply with any of the regulations will potentially rescind certification for a short amount of time"[522]. The twenty-two specifications include the ability to record and chart vital signs, the maintenance of active medication lists, the maintenance of medication allergy lists, the ability to include laboratory test results, and the capability to generate lists of patients with specific conditions[523].

The ONC has also established privacy-protecting standards that the software must respect[524]. First, the information must be encrypted using an algorithm developed by the National Institute of Standards and Technology[525]. Subsequently, the requirement that

---

[515] *An Introduction to the Medicare EHR Incentive Program for Eligible Professionals*, *supra* note 511, at 30-31. The 15 "core objectives" are: (1) Computerized provider order entry (CPOE); (2) Drug-drug and drug-allergy checks; (3) Maintain an up-to-date problem list of current and active diagnoses; (4) E-Prescribing (eRx); (5) Maintain active medication list; (6) Maintain active medication allergy list; (7) Record demographics; (8) Record and chart changes in vital signs; (9) Record smoking status for patients 13 years or older; (10) Report ambulatory clinical quality measures to CMS/States; (11) Implement clinical decision support; (12) Provide patients with an electronic copy of their health information, upon request; (13) Provide clinical summaries for patients for each office visit; (14) Capability to exchange key clinical information; (15) Protect electronic health information. Id. at 32.

[516] SZEREJKO, *supra* note 80, at 1112 (referring to BLUMENTHAL & TAVENNER, *supra* note 503, at 503).

[517] TERRY, *supra* note 41, at 45.

[518] SZEREJKO, *supra* note 80, at 1112. *See Medicare and Medicaid EHR Incentive Program Basics*, CMS.gov, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html.

[519] SZEREJKO, *supra* note 80, at 1118-19

[520] TERRY, *supra* note 41, at 62-63.

[521] Centers for Medicare & Medicaid Services, *Certified EHR Technology* (Oct. 11, 2011), http://www.cms.gov/EHRIncentivePrograms/25_Certification.asp.

[522] TURK, *supra* note 623, at 575.

[523] 45 C.F.R. § 170.302. TERRY, *supra* note 41, at 58. TURK, *supra* note 623, at 576.

[524] TURK, *supra* note 623, at 577.

[525] Id. *See* 45 C.F.R. § 170.210(a). The data is thus converted to an unintelligible form called "ciphertext". TURK, *supra* note 623, at 577.

information be hashed was added[526]. Second, the software must record every time that EHR data is created, accessed, deleted, or modified[527]. Third, "there must be verification if information has not been altered"[528]. Fourth, disclosures for treatment or payment should also be recorded[529]. Additionally, the date and time that EHR technology is used or changed must be kept in an audit log[530]. Finally, EHR softwares must include a clock synchronized to the Network Time Protocol[531].

As we have mentioned, certification can be revoked if the vendors fail to maintain the criteria[532]. Violations can occur either if "the vendors violate a law or the integrity of the EHRs" or if they fail to comply with the regulations[533]. The first type is more serious, as there is no warning from the ONC and it causes the vendor to be barred from reapplying for certification for a year[534]. In case of a noncompliance violation, the vendor receives a warning and can address potential false allegations[535].

Arguably, since "having to wait for a year before recertification" seems to be the only consequence, "there are no deterrents of consequence to ensure that vendors will maintain their certification"[536]. This looks very worrisome inasmuch as "[f]ailure to maintain the criteria that directly relate to privacy may leave the door open to breach"[537]. Therefore, a scholar argues, "there still needs to be smarter deterrence in order to protect individual medical information and reflect the importance of maintaining patient health information privacy"[538]. Due to the significant concerns that failure to comply may bring around, "a deterring monetary penalty is necessary"[539] in order to build a "supplemental assurance of patient's privacy"[540]. Such penalty "should not be harsh enough to deter vendors from creating the software", but "should be proportional to the harm" and "efficient in its purpose"[541]. An article proposes the application of the HIPAA Privacy Rule civil monetary penalties to EHR certification[542], which would cause vendors to "be held to the same standard as other covered entities"[543]. Nevertheless, there needs to be a safe harbor provision, too, which "would incentivize the vendor to report a breach of privacy by putting protections for the vendors in place"[544]. When determining the amount of the civil monetary penalty, the judge should consider the failure to report the breach among the factors[545]. Under the proposed "bifurcated notice scheme", the vendor must inform HHS any time he suffers a breach or he stops complying with the certification criteria[546]. Then, HHS will "determine which patients, if any, should be on notice that their health

---

526 TURK, *supra* note 623, at 578. *See* 45 C.F.R. § 170.210(f).
527 TURK, *supra* note 623, at 577. *See* 45 C.F.R. § 170.210(b).
528 TURK, *supra* note 623, at 577. *See* 45 C.F.R. § 170.210(c).
529 TURK, *supra* note 623, at 577. *See* 45 C.F.R. § 170.210(d).
530 TURK, *supra* note 623, at 578. *See* 45 C.F.R. § 170.210(e).
531 TURK, *supra* note 623, at 578. *See* 45 C.F.R. § 170.210(g).
532 TURK, *supra* note 623, at 578. *See* 45 C.F.R. § 170.565(a)-(b).
533 TURK, *supra* note 623, at 578-79.
534 *Id.* at 579. *See* 45 C.F.R. § 170.565(h)(3).
535 TURK, *supra* note 623, at 579. *See* 45 C.F.R. § 170.565(b).
536 TURK, *supra* note 623, at 579.
537 *Id.* at 580.
538 *Id.*
539 *Id.* at 582.
540 *Id.* at 583.
541 *Id.*
542 *Id.* at 586-91.
543 *Id.* at 587.
544 *Id.* at 588.
545 *Id.*
546 *Id.* at 589.

information may have been compromised"[547]. Timely notification to HHS by the vendors will "positively influence the court's decision" when determining the amount of the penalty[548].

Arguably, imposing a monetary penalty will also cause patients to be more comfortable: they will know "that the vendors securing their records will be held accountable of a breach regardless if individual patients are harmed"[549].

7.2 The Privacy-enhancing HITECH Measures: Still Some Work to Do

We have seen in Chapter I that the HITECH Act extended the applicability of the HIPAA Privacy Rule to business associates[550]. Nevertheless, it still does not apply to independent online personal record vendors[551]. There is only a requirement on the Department of Health and Human Services to "conduct a study to determine what—if any—additional privacy and security requirements should be applied to personal health record vendors"[552]. Also, the data breach notification rule does not cover independent online personal record vendors, who are only "subject to a similar Health Breach Notification Rule as implemented by the FTC", pursuant to which "[v]iolations […]will be treated as unfair and deceptive acts or practices in violation of the FTC Act"[553].

Independent PHR vendors are a relevant part of the e-Health market: both Microsoft and Google have tried to develop their own system[554]. Microsoft HealthVault was launched in 2007 whereas Google launched its own service called Google Health in 2008[555]. Other companies within the health industry have started similar programs, too[556]. The Google Health privacy policy was very similar to the HIPAA Privacy Rule, as it promised it would "not sell, rent, or share information with others unless the user specifically authorizes the dissemination of information", but there were some limited instances where information [would] be shared without the user's consent[557]. Google Health was permanently discontinued in 2013 because it did not have "the broad impact that [Google] hoped it would"[558]. Similarly, Microsoft HealthVault "will not share PHRs without the consent of the user", but "reserves the right to share information without a user's authorization in limited circumstances"[559]. Furthermore, HealthVault complies with the HONcode standard for trustworthy health information, which is "an ethical code for websites that electronically store medical and health information" and requires companies to "respect the privacy and confidentiality of personal data submitted to the site by the visitor"[560]. Despite these privacy protections, it is easy to notice how "without HIPAA regulation, it is up to each individual PHR vendor or online health service to determine

---

547 *Id.*
548 *Id.*
549 *Id.*
550 *See* Chapter I, Paragraph 4.1.3.
551 DUMORTIER & VERHENNEMAN, *supra* note 31, at 51-52.
552 *Id.* at 52.
553 *Id.* at 48.
554 *See* STACCINI ET AL., *supra* note 25, at 338-39.
555 J. CALDARELLA, *Privacy and Security of Personal Health Records Maintained By Online Health Services*, 20 *Alb. L.J. Sci. & Tech.* 203, 206 (2010).
556 *Id.* at 207.
557 *Id.* at 208.
558 Google Official Blog, *An update on Google Health and Google PowerMeter*, June 24, 2011, available at: http://googleblog.blogspot.it/2011/06/update-on-google-health-and-google.html?m=1.
559 CALDARELLA, *supra* note 555, at 208-09.
560 *Id.* at 209.

whether its consent policies are adequate"[561].

Many scholars have noticed how this represents a gap in the U.S. legislation, which should be bridged by subjecting PHR vendors to regulations requiring them to adopt "reasonable administrative, technical, and physical safeguards to ensure [the] confidentiality, integrity, and availability [of individually identifiable health information], and to present unauthorized or inappropriate access, use, or disclosure"[562]. Given the nature of the data they deal with, "PHRs should be required to employ best practices in data encryption, password protection, and authentication"[563].

8. A Glance On Two More Topics

The last part of this Chapter has been devoted to providing an overview of two very interesting topics, which are closely related to electronic health records and largely feature the same issues and concerns. Firstly, we will look at mobile health apps, whose growing popularity tends to conceal the crucial risks connected to the dehumanization of healthcare. Secondly, we will analyze the legal concerns connected to cloud computing in the field of healthcare.

8.1 Mobile Health Apps: Relevant Issues

Mobile health is "the use of mobile communications devices like smartphones and tablet computers for health or medical purposes, usually for diagnosis, treatment, or simply well-being and maintenance"[564]. Usually, mobile health technologies "interface with users through applications ("apps")"[565] and "take advantage of a smartphone's built in features", thereby arguably "turning phones into medical devices"[566]. The growth of this market has been astonishing, and an estimate predicts that "by 2018, the market will generate $26 billion in revenues"[567]. Mobile health apps can be divided between patient/consumer apps, such as health and wellness apps and self-management tools for chronic diseases, and provider apps, such as information and reference apps and diagnostic aids[568]. Apps relating to EHR fall within both categories.

The so-called mobile health revolution "sits at the intersection of several converging phenomena", including the "quantified self" movement[569]. We have discussed how an excessive reliance on efficiency as a goal causes policymakers and citizens to overlook more important interests. This is why some scholars argue that regulators should conduct a

---

[561] *Id.* at 210-11.

[562] C.P. MCCARTHY, *Paging Dr. Google: Personal Health Records and Patient Privacy*, 51 *William & Mary L. Rev.* 2243, 2264-65 (2010).

[563] *Id.* at 2267.

[564] N. CORTEZ, *The Mobile Health Revolution?*, 47 *U.C.D. L. Rev.* 1173, 1176 (2014).

[565] *Id.*

[566] *Id.* at 1177. For an analysis of the different categories of mobile health apps, see *id.* at 1181-90.

[567] *Id.* at 1191 (citing *Mobile Health Market Report 2013-2017: The Commercialization of mHealth Applications* (Vol. 3), RESEARCH2GUIDANCE 7 (Mar. 4, 2013)).

[568] A.M. HELM & D. GEORGATOS, *Privacy and mHealth: How Mobile Health "Apps" Fit Into A Privacy Framework Not Limited To HIPAA*, 64 *Syracuse L. Rev.* 131, 148 (2014).

[569] CORTEZ, *supra* note 564, at 1178. The "quantified self" movement was founded by two Wired magazine editors and consists in using technologies such as wearable devices to collect data about our health. *See* K. HILL, *Adventures in Self-Surveillance, a.k.a. The Quantified Self, a.k.a. Extreme Naval-Gazing*, *Forbes* (Apr. 7, 2011); The Economist, *The Quantified Self: Counting Every Moment* (Mar. 3, 2012); M. SWAN, *Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen*, 2 *J. Personalized Med.* 93 (2012).

"meaningful regulatory oversight", in order to "prevent […] health policy […] from being dictated by "technological solutionism," or the idea that technology can solve any and all of our problems, no matter how complicated or persistent"[570]. The goals of "mHealth" are largely the same as those of EHR technologies, including the improvement of quality of health care, the reduction of costs, and increased access to care[571]. Therefore, we should look at how mHealth pursues these goals with the same critical glance, bearing in mind the centrality of human dignity.

First of all, mobile health aims at reducing medical errors and improving the quality of health care. Indeed, if "more granular health data" is gathered, it can be used "to better tailor care, to better coordinate care, and to avoid duplicative or unnecessary care"[572]. Nevertheless, several mobile health apps do not follow evidence-based guidelines and are not grounded on scientific foundations[573]. The second goal for mobile health is reducing health spending. For instance, mHealth can prevent more acute episodes of care and help to better manage chronic diseases[574]. However, "for all this to be true, these technologies must work", whereas apps deceptively promising therapeutic effects "will squander rather than save money"[575]. Thus we need to inquire into "what net economic effect mobile health care will have on overall spending"[576]. The third, and arguably more interesting, aspiration for mHealth is the decentralization, demystification, and democratization of medicine[577]. The "shift [of] the locus of care […] towards individual patients" is a trend we have already noticed in the development of EHR technology and is a part of a broader cultural phenomenon[578]. The "demystification" of medical practice is supposed to promote a greater reliance on evidence rather than on professional judgments[579], but, as we have argued, the provision of health care is an inherently human activity, as it is performed by humans, for humans. As any human activity, it entails the possibility of mistake. On the other hand, the "automation bias" mindset, which consists in considering computers error-resistant, "disarms us from critically evaluating potential errors"[580]. We should acknowledge that human activities are nuanced, complex, and may be featured by mistakes. Bright-line rules should be regarded with suspicion as they tend to overlook crucial issues and simplify reality. Automation is attractive because "it represents rule-bounded, binary-coded clarity"[581]. This "reductionist allure" of automation, based on the fact that "software at its core is ones and zeroes and nothing in between"[582], should not lead policymakers and citizens to disregard the privacy and dignity risks. Indeed, health apps "expose users to illegitimate information and privacy risks", therefore "users should […] be wary of releasing health information on health apps, as many apps share information with third

---

570 *Id.* at 1179 (citing E. MOROZOV, *To Save Everything, Click Here: The Folly of Technological Solutionism* 5-6 (2013)).
571 *Id.* at 1192. These goals have been called "the Holy Trinity of health care". *Id.* at 1199. *See also* J.L. FLAHERTY, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 *Am. J.L. & Med.* 416, 419 (2014).
572 *Id.* at 1192-93.
573 *Id.* at 1194. For example, an app claimed to "treat seasonal affective disorder ("SAD") and depression" through light therapy, but a smartphone is unable to deliver light in therapeutic doses. *Id.*
574 *Id.* at 1195. *See also* FLAHERTY, *supra* note 571, at 420.
575 *Id.* at 1197.
576 *Id.*
577 *Id.*
578 *Id.*
579 *Id.* at 1198.
580 *Id.* at 1227.
581 *Id.*
582 *Id.*

parties, and it is unclear what these apps do with allegedly "anonymous" and protected information"[583]. Looking more specifically at the "privacy risks posed by accessing one's health record by mobile device", they "might include surveillance, identification, insecurity, disclosure, and aggregation"[584].

We can now look at the interplay between European data protection laws and the development of mobile health apps[585]. On February 5, 2015, the Article 29 Working Party issued a guidance document in order to clarify the scope of the definition of data concerning health in relation to wellbeing apps[586]. The Working Party starts by reaffirming that the category of "medical data" (i.e., "data about the physical or mental health status of a data subject that are generated in a professional, medical context") certainly falls within "health data" even when "generated by devices or apps, which are used in this context, irrespective of whether the devices are considered as 'medical devices'"[587]. However, the concept "health data" has a much broader scope than just medical data, and this is also reflected in the proposed GDPR, as we have seen in Chapter I. For example, health data also includes "disease risk", which refers to "the potential future health status of a data subject". There are also some data generated by lifestyle apps and devices that, according to the Working Party, are "not to be regarded as health data within the meaning of Article 8": this is the case of "data from which no conclusions can be reasonably drawn about the health status of a data subject". There are also grey areas in between, especially "where the data are processed for additional purposes and/or combined with other data or transferred to third parties". According to the Working Party, "even the seemingly most innocuous data, combined with other data sources, and used for other purposes, [can] come within the definition of 'health data'". Therefore, the document tries to "provide a set of criteria that help determine in which cases lifestyle data should be treated as health data". In order to make this assessment, "it does not suffice to look at the character of the data as is", but "[t]heir intended use must also be taken into account". If there is "a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data itself or on the data in combination with data from other sources", then we are dealing with health data. Interestingly, data are considered to fall within health data whenever conclusions can be drawn about an individual's health status or health risk, "irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate".

It is important to note that any processing taking place on the device itself that does not cause data to be transmitted outside the device does not trigger the applicability of data protection laws because of the exception for purely personal use pursuant to Article 3 (2) of the Directive.

As we have seen, the processing of health data needs to rely on a derogation from the general prohibition in Article 8 (1) of the Directive. The Working Party notes that the most likely derogation applying to mHealth apps is explicit consent (Article 8(2)(a)). In order for consent to be legitimate, "information must be made available whether the data will be combined with other data stored on the device or collected from other sources and clear examples of the consequences of such combination of data, what the purposes are of

---

583 FLAHERTY, *supra* note 571, at 440.

584 HELM & GEORGATOS, *supra* note 568, at 150.

585 *See also* European Commission Green Paper on mobile health, 10 April 2014, COM(2014) 219 final, complemented by a Staff Working Document (SWD(2014) 135 final).

586 Article 29 WP Annex on health data in apps (2015).

587 *Id.* According to the Working Party, "medical data" includes "all data related to contacts with individuals and their diagnosis and/or treatment by (professional) providers of health services, and any related information on diseases, disabilities, medical history and clinical treatment". *Id.*

further processing and to what third parties the data may be transferred".

The Working party also advises to apply proper anonymisation techniques and other security measures, including privacy by design and data minimization[588].

The European Data Protection Supervisor (EDPS) has also issued an Opinion in May 2015 concerning Mobile Health[589]. The Opinion agrees with the Working Party on the criteria to assess whether wellbeing data fall within the concept of health data, and maintains that "[i]n the absence of a clear definition, after an assessment of the case-specific circumstances, the notion of what constitutes health data should be construed broadly, so as to include any data relating to a person's physical and mental health"[590]. The EDPS also notes that "considering the multiplicity of parties involved in the mHealth industry and the different role played by each, it can be difficult to identify all controllers and processors and ensure an appropriate allocation of responsibilities", therefore "[e]ach entity must be transparent, visible, accountable, alone or jointly with others, for the handling of personal data it carries out"[591]. Another major issue is the "information asymmetry existing between operators and users", which causes the latter to "have almost no visibility or understanding of the commercial dynamics that entail use of their personal information"[592]. One of the suggestions the EDPS makes is that "controllers and processors make an effort to improve transparency on the way they process, share and re-use personal data as well as on the purposes they aim at"[593]. More precisely, the Opinion argues that apps should allow users "the choice to limit the processing of mHealth data locally – on their smart devices, rather than on a remote server", as well as "the option to freely allow the sharing/transfer of the personal data to a third party or not"[594]. This also goes in the direction of truly enhancing patient empowerment[595]. The EDPS aptly remarks that "[d]esigners and manufacturers should apply the same level of creativity and dynamicity they usually display in introducing attractive devices and apps to also provide individuals with effective and user-friendly privacy notices and setting options"[596]. Clearly, the new principles of "privacy by design" and "privacy by default" introduced by the GDPR will have a great impact on the design of mHealth apps and devices[597].

Turning to the U.S. legal framework on mHealth apps, it deals with the Food and Drug Administration authority, with HIPAA, and with the privacy-promoting efforts by the Federal Trade Commission.

The FDA has jurisdiction over medical devices[598], i.e. "any product intended to diagnose, cure, mitigate, treat, or prevent disease, or any product intended to affect the structure or function of the body (and that is not a drug)"[599]. Thus, the definition of "medical devices" largely depends on the "intended use" language, which has been defined

---

[588] *See* European Union Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices*, 00461/13/EN WP 202 (February 27, 2013), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, at 18-21.

[589] European Data Protection Supervisor, Opinion 1/2015 – Mobile Health – Reconciling technological innovation with data protection, May 21, 2015.

[590] *Id.* at 6.

[591] *Id.* at 8.

[592] *Id.* at 8-9.

[593] *Id.* at 12-13.

[594] *Id.* at 13.

[595] *Id.* at 15.

[596] *Id.* at 13.

[597] *Id.* at 14.

[598] *See* Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 301-99 (2012)).

[599] CORTEZ, *supra* note 564, at 1200-01.

as "the objective intent of how those responsible for marketing the product intend it to be used"[600]. The FDA published a guidance document in 2013 on mobile medical apps, which engages in the hard task of identifying the types of apps that it will and will not regulate[601]. Pursuant to the guidance, "the FDA would regulate only those apps that constitute medical devices and/or pose significant risks to patients"[602]. This means that "[a]pps that are considered medical devices under the FDA guidance nonetheless may escape regulation if they are not considered high-risk"[603]. Despite the fact that the FDA's guidance does not directly address privacy issues, the FDA has nevertheless dealt with "the problem of insecurity in medical devices" by stating that "[t]he need for effective cybersecurity to assure medical device functionality has become more important with the increasing use of wireless, Internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information"[604]. Thus, "mHealth applications seeking approval as medical devices might expect greater success in the FDA approval process if they conform their security features to the FDA's guidance"[605].

Furthermore, some mobile health apps also need to comply with HIPAA, but this is not the case for many of them[606]. As we have discussed, "[f]or HIPAA's privacy protections to apply to a mobile app, that app must involve a covered entity as well as PHI"[607]. This means that "[p]rovider apps that contain patients' PHI would be subject to HIPAA", but, for example, general reference apps operating without PHI are exempt[608]. As to consumer/patient apps, HIPAA "rarely extends to apps used only by individuals because consumers using the app outside of a healthcare setting are not 'covered entities'"[609]. Therefore, some have suggested "expanding regulation by, for example, requiring more apps to be HIPAA compliant"[610].

As to the FTC, it has the power to oversee mHealth within its broader authority to fight unfair competition under the FTC Act[611]. For example, in 2013, the FTC filed an administrative action against LabMD, a clinical lab that tests patients' specimens and reports results through the patients' health care providers[612], and claimed that LabMD's inadequate security features amounted to an "unfair act or practice"[613]. Because consumer protection laws "rely on broader standards, as opposed to narrower definitions, which may become outdated with technological innovation", they "are likely to remain the tool of choice in addressing privacy concerns in the mobile device industry"[614].

We have seen how the legal issues concerning mHealth apps are largely the same as

---

600 *Id.* at 1201 (citing 21 C.F.R. § 801.4 (2013)). *See also* V.J. ROTH, *The mHealth Conundrum: Smartphones & Mobile Medical Apps – How Much FDA Medical Device Regulation is Required?*, 15 *North Carolina Journal of Law & Technology* 359 (2014).

601 *See* U.S. Food & Drug Admin., *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff* (Sept. 25, 2013); CORTEZ, *supra* note 564, at 1202-06.

602 FLAHERTY, *supra* note 571, at 418.

603 *Id.* at 422.

604 HELM & GEORGATOS, *supra* note 568, at 169 (citing *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff* § 1 (2013)).

605 *Id.* at 169-70.

606 FLAHERTY, *supra* note 571, at at 426.

607 HELM & GEORGATOS, *supra* note 568, at 156.

608 *Id.*

609 FLAHERTY, *supra* note 571, at 426. *See id.* at 426-31 for an analysis of three commercially available apps and their compliance with HIPAA.

610 *Id.* at 436.

611 *See generally* 15 U.S.C. §§ 41-58.

612 Complaint, *In the Matter of LabMD, Inc.,* No 9357, F.T.C. (Aug. 28, 2013).

613 *Id.* at 5.

614 HELM & GEORGATOS, *supra* note 568, at 163.

those concerning EHR, especially with respect to the trend towards seeing perfection and efficiency as goals rather than as means to a greater end, i.e. the defense and pursuit of human dignity.

8.2 Cloud Computing: Relevant Issues

Cloud computing has been defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[615]. The use of cloud computing involves "innovations in both technology and business models that create new opportunities – and perils – for healthcare providers and contractors"[616].

Nevertheless, cloud technology is largely used in the healthcare field, and "has taken on such sensitive issues as patient account management, managing patients, HIPAA compliance, patient portals, and appointment scheduling"[617]. As we have seen, "the logic of efficiency and specialization is compelling"[618]. The benefits brought about by the use of cloud computing services in the healthcare arena are several. If a company can avoid setting up its own infrastructures and services and can use those provided by third parties in the cloud, it can gain substantial advantages[619]. Even small enterprises "may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range" [620]. Corporations that use cloud technology "no longer are responsible for maintaining their own information technology structure and can focus on their core competencies"[621]. Furthermore, medical research based on "big data" can generate more accurate and up-to-date results[622]. EHR systems are increasingly stored in cloud computing services. We can identify two different types of EHR: cloud-based and on-premise[623]. Cloud-based EHRs are based in the web and are provided to health care facilities by vendors charging a monthly fee[624]. An important issue concerns ensuring continued access, which depends on the vendor's availability: this can be tackled by establishing an off-site backup server[625]. Another major concern is that of hacking and data breaches[626]. On the other hand, on-premise software requires the medical facility to buy the software package

---

615 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *NIST Cloud Computing Program* (Jan. 28, 2014), available at: http://csrc.nist.gov/groups/SNS/cloud-computing/.

616 F. PASQUALE & T. ADAMS RAGONE, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 *Stan. Tech. L. Rev.* 595, 600 (2014).

617 *Id.* at 601 *See* A.K. SOMAN, *Cloud-based Solutions for Healthcare IT* (2011).

618 PASQUALE & ADAMS RAGONE, *supra* note 616, at 596.

619 A.C. DEVORE, *Cloud Computing: Privacy Storm on the Horizon?*, 20 Alb. L.J. Sci. & Tech. 365, 366-67 (2010).

620 European Union Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196 (July 1, 2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [hereinafter Article 29 WP Opinion 5/2012 on cloud computing], at 4.

621 J. RYAN, *The Uncertain Future: Privacy and Security in Cloud Computing*, 54 *Santa Clara L. Rev.* 497, 513 (2014).

622 *See* PASQUALE & ADAMS RAGONE, *supra* note 616, at 603-04. *See also* President's Council of Advisors on Sci. & Tech., *Report to the President Realizing the Full Potential of Health Information Technology to Improve Health Care for Americans: The Path Forward* (2010), available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf, at 63-64 (recommending use of large databases to improve clinical research).

623 M. TURK, *Electronic Health Records. How to Suture the Gap Between Privacy And Efficient Delivery of Healthcare*, 80 *Brook. L. Rev.* 565, 573 (2015).

624 *Id.*

625 *Id.* at 573-74.

626 *Id.* at 574.

and install it onto their computers[627]. The health care facility is entirely responsible for storing and maintaining data, as well as complying with HIPAA[628]. This second type of system allows for easier control concerning access and security, but is more expensive so that most small facilities are not able to afford it[629].

Also, the proliferation of self-tracking devices that we have just discussed generates an increasing demand of more cloud computing services, both from providers and patients[630].

The use of cloud services in the healthcare sector entails very deep issues. The cloud computing systems "need to be designed to protect the integrity and security of protected health information"[631]. Many problems are connected to certain vulnerabilities that cloud services suffer from: they are "at the mercy of Internet access", and create the risk of breaches of massive databases[632]. Several risks are due either to lack of control over the data, or lack of information on the processing operation (or lack of transparency)[633]. First of all, "cloud clients may no longer be in exclusive control of [personal] data" when they commit them to cloud systems[634]. For example, it will be hard for the cloud client "to shift data and documents between different cloud-based systems" (so-called vendor lock-in), and personal data in the cloud could be "subject to law enforcement requests from law enforcement agencies"[635]. Secondly, "[i]nsufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks"[636]. For instance, the user may not know that chain processing is taking place, or that the processing is occurring in different locations[637].

The European framework on cloud computing has been defined by an Article 29 Working Party Opinion in 2012[638]. This document specifies that the cloud client acts as a data controller, because it "determines the ultimate purpose of the processing and decides on [its] outsourcing […] and the delegation of all or part of the processing activities to an external organisation"[639]. Thus, the cloud client "must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in [the Directive]"[640]. The cloud provider, i.e. the entity that provides the cloud computing services, is considered as a data processor[641]. Therefore, it has a "duty to ensure confidentiality"[642]. Often data processors subcontract additional entities, which then can

---

627 *Id.*

628 *Id.*

629 *Id.* at 575.

630 PASQUALE & ADAMS RAGONE, *supra* note 616, at at 602. *See also id.* at 606 ("[T]here is the growing pressure from patients to develop control over medical record for their own purposes").

631 PASQUALE & ADAMS RAGONE, *supra* note 616, at 653.

632 *Id.* at 601.

633 Article 29 WP Opinion 5/2012 on cloud computing, at 5.

634 *Id.*

635 *Id.* ("There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur"). Other risks connected to the lack of control are: "lack of integrity caused by the sharing of resources", "lack of intervenability due to the complexity and dynamics of the outsourcing chain", "lack of intervenability (data subjects' right", and "lack of isolation". *Id.* at 5-6.

636 *Id.* at 6.

637 *Id.*

638 *See* Article 29 WP Opinion 5/2012 on cloud computing.

639 *Id.* at 7.

640 *Id.* at 8.

641 *Id.*

642 *Id.* at 9.

access the data, and the client must be informed of this instance[643] and, according to the Working Party, provide his consent[644]. The Opinion underlines that the client-provider relationship within the cloud computing scenario must comply with the fundamental data protection principles[645]. Transparency must be ensured, both vis-à-vis the data subject and in the relationship between client, provider and subcontractor[646]. In order to comply with the principles of purpose specification and limitation, the cloud client must determine the purposes of the processing prior to collecting the data and must ensure that the data is not processed for other, non-compatible purposes, also by including appropriate provisions in the contract with subcontractors[647]. Personal data that are not necessary any more must be anonymized or erased, and it must be ensured that erasure is accurate and irretrievable[648]. The controllers must "choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing"[649] and must "sign a formal contract with the cloud service provider"[650]. The contract must specify the measures that shall be implemented to adequately protect personal data[651].

There is one more interesting topic that we can glance at, i.e., international data transfers in the cloud. Interestingly, well before the Schrems decision the Working Party warned that "sole certification with Safe Harbor may not [have been] deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment"[652]. Thus, according to the 2012 Opinion companies exporting data could not merely rely on the claim of the data importer that it had a Safe Harbor certification, but should have "request[ed] evidence demonstrating that [the Safe Harbor] principles [were] complied with"[653]. Also, "several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures" were "not sufficiently addressed" by the Safe Harbor principles, thus it was (and all the more is) "advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud"[654]. It will be extremely interesting to see how we will deal with issues specific to the cloud computing realm in the post-Safe Harbor era.

With respect to the U.S. legislation, we can note that, under the HIPAA Privacy Rule, "liability extends down the chain well beyond covered entities to reach business associates, which include certain subcontractors" [655]. Covered entities and business associates are both directly liable for civil monetary penalties and need to comply with the breach notification rule. A cloud service provider is considered to fall within HIPAA's definition of business associate if it "creates, receives, maintains, or transmits PHI on behalf of a covered entity"[656]. Indeed, the definition of business associate expressly includes

---

643 *Id.*
644 *Id.* at 10.
645 *Id.*
646 *Id.* at 10-11.
647 *Id.* at 11.
648 *Id.* at 11-12.
649 *Id.* at 12. Such measures must accomplish the objectives of availability, confidentiality and integrity and must also pay attention to the complementary data protection goals of transparency, isolation, intervenability, accountability and portability. *Id.* at 14. *See also id.* at 14-17.
650 *Id.* at 12. *See* Data Protection Directive, Art. 17(2)-(3).
651 Article 29 WP Opinion 5/2012 on cloud computing, at 12.
652 *Id.* at 17.
653 *Id.*
654 *Id.* at 18.
655 PASQUALE & ADAMS RAGONE, *supra* note 616, at 607.
656 *Id.* at 608.

a "Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to [PHI] to a covered entity and that requires access on a routine basis to such [PHI]"[657]. This excludes mere conduits of PHI, such as the U.S. Postal Service or Internet Service Providers (ISPs), who provide mere data transmission services[658]. Entities that "maintain" PHI on behalf of covered entities are instead included. The difference between "merely transmitting" and "maintaining" PHI is based on the "transient versus persistent nature" of the opportunity to access the protected information[659]. It is important to note that "[t]he test is persistence of custody, not the degree – if any – of access"[660]. Also considered business associates for the purposes of the HIPAA Privacy Rule are entities that offer PHRs to individuals on behalf of a covered entity[661]. Therefore, a "fact-sensitive inquiry" must be performed in order to figure out whether a vendor offers PHRs on behalf of a covered entity[662]. For instance, if a vendor is hired by a covered entity, which gives it access to PHI in order to allow the vendor to manage a PHR service for the covered entity's patients, it is a business associate[663]. A similar fact-specific analysis must be carried out to understand whether a subcontractor can be considered a business associate[664]. For instance, if the subcontractor is hired to support a business associate with PHR functions, he falls within the definition[665].

9. Comparative Conclusions

The analysis of the different issues arising from electronic health record systems has allowed us to appreciate the importance of adopting a modular, nuanced approach to e-Health phenomena. As we have seen, the pursuit of efficiency *per se* has created tricky incentives and has sometimes overshadowed privacy concerns.

The use of Information and Communication Technology in health care is part of the broader transformation of our society and allows for positive change yet with deep challenges. The benefits arising from the digitization of health records should be pursued together with the enhancement of individual freedom and dignity. Thus, individual privacy does not represent a barrier to the full implementation of EHRs; rather, it provides us with a valuable opportunity to take the different interests into account.

It is most important to bear in mind that the provision of health care services is an intrinsically human activity and should therefore not be deprived of its human features. More efficient and cheaper health care should not lead to the depersonalization of medicine. Doctors' ability to cast judgments and interact with patients should be cherished and should not be replaced by forms and standardized roadmaps. At the same time, patients should not be reduced to a mere stack of data, nor should they be considered absolute masters of their own health. The physician-patient relationship should evolve while keeping its fundamental features. Therefore, given the asymmetry of information and the shortcomings of the informed consent mechanisms, novel solutions should be

---

657 45 C.F.R. § 160.103.
658 PASQUALE & ADAMS RAGONE, *supra* note 616, at 611. *See* Final Omnibus HIPAA Rule Preamble, 78 Fed. Reg. at 5571-72.
659 *Id.*
660 K.C. PLANK, *Cloud Providers Often Are Business Associates Under HIPAA, Officials Say*, 22 *Health L. Rep.* (BNA) 858 (June 6, 2013).
661 45 C.F.R. § 160.103.
662 Final Omnibus HIPAA Rule Preamble, 78 Fed. Reg. at 5572.
663 *Id.*
664 *Id.*
665 *Id.*

envisioned. We have seen examples of how risk assessments by independent experts often possess greater privacy-protective potential than merely seeking consent by requiring patients to sign a form. Rather than a reliance on automatic procedures, a focus on risk assessment and accountability is the means toward a more sound policy.

Chapter III • Anonymization in the Field of Health Data

1. Preliminary Considerations

"Scholars should cast out the myth of perfection, as Lucifer was cast out of heaven. In its place, we should adopt the more realistic, and helpful, conclusion that often good enough is . . . good enough"[1]. This is the concept underlying this whole chapter.

De-identification is certainly one of the main areas of research in the field of privacy law, since in most legal systems anonymized data falls outside the scope of data protection laws. The concept of "anonymity" is conceived as absolute in common language, as "an anonymous person is one of whom you do not know anything, somebody you cannot recognize or identify", but "anonymity in the legal context is actually a relative concept"[2]. Recent studies show how it is very hard, arguably impossible, to fully de-identify data: technological innovation and the interconnected nature of today's world make it relatively easy to match data to a unique individual. Yet, anonymization represents the boundary of privacy law protection. This issue has even deeper effects in the field of health data: on one hand, this kind of data need to be dealt with in a particularly cautious way due to their intrinsically sensitive nature, but on the other hand the ability to re-use health data, e.g. in the field of scientific research, represents a crucially important tool for the progress of medicine.

This chapter aims at carrying out an overview of the existing anonymization standards in the European Union and in the United States, as well as providing some insights on the role of anonymization with respect to health data. As we will see, the two legal frameworks have some differences but share the basic distinction between personal data and anonymized data, which is very clear in theory but proves extremely hard to determine in practice.

Furthermore, this chapter also has another goal, that is, showing that the anonymization debate is one of the clearest examples of the need for privacy law to be less reliant on bright-line standards and more open to a nuanced approach. This is not just a matter of more sound policy or better law, but really it deals with better adhering to the complexity of reality. We need to avoid relying on the anonymized data vs. personal data dichotomy first and foremost because perfect anonymization is impossible and often undesirable. Since reality is more complex than our attempts to build up black and white standards, this work can be a reminder of our need to constantly adapt law to how things really are. As a consequence, this work joins the several voices in privacy law advocating for considering identifiability as a spectrum rather than a two-way alternative. Also, the impossibility to have perfectly de-identified data and the awareness of all the different interests at stake leads us to reflecting on solutions that do not promise perfect efficiency but rather rely on human expertise and relationships. Better privacy protection for health data cannot be achieved by looking for perfect solutions that are not workable, but rather it can be obtained by accepting imperfection and dealing with it, just as we deal with inherent

---

[1] D.E. BAMBAUER, *The Myth of Perfection*, 2 *Wake Forest L. Rev.* 22 (2012).

[2] S. MASCETTI, A. MONREALE, A. RICCI AND A. GERINO, *Anonymity: A Comparison Between the Legal and Computer Science Perspectives*, in S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer 2013, at 88. This is shared by both law and computer science, as they both share "the intuition that simply dropping explicit identifiers is not sufficient to guarantee anonymity". *Id.* at 107.

flaws in all things that are human.

2. Legal Standards for Anonymization

In both the EU and the United States privacy legislation anonymization is mentioned and employed as a mechanism that puts data outside the scope of protection. Only "personal data" are protected, and as we will see it is important to understand the scope of the concept of "personal data" in these two legal systems. Generally speaking, it has often been said that the European definition tends to be too broad, whereas the US concept often seems too narrow[3]. However, both frameworks are based on the assumption that "[w]here […] data are truly non-identifiable, privacy interests are minimal" [4]. Anonymization basically "grant[s] a get-out-of-jail-free card to those who anonymize their data"[5]. However, very often "[d]efinitions of anonymity in privacy laws and regulations do not provide an operational method to follow for anonymising health information"[6]. As we will discuss, "anonymization" is a term that "simply overpromise[s]"[7], which means that existing legal standards must be revisited and rethought.

2.1 Anonymization in the European Union

According to the Data Protection Directive 95/46/EC, anonymized data are not subject to the principles of protection[8] as long as the anonymization process has been successful, i.e., as long as there is nothing which through reasonable effort may lead to re-identifying the data subject[9]. In other words, anonymization consists in "processing personal data in order to irreversibly prevent identification"[10].

EU lawmakers kept anonymized data outside the scope of data protection law because they sought to provide "room for unencumbered innovation and free expression"[11]. However, because of new advancements in technology, some commentators have argued that the risk of re-identification is growing. Because re-identification techniques have now expanded the European concept of 'personal data' to include

---

[3] *See* P. SCHWARTZ & D. SOLOVE, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 *NYU L. Rev.* 1814, 1817 (2011) (criticizing "both the United States' reductionist view of PII, and the European Union's expansionist view"). "In the reductionist view, the tendency is to consider PII as only that personal data that has been specifically associated with a specific person. That model protects only identified data, and thereby leaves too much personal information without legal protections. In the expansionist approach, it is irrelevant if information has already been linked to a particular person, or might be so linked in the future; this view treats identified and identifiable data as equivalent". *Id.*

[4] L.O. GOSTIN & J.G. HODGE, JR., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 *Minn. L. Rev.* 1439, 1459 (2002).

[5] P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. Rev.* 1701, 1704 (2010).

[6] K. EL EMAM, S. RODGERS, B. MALIN, *Anonymising and sharing individual patient data*, BMJ 2015; 350 :h1139, at 1.

[7] I.S. RUBINSTEIN AND W. HARTZOG, *Anonymization and Risk*, New York University School of Law, Public Law & Legal Theory Research Paper Series, Working Paper No. 15-36 (2015), at 48.

[8] *See* Data Protection Directive, Recital 26.

[9] *Id.*

[10] European Union Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP 216 (April 10, 2014) [hereinafter Article 29 WP Opinion 05/2014 on anonymisation techniques], at 3.

[11] *See* OHM, *supra* note 5, at 1737-38 (casting doubt on the power of anonymization as a "stand-in for a meaningful cost-benefit balancing").

potentially all data[12], they fear that the EU Data Protection Directive is becoming "overbroad – in fact, essentially boundless . . . [and is] disrupting the careful legislative balance between privacy and information and extending datahandling requirements to all data in all situations"[13]. This is why Schwartz and Solove defined the European approach as "expansionist", as opposed to the "reductionist" U.S. view[14]. The Article 29 Working Party has always been aware of the need to carefully balance the scope of the concept of "personal data" and of the data protection rules, highlighting how it "should not be overstretched" nor should it be "unduly restrict[ed]"[15].

The Opinion released by the Article 29 Working Party, together with other documents such as the code of good practice published by the UK Information Commissioner's Office[16], aims at bridging the gap left by the Directive, which does not provide guidance on anonymization standards and "encourage[s] the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive"[17]. Therefore, the Opinion analyzes "the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection" and providing "recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them"[18].

2.1.1 Anonymization in the Data Protection Directive

In order to understand what anonymizing data means in the EU legal framework, we need to inquire into what is considered "personal data". As we have seen in Chapter I, the Directive adopts a very broad definition, including "any information relating to an identified or identifiable natural person ('data subject')"[19]. A pivotal role is played by the concept of identifiability, since identifiable data is given the same protection as identified data[20]. On one hand, this can be seen as "in tune with technology"[21], because of the increasing risks of re-identification, but on the other hand it has been criticized for its virtually boundless potential expansion and because the two situations are actually quite different[22]. Indeed, "[d]ifferent levels of effort will be required to identify information, and

---

12 *Id.* at 1763.
13 *Id.* at 1741.
14 SCHWARTZ & SOLOVE, *supra* note 3, at 1873-74.
15 Article 29 WP Opinion 4/2007 on the concept of personal data, at 5.
16 UK Information Commissioner's Office, ANONYMISATION: MANAGING DATA PROTECTION RISK CODE OF PRACTICE (2012), available at: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf [hereinafter UK ICO Code].
17 Data Protection Directive, Art. 27(1); *see also id.*, Recital 26 (stating, in relevant part, "codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible").
18 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 3.
19 Data Protection Directive, Art. 2(a). See Article 29 WP Opinion 4/2007 on the concept of personal data.
20 This equalization was brought about by the German Federal Data Protection Act of 1977 which first put the two situations on the same level. *See* SCHWARTZ & SOLOVE, *supra* note 3, at 1874 (describing how in the European mindset the risk of re-identification was predicted from the very start and there was no difference in treatment between data relating to 'identified' and 'identifiable' individuals).
21 SCHWARTZ & SOLOVE, *supra* note 3, at 1875.
22 *Id.* at 1876.

varying risks are associated with the possible identification of data," so it is arguably erroneous to fit both in the same category[23].

Pursuant to the Directive, "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[24]. A person can first of all be identified "directly": the "name" is the most common direct identifier, even if sometimes it needs to be combined with other pieces of information[25]. The identification, though, can also occur "indirectly", that is, through "unique combinations," and this is what the last part of the clause ("in particular by reference to…") refers to[26]. A name may not be necessary when other identifiers can be used to single the individual out[27]. Therefore, the European Court of Justice has held that "identifying [various persons] by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data"[28].

According to Recital 26 of the Data Protection Directive, in order to assess whether the person is identifiable, "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Therefore, it looks like the Directive uses a "reasonableness" standard to assess whether data are sufficiently de-identified[29]. In order to apply the "all the means reasonably to be used" criterion, several factors must be taken into account, including: (1) the cost of conducting identification, (2) the intended purpose, especially considering that "where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means likely reasonably to be used" to do so and "the information should be considered as relating to identifiable individuals", (3) the way the processing is structured, (4) the advantage expected by the controller, (5) the interests at stake for the individual, (6) the risk of organizational dysfunctions (like breaches of confidentiality duties) and technical failures, (7) the state of the art in technology at the time of processing and the possibilities for development throughout the time for which the data will be processed[30].

After the initial period of time during which the retention of data in a form which permits identification is necessary for the purposes for which the data was collected or are further processed, data needs to be either erased or, if kept, anonymized[31]. An exception is

---

[23] *Id.*

[24] Data Protection Directive, Art. 2(a). In the same direction goes, for instance, Article 2(a) of the Convention 108 of the Council of Europe.

[25] Article 29 WP Opinion 4/2007 on the concept of personal data, at 13.

[26] *Id.*

[27] *Id.* at 14.

[28] Lindqvist, Case C-101/01, [2003] E.C.R. I-12992, ¶ 27.

[29] *See* R. GELLMAN, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 *Fordham Intell. Prop. Media & Ent. L.J.* 33, 43 (2011). There is a potential difference between the wording of the Directive, that refers to "all means likely reasonably to be used" and that of some national provisions that do not refer to a reasonableness standard, but the UK ICO Code maintains that "the practical problems that arise are much the same whether the test is of 'likelihood' of identification or 'reasonable likelihood' of it', especially considering that the national courts often refer directly to the EU Directive. UK ICO Code, *supra* note 16, at 12-14 (mentioning, e.g., the United Kingdom case R (on the application of the Department of Health) v Information Commissioner [2011] EWHC 1430 (Admin)). It has been written that the UK Data Protection Act can be considered as "incorporat[ing] a reasonableness test implicitly". GELLMAN, at 45-46 n.66.

[30] Article 29 WP Opinion 4/2007 on the concept of personal data, at 15-16.

[31] *See* Handbook on European data protection law 39 (2014), *available at* http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law, at 44, 73. Directive 2002/58/EC , Recital 9 considers "minimizing the processing of personal data" and "using anonymous or

carved out for the retention of data in a personalized form for the purpose of historical, statistical or scientific use, provided that appropriate safeguards against misuse are applied[32]. Looking more specifically at health records, the Article 29 Working Party specified in 2007 that "whenever feasible and possible, data from EHR systems should be used for other purposes (e.g. statistics or quality evaluation) only in anonymised form or at least with secure pseudonymisation"[33]. Similarly, the Recommendation on cross-border interoperability of electronic health record systems released by the European Commission in 2008 calls for a "comprehensive legal framework"[34] that should recognize the principle of only collecting, processing or using "as little personal data as possible", employing all the chances for anonymization as long as they are feasible and "the effort involved is reasonable in relation to the desired level of protection"[35].

Despite the fact that the Directive uses a "reasonableness" standard to assess identifiability, it focuses on the outcome of anonymization process, i.e., "that data should be such as not to allow the data subject to be identified via "all" "likely" and "reasonable" means"[36]. The Article 29 Working Party opinion "never quite resolves [the] tension in European data protection law between the legal implications of anonymization", referring to perfectly achieved de-identification, and the "reasonableness standard for determining whether a person is identifiable"[37]. The UK Information Commissioner's Office has engaged in the attempt to make the threshold more workable by underlining how this does not mean that data are considered personal data when there is the mere possibility of identification; rather, the focus is only on whether re-identification can be attained through all likely (and reasonable, in the EU directive) means[38]. The code is "risk tolerant and focused on process rather than output"[39], something we will discuss in the last part of this chapter. Nevertheless, the European provisions are clear: the underlying rationale is that "the outcome of anonymisation […] should be as permanent as erasure, i.e., making it impossible to process personal data"[40]. In the same direction goes the clarification that the intentions of the data controller or recipient are irrelevant[41]. This focus on the outcome is probably misplaced, since as we will see in Paragraph 4 we should refrain from relying too much on anonymization *per se*. Interestingly, the European Data Protection Supervisor has established a distinction between anonymous data for the purposes of data protection law and statistical anonymous data[42]. The first consist in data which cannot lead to re-

---

pseudonymous data where possible" objectives of which the Member States should "[take] particular account."

[32] Data Protection Directive, Art. 6(1)(e).

[33] Article 29 WP Working Document 2007 on EHR, at 16.

[34] European Commission Recommendation on cross-border interoperability of EHR systems, at 14.

[35] *Id.* at 14(c).

[36] Article 29 WP Opinion 05/2014 on anonymisation techniques, at 6.

[37] RUBINSTEIN & HARTZOG, *supra* note 7, at 43.

[38] UK ICO Code, *supra* note 16, at 12 (concluding that "although it may not be possible to determine with absolute certainty that no individual will ever be identified as a result of the disclosure of anonymised data, this does not mean that personal data has been disclosed" and mentioning an opinion from the UK High Court that states that the risk of identification must be greater than remote and reasonably likely for information to be classified as personal data under the DPA. R (on the application of the Department of Health) v Information Commissioner [2011] EWHC 1430 (Admin)).

[39] RUBINSTEIN & HARTZOG, *supra* note 7, at 43.

[40] Article 29 WP Opinion 05/2014 on anonymisation techniques, at 5.

[41] *Id.* at 10.

[42] M.V. DE AZEVEDO CUNHA, D. DONEDA, N. ANDRADE, *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriori finalità: sfide alla* privacy, *Ciberspazio e diritto* 2010, Vol. 11, n. 4, 641, 646 (2010). *See* European Data Protection Supervisor, *Opinion on the proposal for a Regulation of the European Parliament and of the Council on European Statistics*, COM(2007) 625 final (2008), OJ C 308, at 4; European Data Protection

identification at all, according to the evaluations we have just discussed, whereas "statistical anonymous data" cannot lead to direct re-identification but might include an indirect chance of re-identification[43].

Some of the explanations provided by the Article 29 Working Party, though, go in the direction of a risk assessment approach. The Working Party highlights that anonymization must be engineered in an appropriate way, which means that "the optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion"[44]. Data controllers are also warned against considering anonymization as a "one-off exercise": because it is an active field of research and because even anonymized data may be used to enrich existing profiles of individuals, thereby leading to re-identification, data controllers cannot rely on the "release and forget" approach[45]. Rather, they should (i) identify new risk and re-evaluate the residual risks regularly, (ii) assess whether the controls for identified risks suffice and adjust accordingly, and (iii) monitor and control the risk[46].

2.1.2 Anonymization in the GDPR

The proposed General Data Protection Regulation aims at introducing many important changes, but "[d]espite much anticipation [it] did not significantly alter the definition of "personal data" and the related concept of anonymization"[47]. In particular, the proposed Recital 23 replaces "likely reasonably to be used" with a more euphonic "reasonably likely to be used" but maintains the dichotomy between anonymized data and personal data (covered by data protection law), which has been considered an "outmoded"[48] approach for several reasons that we will further discuss below[49], including the fact that some commentators propose assessing the identifiability of data "on a spectrum", i.e. considering not only technical de-identification but also legal and administrative safeguards that may decrease the risk of re-identification[50]. Quite disappointingly, the Regulation specifies that it "does […] not concern the processing of […] anonymous information", i.e., "information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable"[51]. Recital 23 also adds a new clause, which asks data controllers that try to "ascertain whether means are reasonably likely to be used to identify the individual" to take into account "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development." This goes in the

---

Supervisor, *Opinion on the proposal for a Regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work*, COM(2007) 46 final, at 4.

[43] *Id.*

[44] Article 29 WP Opinion 05/2014 on anonymisation techniques, at 3-4.

[45] *Id.*, p. 23.

[46] *Id.*, p. 4, 24. *See also* UK ICO Code, *supra* note 16, at 21.

[47] O. TENE, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 *Ohio St. L.J.* 1217, 1233 (2013).

[48] *Id.* at 1242.

[49] See Paragraph 4.

[50] O. TENE & C. WOLF, *Future of Privacy Forum – White Paper. The Definition of Personal Data: Seeing the Complete Spectrum* (2013), at 5; *see also* K. EL EMAM, *Risk-based de-identification of health data*, *IEEE Security & Privacy* 2010, 8:64-67.

[51] GDPR – Consolidated text, Recital 23.

same direction as that envisioned by the Article 29 Working Party, and makes it even more advisable to follow its recommendations.

The proposed Article 10 clarifies that "[i]f the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with [the] Regulation" [52]. This can be a "powerful incentive" to use anonymization[53].

Despite the attempt to underline how the assessment of the risk of re-identification is based on a multi-factor test, it is quite disappointing to see that the long-awaited new Regulation does not even make a small step in the direction of abandoning the dichotomy between personal and anonymous data, and is therefore already obsolete.

2.1.3 The Italian Legal Framework on Anonymization

We will now take a look at the Italian example to see how the provisions on anonymization have been implemented in this Member State.

Unlike the Directive, the Italian Data Protection Code explicitly defines "anonymous data" as "any data that either in origin or on account of its having been processed cannot be associated with any identified or identifiable data subject"[54].

Section 3 of the Data Protection Code, while establishing the "Data Minimisation Principle", specifies that "[i]nformation systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively"[55]. Therefore, anonymization plays an important role in the practical application of this fundamental principle. Similarly, the Garante's Authorization no. 9/2014 on scientific research specifies that only "such operations as are absolutely indispensable to conduct the given study" should be implemented[56]. Only "[i]f the research cannot achieve its objectives without identifying data subjects, also transiently", then a different rule triggers: "encryption techniques shall be implemented or ID codes used or any other solutions shall be implemented that – by having regard to the number of cases considered – prevent the data in question from being traced back directly to the data subjects"[57]. Anyways, the measures taken must "only allow [data subjects] to be identified where necessary"[58]. The Garante further specifies that "the codes to be used may not be

---

[52] *Id.*, Art. 10.

[53] C. KUNER, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Privacy & Security Law Report, 11 PVLR 06, 02/06/2012. Copyright 2012 by The Bureau of National Affairs, Inc., at 5.

[54] Italian Personal Data Protection Code, Section 4 (1) (n).

[55] Italian Personal Data Protection Code, Section 3. The same concept is expressed, in more specific cases, in Section 22 (3) ("Public bodies may process exclusively such sensitive and judicial data as are indispensable for them to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature.") and Section 22 (6) ("Sensitive or judicial data that are contained in lists, registers or data banks kept with electronic means shall be processed by using encryption techniques, identification codes or any other system such as to make the data temporarily unintelligible also to the entities authorised to access them and allow identification of the data subject only in case of necessity, by having regard to amount and nature of the processed data.").

[56] Garante – Authorisation no. 9/2014, Paragraph 5.

[57] *Id.*

[58] *Id.*

derived from the personal data identifying data subjects - except where this proves impossible on account of the specific features of the processing or requires clearly disproportionate efforts, whereupon the relevant grounds must be specified in writing in the research project". The provisions on EHRs confirm that whenever data from FSE are used for scientific purposes they should be de-identified[59].

Identification data, i.e., "personal data allowing a data subject to be identified directly"[60], are dealt with in Section 104 concerning statistical and scientific purposes. According to this provision, "account shall be taken with regard to identification data of all the means that can be reasonably used by a data controller or others to identify the data subject, also on the basis of the knowledge acquired in connection with technological developments"[61].

Consistent with the approach taken in virtually all legal systems, anonymous data can be freely disclosed. Indeed, the Authorization on the processing of health data states: "the possibility to disclose anonymous data, whether aggregated or not, and include them into publications for scientific, educational, preventive or information purposes in the medical sector shall also be left unprejudiced"[62].

With respect to electronic health records, we have seen that the provisions on the FSE in Italy sometimes require de-identification. The removal of directly identifying data is required, for instance, when the data contained in the FSE are processed for the purposes of "study and scientific research in the medical, biomedical and epidemiological field"[63]. Furthermore, among the security measures we can find "procedures of anonymization of the directly identifying elements"[64].

2.2 Anonymization Standards in the United States

As we have seen, in the United States there is no unique comprehensive law on data protection: rather, the US framework is featured by a sector-specific approach. Similarly to how it works in the EU, though, protection is only granted to "personal data", *rectius*, "personally identifiable information" (PII), a concept which thus is said to serve a "gatekeeping function"[65]. As Schwartz and Solove highlighted, this concept "defines the scope and boundaries of a large range of privacy statutes and regulations", as they "all share the same basic assumption – that in the absence of PII, there is no privacy harm"[66].

The U.S. legal system has been said to be "only dimly cognizant of the deidentification model", as "while the federal standards are generally inapplicable to deidentified health information, they do not require deidentification"[67]. The lack of awareness as to the re-identification risk is a flaw that the U.S. approach shares with the

---

[59] Decree-law no. 179 of 2012, Art. 16.1.
[60] Italian Personal Data Protection Code, Section 4 (1) (c).
[61] *Id.*, Section 104 (2).
[62] Garante – Authorisation No. 2/2014, Paragraph 7.
[63] FSE DPCM, Art. 15. *See* Decree-law no. 179 of 2012, Art. 12.2 b) and Art. 16.1.
[64] FSE DPCM, Art. 23.5 g) ("Per la consultazione in sicurezza dei dati contenuti nel FSE sono assicurati: […] g) procedure di anonimizzazione degli elementi identificativi diretti, come definito dai decreti attuativi di cui all'articolo 35 del decreto legislativo 23 giugno 2011, n. 118, per il perseguimento delle finalità di cui ai punti b) e c) del comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, fermo restando quanto previsto dall'articolo 15, comma 25-bis, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135").
[65] SCHWARTZ & SOLOVE, *supra* note 3, at 1815.
[66] *Id.* at 1816.
[67] N.P. TERRY, *What's Wrong With Health Privacy?*, 5 *J. Health & Biomedical L.* 1, 3 (2009).

European model, whereas the two frameworks differ with respect to other aspects. For instance, the U.S. standards have been said to adopt a "reductionist" view of personal data, which are seen as only those data that "[refer] to a currently identified person"[68].

We are now going to analyze the anonymization standard provided by the FTC, by the HIPAA Privacy Rule, by the so-called Common Rule, and by the NIST.

2.2.1 The Federal Trade Commission Standard

The report "Protecting Consumer Privacy in an Era with Rapid Change: Recommendations for Businesses and Policymakers"[69] was published by the FTC in March 2012 and provides, as of today, the FTC's view on anonymization.

The 2012 Report created a privacy framework "intended to articulate best practices for companies that collect and use consumer data"[70], necessary because of how "[blurred] the traditional distinction between personally identifiable information and 'anonymous' data has [become]"[71]. For instance, the 2012 Report refers to Google's comment to the draft report that, "[s]upporting a scaled approach rather than a bright line distinction, . . . noted that all data derived from individuals deserves some level of protection"[72]. This awareness is very interesting in the context we are analyzing, since it reveals an attempt to focus on what is at stake rather than on merely complying with legal standards.

Despite the fact that FTC report does not directly deal with health data, it is useful for us to analyze the provisions on anonymization in order to make useful comparisons and gain some insights. The FTC privacy framework applies to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties"[73]. The FTC chose to consider data that is not just "linked" but rather "linkable" to face the new technological developments and the incentives for companies to engage in efforts to re-identify data[74]. The FTC does not rely on the unhelpful concept of PII, as individuals can be re-identified from publicly released datasets that do not contain PII[75].

The FTC's definition of anonymous data is then: data that cannot be reasonably linked to a specific consumer, computer, or other device. In particular, the FTC provided some guidance, in order to address some of the commenters' concerns that the standard was "overly broad," to give companies an incentive to use data in a de-identified form and

---

[68] SCHWARTZ & SOLOVE, *supra* note 3, at 1873. This remark refers especially to "the FTC's view of a "persistent identifier", such as a cookie" and to "the Privacy Act's definition of a "system of records"". *Id.*

[69] FEDERAL TRADE COMMISSION, Protecting Consumer Privacy in an Era with Rapid Change: Recommendations for Businesses and Policymakers (March 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter 2012 FTC Report]. In 2013 the FTC underlined that it is not part of its policy to "provide specific technical guidance in areas like [anonymization], which are constantly changing," because it is "a company's responsibility to keep abreast of and select the technology that it believes best meets its needs and requirements while appropriately protecting consumer privacy. Therefore, it reinstated its reliance on the 2012 report. FTC's Letter to Commenter Electronic Privacy Information Center (EPIC), within *In the Matter of Compete, Inc.*, February 25, 2013, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competeepicletter.pdf.

[70] 2012 FTC Report, at vii.

[71] *Id.* at 2.

[72] *Id.* at 19 (citing *Comment of Google Inc.*, cmt. #00417, at 8).

[73] *Id.* at 22.

[74] *Id.* at 20.

[75] *Id.* at 18.

to promote accountability[76]. Thus, it specified that data can be considered "not reasonably linkable to a particular consumer, computer or device," and therefore fall out of the scope of the framework, provided that the company implements three protections for such data[77]. The three requirements envisioned by the FTC are:

(1) The company "must take reasonable measures to ensure that the data is de-identified," i.e. it must reach a "reasonable level of justified confidence that the data cannot reasonably be […] linked to a particular consumer, computer, or other device." [78] Therefore, the data set must be "not reasonably identifiable."[79] The report further clarifies that to understand what is a "reasonable level of justified confidence" the company must make a case-by-case judgment looking at: a) the particular circumstances, including the available methods and technology, b) the nature of the data, and c) the purposes for which the data will be used (e.g., external publication or not…)[80]. The Commission also made clear that this is not an absolute standard, but rather "companies must take reasonable steps to ensure that data is de-identified": various techniques can be deemed reasonable based on a case-by-case judgment[81].

(2) The company must "publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data." [82] Attempts of re-identification can be actionable under Section 5 of the FTC Act.

(3) The company should contractually prohibit the entities to which it makes the de-identified data available from attempting to re-identify it,[83] or, in other words, it should require "any downstream users of the data to keep it in de-identified form."[84] Additionally, it should "exercise reasonable oversight to monitor compliance with these contractual provisions" and appropriately address violations.[85]

It is interesting to notice how the FTC does not focus simply on a "factual" concept of identifiability, which would have been a very risky choice given the huge developments in re-identification techniques, but rather "shifts the crux of the inquiry . . . to a *legal* examination of an organization's *intent* and *commitment* to prevent re-identification"[86]. As we will discuss below, this goes in the right direction as it shifts the focus from compliance to human judgment. Indeed, this approach is much more realistic in that it accepts the fact that meaningful de-identification must be based on all the relevant factors and that privacy protection is an inherently human activity.

---

[76] *Id.* at 22.

[77] *Id.* at 21. The Commission mentioned its closing letter to Netflix as a "good illustration" of these principles. *Id.* (citing Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix, 2 (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf).

[78] *Id.* at 21.

[79] *Id.* at 22.

[80] *Id.* at 21.

[81] *Id.* The Commission mentioned some techniques (deletion or modification of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data) but invited companies and researchers to keep on innovating in the field. *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.* at. 22.

[85] *Id.* at 21.

[86] O. TENE & J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 *Nw.J. Tech. & Intell. Prop.* 239, 259 (2013).

2.2.2 The HIPAA Privacy Rule Standards

The HIPAA Privacy Rule provides a very detailed standard for anonymization, which is an exception in the comparative landscape as "[n]o other country has developed a more rigorous or detailed guidance for how to convert personal data covered by privacy regulations into non-personal data"[87].

The outcome of de-identification (HIPAA refers to 'de-identification' rather than 'anonymization') is "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual"[88]. This data is not considered "individually identifiable health information"[89]. Congress and HHS enumerated a list of identifiers in order to protect privacy and allow health professionals to trade health data without infringing on patient privacy. A HIPAA-covered entity[90] has two options to de-identify patient data.

As to the first option, it consists in hiring a statistician[91] who "(i) determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) documents the methods and results of the analysis that justify such determination."[92] In other words, the statistician must "determine which of the 18 identifiers [listed by the statute can be retained] without creating more than a 'very small' risk that the data could be re-identified when publicly released"[93].

The second available option is the so-called 'safe harbor' method, consisting in stripping the data of all of the 18 identifiers listed by the statute[94], combined with not having "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information"[95]. The eighteen "identifiers of the individual or of relatives, employers, or household members of the individual" that must be removed are[96]: (A) names; (B) all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their

---

[87] J. CLINE, *Privacy Matters: When Is Personal Data Truly De-Identified?*, COMPUTERWORLD (July 24, 2009). He also adds this rule "arguably has saved lives".

[88] 45 C.F.R. § 164.514(a).

[89] *Id.*

[90] *See* Chapter I, Paragraph 4.1.3.

[91] In particular, the statute refers to "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable." 45 C.F.R. § 164.514(b)(1). The Electronic Privacy Information Center has noticed how there are no "specific guidelines on threshold requirements that would allow qualified statisticians to make determinations that a particular set of data has been adequately de-identified," therefore there is the risk that the statisticians will use different methodologies and will not be held to the same standards throughout the nation, not to mention the risk of covered entities "seek[ing] out" statisticians that are more likely to "minimize their notice obligations." Comments of the Electronic Privacy Information Center (EPIC) to the Federal Trade Commission, "Health Breach Notification Rulemaking," Project No. R911002 (2009), p. 6-7.

[92] 45 C.F.R. § 164.514(b)(1)(i)-(ii).

[93] CLINE, *supra* note 87.

[94] 45 C.F.R. § 164.514(b)(2).

[95] *Id.* § 164.514(b)(2)(ii). This provision has been praised for its inclusion in the 'threat model' of insiders with specialized knowledge and not just outsiders. F. T. WU, *Defining Privacy and Utility in Data Sets*, 84 *U. Colo. L. Rev.* 1117, 1156 (2013). Conversely, the Electronic Privacy Information Center has noted how this would provide "too much leeway to regulated entities." Comments of the Electronic Privacy Information Center (EPIC) to the Federal Trade Commission, "Health Breach Notification Rulemaking," Project No. R911002 (2009), p. 7.

[96] 45 C.F.R. § 164.514(b)(2)(i).

equivalent geocodes[97]; (C) all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older[98]; (D) telephone numbers; (E) fax numbers; (F) e-mail addresses; (G) social security numbers; (H) medical record numbers; (I) health plan beneficiary numbers; (J) account numbers; (K) certificate/license numbers; (L) vehicle identifiers and serial numbers, including license plate numbers; (M) device identifiers and serial numbers; (N) web URLs; (O) IP address numbers; (P) biometric identifiers, including finger and voice prints; (Q) full face photographic images and any comparable images; and (R) any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section[99].

A covered entity may retain the chance to re-identify the data by assigning "a code or other means of record identification" if two requirements are met[100]. The first is the "derivation" requirement, according to which "the code or other means of record identification [must not be] derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual"[101]. The second requirement concerns "security" and provides that the entity cannot "use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification"[102].

Alternatively, the covered entity may choose the "limited data set" method[103], which calls for removing 16 of the 18 identifiers[104] and protecting the remaining data with additional security measures. Information in these 'limited data sets' may include addresses other than street name or street address or post office boxes, all elements of dates and any unique codes or identifiers not listed as direct identifiers[105]. It is important to bear in mind that this method does not achieve anonymization and the data is still regarded as protected

---

[97] An exception is carved out for "the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000." *Id.* § 164.514(b)(2)(i)(B)(1)(2).

[98] Birth dates must be generalized to years and ZIP codes to their initial three digits because of the release of a famous study according to which it is possible to identify most of the American population based on sex, ZIP code and birth date. *See* OHM, *supra* note 5, at 1737; L. SWEENEY, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3. *See also* P. GOLLE, *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 *ACM Workshop on Privacy in the Elec. Soc'y* 77, 78 (2006).

[99] 45 C.F.R. § 164.514(b)(2)(i)(A)-(R).

[100] *Id.* § 164.514(c).

[101] *Id.* § 164.514(c)(1). "For example, an encrypted individual identifier (e.g., a social security number) would not meet the conditions for use as a re-identification code for de-identified health information because it is derived from individually identified information." NIH Publication Number 04-5489, RESEARCH REPOSITORIES, DATABASES, AND THE HIPAA PRIVACY RULE 3 (2004).

[102] *Id.* § 164.514(c)(2).

[103] *Id.* § 164.514(e).

[104] The identifiers that must be excluded from the limited data set are: (i) names; (ii) postal address information, other than town or city, State, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) e-mail addresses; (vi) SSNs; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web URLs; (xiv) IP address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images. *Id.* § 164.514(e)(2)(i)-(xvi).

[105] If compared with the list in § 164.514(b)(2)(i), we can see this list allows retention of some geographic information and does not include dates nor the catch-all eighteenth identifier.

health information subject to HIPAA[106]. However, the dataset can still be used or disclosed, "only for the purposes of research, public health, or health care operations"[107], provided that the covered entity receives "satisfactory assurance, in the form of a data use agreement . . . that the limited data set recipient will only use or disclose the protected health information for limited purposes"[108]. If the limited data set recipient engages in a "pattern of activity or practice . . . that constitute[s] a material breach or violation of the data use agreement", the covered entity will be considered in compliance with HIPAA only if it did not know about it or, if it did know, if it took "reasonable steps to cure the breach or end the violation"[109].

Furthermore, the HIPAA Privacy Rule provides that a "covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity"[110]. These requirements do not apply to data that has been de-identified under § 164.514(a) and (b) provided that (i) disclosure of code or other means of record identification that allow re-identification amounts to disclosure of PHI; and (ii) if de-identified information is re-identified, it can only be disclosed as permitted or required by § 164.502[111].

As always happens with exhaustive lists, the list of identifiers has been criticized because of its reliance on the allegedly flawed assumption that any information other than those 18 identifiers cannot be used for re-identification[112]. Meanwhile, it provides a clear rule for companies in a field that is usually left to each company's understanding of vague standards. Indeed, the safe harbor method "offers the promise of a straightforward application of rules, a repeatable process, and a known result"[113]. The need for workable standards should not be overlooked, especially if we consider all the different interests at stake with respect to the exchange of data.

---

[106] Some studies have further demonstrated that limited data sets should not be considered properly de-identified since the risk of re-identification ranges from 10% to 60%. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Internal Report 8053, De-Identification of Personal Information* (2015) [hereinafter NIST Internal Report 8053], at 26. *See* D. LAFKY, *The Safe Harbor Method of De-Identification: An Empirical Test, Department of Health and Human Services*, Office of the National Coordinator for Health Information Technology, October 8, 2009, available at: http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf; BENITEZ & MALIN, note 169.

[107] *Id.* § 164.514(e)(3)(i).

[108] *Id.* § 164.514(e)(4)(i). Such data use agreement must meet the requirements specified in § 164.514(e)(4)(ii).

[109] *Id.* § 164.514(e)(4)(iii)(A). If such steps were unsuccessful, the covered entity can still be compliant if it "(1) discontinued disclosure of protected health information to the recipient; and (2) reported the problem to the Secretary." *Id.*

[110] *Id.* § 164.502(d)(1).

[111] *Id.* § 164.502(d)(2).

[112] OHM, *supra* note 5, at 1738. For instance, HIPAA excludes from the list data about patient visits (like hospital name, diagnosis, year of visit, patient's age, and the first three digits of ZIP code) that "an adversary with rich outside information can use to defeat anonymity." *Id.* at 1740. Therefore, Ohm maintains that "HIPAA's approach to privacy is like the carnival whack-a-mole game: as soon as you whack one mole, another will pop right up. No matter how effectively regulators follow the latest reidentification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII will never stop growing until it includes everything." *Id.* at 1742 (citing Appendix B of the draft version of A. NARAYANAN & V. SHMATIKOV, *De-Anonymizing Social Networks*, in *Proc. 2009 30th IEEE Symp. On Security & Privacy 173* (the draft version is available at http://arxiv.org/pdf/0903.3276.pdf); I. DINUR & K. NISSIM, *Revealing Information While Preserving Privacy*, in *Proc. 22nd ACM Symp. On Principles Database Sys.* 202, 203 (2003).

[113] NIST Internal Report 8053, at 24.

Some scholars have pointed out that "[t]he quality of de-identification may vary among different EHR systems", as "de-identification capacity often is not designed into [them], and, thus, it must be added after data is exported from an EHR system", resulting in a "very labor-intensive and time-consuming" process[114]. Therefore, "if de-identification is not automated, it would need to be assigned to trusted professionals"[115].

2.2.3 Federal Policy for the Protection of Human Subjects (or the "Common Rule")

The regulations concerning research on human subjects were based on a report published by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (the so-called Belmont Report), which identified some basic ethical principles for all human subjects research. In 1991 the "Common Rule" was issued by several federal department and agencies[116]. It sketches the basic provisions about Institutional Review Boards (IRBs) and informed consent. The head of the relevant department or agency retains final judgment as to whether a particular activity is covered by the Common Rule[117].

The Common Rule involves "human subjects,"[118] i.e. "living individuals about whom an investigator […] conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information"[119]. In order for information to be "private," it must be "individually identifiable"[120]. This means that "the identity of the subject is or may be readily ascertained by the investigator or associated with the information"[121].

Health research that uses information that is not individually identifiable is exempt from the Common Rule (and therefore from IRB oversight), under 45 C.F.R. § 46.101(b)(4). Specifically, the provision exempts from the policy "research, involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or *if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects* [emphasis added]"[122]. This standard is obviously less stringent than the HIPAA Privacy Rule, leading to situations in which some data is exempt from the Common Rule but still subject to the Privacy Rule.[123]

---

[114] S. HOFFMAN AND A. PODGURSKI, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 *S. M. U. L. Rev.* 85, 104 (2012).
[115] *Id.* at 104-05.
[116] HHS Website, "The Common Rule," http://www.hhs.gov/ohrp/humansubjects/.
[117] HHS Website, "Federal Policy for the Protection of Human Subjects ('Common Rule')," http://www.hhs.gov/ohrp/humansubjects/commonrule/.
[118] 45 C.F.R. § 46.102(f) (2006).
[119] *Id.* § 46.102(f)(1)-(2).
[120] *Id.* § 46.102(f)(2).
[121] *Id.*
[122] 45 C.F.R. § 46.101(b)(4) (2006).
[123] *See* Institute of Medicine (US), Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule (S.J. NASS ET AL., eds., National Academies Press 2009), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, at 173.

2.2.4 NIST - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

The National Institute of Standards and Technology (NIST) developed a "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," [124] which provides a guideline to Federal agencies that can also be used by nongovernmental organizations on a voluntary basis.

According to the NIST Guide, PII is "any information about an individual maintained by an agency, including"[125]: (1) "any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records" [126]. This definition refers to the concepts of "distinguishing" and "tracing" and defines the first as "identify[ing] an individual"[127] and the latter as "process[ing] sufficient information to make a determination about a specific aspect of an individual's activities or status" [128]; (2) and "any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information"[129]. "Linked" information is "information about or related to an individual that is logically associated with other information about the individual" [130], whereas "linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual"[131].

The NIST Guide recommends that organizations "evaluate how easily PII can be used to identify specific individuals," i.e, the issue of identifiability, and maintains that "PII that is uniquely and directly identifiable [such as names, fingerprints, or SSNs] may warrant a higher impact level than PII that is not directly identifiable by itself"[132].

Interestingly, the NIST Guide provides two different definitions for "de-identification" and "anonymization."

The Guide defines "de-identified information" as "records that have had enough PII removed or *obscured*, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual"[133]. This definition is "loosely based on" the HIPAA Privacy Rule and is "generalized to apply to all PII," but does not require the removal of the 18 identifiers listed in HIPAA[134]. De-identified information can be re-identified/rendered distinguishable "by using a code, algorithm, or pseudonym that is assigned to individual records."[135] Such code "should not be derived from other related

---

[124] National Institute of Standards and Technology, E. MCCALLISTER, T. GRANCE AND K. SCARFONE, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-122 (2010) [hereinafter NIST Guide].

[125] See *id.* at 2-2 for a list of examples of information that may be considered PII.

[126] *Id.* at 2-1 (citing GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, available at: http://www.gao.gov/new.items/d08536.pdf).

[127] *Id.* For example, some information that could distinguish an individual are name, passport number, SSN or biometric data. *Id.* Credit scores would not per se be able to distinguish an individual. *Id.*

[128] *Id.* For instance, an audit log containing records of user actions would trace an individual's activities. *Id.*

[129] *Id.* (citing GAO Report 08-536, *supra* note 126).

[130] *Id.*

[131] *Id.* If different PII elements are contained in two databases, the data is linked if the second database is present on the same system or a closely-related system and there are no security controls that segregate the two sources. Otherwise, if the second database is maintained in an unrelated system within the organization, available in public records or otherwise readily obtainable, the data is linkable. *Id.*

[132] *Id.* at 3-3.

[133] *Id.* at 4-4.

[134] *Id.* at 4-4, fn. 54.

[135] *Id.* at 4-5.

information about the individual" and it should only be known to the one who has the authority to re-identify records[136]. Using a hash function (a one-way cryptographic function) on the PII is mentioned as a common de-identification technique[137]. If (a) the re-identification code/algorithm/pseudonym is maintained in a separate system, (b) there are appropriate measures in place to prevent unauthorized access, and (c) the data elements are not linkable via reasonably available external records (such as public records) to re-identify the data, de-identified information has a low PII confidentiality impact level[138]. De-identified information therefore is suitable for being used in research and analyses, such as trend analyses or research using health care test results, and for being aggregated for the purposes of statistical analysis[139].

"Anonymization" is different insofar as it consists in de-identifying information and making sure it will never be re-identified[140]. Therefore, anonymized information is "previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists"[141]. Of course, due to the growing amount of data available, full anonymity is hard to achieve[142]. Some anonymization techniques that allow the information to "retain its useful and realistic properties"[143] are listed, such as: generalizing the data, suppressing the data, introducing noise into the data, swapping the data, replacing data with the average value[144].

Anonymized data is particularly useful for system testing: because testing should simulate reality as closely as possible to ensure the new system runs correctly, randomly generated fake data is often ineffective[145].

2.3 Some Remarks on Pseudonymization

Pseudonymization consists of "replacing one attribute (typically a unique attribute) in a record by another"[146], or, in other words, of replacing the identifiers (e.g, name, date of birth, sex, address) by a pseudonym, such as encrypting the identifiers in personal data[147]. This technique "allows linking information belonging to an individual across multiple data records or information systems, provided that all direct identifiers are systematically pseudonymized"[148].

Pseudonymization differs from de-identification because it explicitly "allows for the pseudonyms to be reversed at some time in the future, re-identifying the data subjects"[149]. Many factors affect the ability to reverse pseudonyms, "including whether [they] are

---

136 *Id.*
137 *Id.* However, the guide further specifies that hashing does not meet the HIPAA standard. *See id.* at 4-5, fn. 56.
138 *Id.* The PII confidentiality impact level can be low, moderate, or high, and it "indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed." *Id.* at 3-1.
139 *See id.* at 4-5.
140 *See id.*
141 *Id.*
142 *See id.* at 4-5 n.58.
143 *Id.* at 4-6.
144 *Id.*
145 *Id.*
146 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 20.
147 Handbook on European data protection law, at 45.
148 NIST Internal Report 8053, at 16.
149 *Id.* We say "explicitly" because de-identification techniques sometimes allow for such reversal, too.

generated randomly or by an algorithm […], the availability of the key, and whether [they] are unique or reused"[150].

The Data Protection Directive and Convention 108 do not explicitly mention pseudonymization, but Article 5, Paragraph 42 of the Explanatory Report to Convention 108 points out how the requirements on the time-limits for the storage of data in their identifiable form are met if it is not "possible to link readily the data and the identifiers"[151]. This outcome can be attained through pseudonymization, because identification is not readily possible for anyone who does not have the encryption key available[152]. This is particularly useful when data controllers need to deal with the same data subject in a consistent manner but do not need his or her precise identity[153]. The ICO Code of Practice, while calling pseudonymization a "relatively high risk technique"[154], acknowledges this circumstance and clarifies that the UK Data Protection Act does not ban the types of research that are only possible if different data can be linked reliably to the same individual, as long as identification does not occur or, if it does, there is no violation of the data protection principles (which would occur, e.g., if individuals were told that only anonymized data would be disclosed but in fact personal data were also disclosed)[155].

However, the Opinion chooses a stricter approach to the issue of pseudonymization and highlights that, because identification is still possible to whoever has the encryption key, pseudonymized data are not equivalent to anonymized data, because they allow the singling out of a data subject and his linkability across different datasets and remain therefore within the scope of data protection laws[156]. Thus, pseudonymization is not considered a method of anonymization, but is nevertheless recognized as a "useful security measure" [157]. Data controllers should take extra steps in order to anonymize a pseudonymized dataset, such as removing and generalizing attributes or deleting or bringing to a highly aggregated level the original data[158].

Some of the proposed changes in the GDPR regard pseudonymized data. First of all, the proposed Article 4 includes a definition of pseudonymisation, i.e., "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person"[159]. The proposed Recital 23 specifies that "[d]ata which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person"[160], which is consistent with the previous application of the Directive. Recital 23a highlights that pseudonymisation "can reduce the risks for the data

---

150 *Id.* at 17.
151 Council of Europe Convention 108, Explanatory Report.
152 *See* Handbook on European data protection law, at 45.
153 *Id.* at 46.
154 UK ICO Code, at 51. The ICO Code of Practice equates pseudonymization with "deterministic modification," another technique where "the same original value is always replaced by the same modified value." *Id.*
155 *Id.* at 21.
156 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 10. The Opinion also refers to the 2006 AOL incident, where a database containing twenty million search keywords for over 650,000 users over a three-month period was released and the public identification of some of the users was possible, even if the user IDs had been replaced by a numerical attribute. *Id.* at 11.
157 *Id.* at 3, 20.
158 *Id.* at 21.
159 GDPR – Consolidated text, Article 4 (3b).
160 Id., Recital 23.

subjects concerned and help controllers and processors meet their data protection obligations", thus "[t]he explicit introduction of 'pseudonymisation' […] is […] not intended to preclude any other measures of data protection"[161]. Furthermore, the GDPR aims at "creat[ing] incentives for applying pseudonymisation" by underlining that "measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure, for the respective processing, that the provisions of [the] Regulation are implemented, and ensuring that additional information for attributing the personal data to a specific data subject is kept separately"[162]. Pseudonymization is mentioned among the "appropriate technical and organisational measures" which are designed to implement the fundamental principles of data protection within the new concept of "privacy by default"[163].

3. The Death of Anonymization?

3.1 Perfect Anonymization is Impossible

Many voices in the privacy law environment have been saying louder and louder that we should forget about perfect anonymization as it is impossible to achieve. Indeed, "[t]he re-identification of databases that were previously said to be 'anonymous' has happened many times"[164]. Therefore, as Woody Hartzog and Ira Rubinstein have recently written, "[t]he credibility of anonymization, which anchors much of privacy law, is now open to attack"[165]. We will now discuss some issues concerning the re-identification risk. Clearly, such risk exists and should not be overlooked by relying on superficial assumptions. On the other hand, this risk is not what we should focus on in order to create a meaningful framework for anonymization.

Generally speaking, "de-identification is based on assumptions that third parties do not have certain information about data subjects that may facilitate re-identification", but "adversaries may legally or illegally obtain such information from a variety of sources"[166]. Indeed, even the most precise de-identification standard is unable to provide perfect anonymity[167]. "To say something is anonymized is to imply a certain threshold of protection has been obtained", but this concept "inherently over-promises"[168]. According to a study performed in 2009[169], there is a risk of unique re-identification ranging from 0.01% to 0.25% of the state's population when de-identification is performed through the

---

[161] Id., Recital 23a.
[162] Id., Recital 23c.
[163] Id., Article 23.
[164] Z. ALEXIN, *Does fair anonymization exist?*, *International Review of Law, Computers & Technology*, Vol. 28, No.1, 21, 22 (2014).
[165] RUBINSTEIN & HARTZOG, *supra* note 7, at 2.
[166] HOFFMAN & PODGURSKI, *supra* note 114, at 105.
[167] GELLMAN, *supra* note 29, at 38 ("[N]otwithstanding HIPAA's determination that the resulting data is deidentified, Professor Sweeney testified that there is a 0.04% chance that data de-identified under the health Act's methodology could be re-identified when the de-identified data was compared to voter registration records for a confined population.") (citing Nat'l Comm. on Vital & Health Statistics, U.S. Dep't of Health and Human Servs., *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data* 36 n.16 (2007)).
[168] RUBINSTEIN & HARTZOG, *supra* note 7, at 28.
[169] K. BENITEZ & B. MALIN, *Evaluating re-identification risks with respect to the HIPAA privacy rule*, 17 *J. Am. Med. Inform. Assoc.* 169-177 (2010).

HIPAA safe harbor method[170]. A study carried out by Latanya Sweeney in 2007 shows a 0.04% chance[171]. Such risk becomes much higher (10% to 60%) for limited datasets[172]. Other studies have shown that "between 63% and 87% of the U.S. population could be accurately identified based on the three factors of gender, zip code, and date of birth, without any need for details such as name, social security number, or a precise address"[173]. Therefore, it has been concluded that this growing re-identification risk "demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data"[174]. This largely depends on the fact that any anonymous piece of information can potentially become personal data if combined with other (even anonymous) pieces of information[175].

The debate has become particularly lively due to several high profile cases. A very famous case of re-identification, performed by Latanya Sweeney, concerned the medical information of William Weld, then Governor of Massachusetts[176]. Similarly well-known are the 2006 case concerning the release by AOL of anonymized search queries, some of which then proved to be re-identifiable[177], and the re-identification of some Netflix users based on their movie ratings in a popular website[178]. These examples show how the re-identification risk also depends on the availability of other pieces of information that taken alone cannot lead to individual identification but can do so when aggregated[179]. Indeed, the question of whether data sets are truly anonymized (assuming this is possible) "cannot be answered in the abstract", but rather depends on the context and on the availability of other linkable pieces of information[180]. This is called the "auxiliary information problem", consisting in the risk that any piece of information can be identifying if combined with others[181]. With respect to this, some scholars have introduced the concept of "unicity" to assess how much outside information would be needed to re-identify a data subject from a deidentified data set[182]. Furthermore, the attempt to prohibit re-identification attacks through agreements (e.g. data use agreements) is not always successful as "these

---

170 *Id.* at 169.

171 Nat'l Comm. on Vital & Health Statistics, U.S. Dep't of Health and Human Servs., *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data* 36 n.16 (2007) (referring to Latanya Sweeney's testimony).

172 BENITEZ & MALIN, *supra* note 169, at 169.

173 HOFFMAN & PODGURSKI, *supra* note 114, at 105. *See* SWEENEY, *supra* note 98, at 2.

174 A. NARANYANAN & V. SHMATIKOV, *Myths and Fallacies of "Personally Identifiable Information"*, 53 Commc'n ACM 24, 26 (June 2010).

175 DE AZEVEDO CUNHA ET AL., *supra* note 42, at 644.

176 *See* OHM, *supra* note 5, at 1719-20; D.C. BARTH-JONES, *The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now* (2012).

177 *See* SCHWARTZ & SOLOVE, *supra* note 3, at 1841-42.

178 *See id.* at 1843; A. NARAYANAN & V. SHMATIKOV, *Robust De-Anonymization of Large Sparse Datasets*, 2008 *IEEE Symp. on Sec. and Privacy* 111, Feb. 5, 2008.

179 *See* SCHWARTZ & SOLOVE, *supra* note 3, at 1843 ("[…] a single piece of non-PII does not exist alone. Rather, such data form only part of a shifting landscape in which extensive information is available about almost every individual. This rich tableau of available information poses significant concerns for information privacy. The more information about a person that is known, the more likely it becomes that this information can be used to identify that person or to determine further data about her. When aggregated, information has a way of producing more information, such that de- identification of data becomes more difficult. Thus, it becomes possible to look for overlap in the data and then to link up different bodies of data.").

180 *Id.* at 1848.

181 RUBINSTEIN & HARTZOG, *supra* note 7, at 10.

182 Y. DE MONTJOYE ET AL., *Unique in the shopping mall: On the reidentifiability of credit card metadata*, 347 *Science* 536, 537 (2015) (cited by RUBINSTEIN & HARTZOG, *supra* note 7, at 11).

agreements may be difficult to enforce for de-identified data sets that are made freely available"[183].

The National Institute of Standards and Technology (NIST) explains in a recent report that there can be many reasons leading to a "re-identification attack"[184]. For example, an "intruder" might attempt a re-identification attack "[t]o test the quality of the de-identification", possibly "at the request of the data controller" who has an interest in ensuring that the de-identification has been successfully performed. Other goals might be related to reputation, such as "gain[ing] publicity or professional standing", or "embarrass[ing] or harm[ing] the organization that performed the de-identification". Furthermore, an intruder such as a marketing company may be able "[t]o gain direct benefit from the re-identified data". Last, the NIST highlights that a re-identification attack might also be performed in order "[t]o cause problems such as embarrassment or harm to an individual whose sensitive information can be learned by re-identification"[185].

On the other hand, other studies maintain that "there is no evidence that re-identification by a true adversary […] has actually happened", and that since re-identification is so hard to obtain, it can be possible "only for small populations under unusual conditions"[186]. Furthermore, it is important to bear in mind that the authors of the afore-mentioned re-identification studies "make particular assumptions about the re-identification scheme and the external data used to implement it" that "may not apply in actual attempts", thus, "the risk figures […] may be misleading"[187]. For instance, William Weld's re-identification has probably been made easier by the fact that "he was a public figure who experienced a highly publicized hospitalization" and was arguably flawed by the fact that the database used in the attack included roughly half of the population[188]. Scholars on this side of the debate ("pragmatists"[189]) go as far as maintaining that "[r]e-identification risks under the current HIPAA Privacy Rule have been reduced to the point that most people wouldn't (and shouldn't) lose any sleep over the issue"[190]. Also, Schwartz and Solove maintain that "computer science is developing metrics that are suitable" for the task of evaluating re-identification risk, and "a standard-based approach can be made operational and predictable"[191]. Therefore, many scholars have engaged in the attempt of precisely measuring the risk of re-identification[192].

---

183 NIST Internal Report 8053, at 19.

184 *Id.* at 9.

185 *Id.*

186 J. YAKOWITZ & D. BARTH-JONES, Tech. Policy Inst., The Illusory Privacy Problem in Sorrell v. IMS Health 7 (2011) (cited by HOFFMAN & PODGURSKI, *supra* note 114, at 106-07).

187 HOFFMAN & PODGURSKI, *supra* note 114, at 106. *See also* RUBINSTEIN & HARTZOG, *supra* note 7, at 8.

188 BARTH-JONES, *supra* note 176, at 3. Anyways, we have to bear in mind that Weld's re-identification was performed before the actual HIPAA Privacy Rule was passed, and that a similar attack could not be successful now.

189 RUBINSTEIN & HARTZOG, *supra* note 7, at 12. *See, e.g.*, BENITEZ & MALIN, *supra* note 169.

190 BARTH-JONES, *supra* note 176, at 12.

191 SCHWARTZ & SOLOVE, *supra* note 3, at 1884.

192 *See, e.g.* EL EMAM, *supra* note 50. This paper engages in the attempt of measuring health data's identifiability distinguishing "three kinds of re-identification risk that we can measure objectively with specific probabilistic metrics". *Id.* at 65. First, "prosecutor risk" refers to "when the adversary is attempting to re-identify a specific (target) individual […], has background knowledge on the individual, and knows that he or she is in the disclosed data". The second type of risk is the "journalist risk", which "is relevant when the adversary is attempting to re-identify an individual in the disclosed data set but doesn't know with certainty whether this individual is actually included". *Id.* For these two types of risk, "we can assign a probability of re-identification to each individual in the disclosed data". *Id.* at 66. Thirdly, "marketer risk" occurs "when the adversary is attempting to re- identify as many people as possible in the disclosed data". This risk "computes the expected number of individuals that would be re-identified". According to El Emam, "[d]ata custodians

Given this debate, it is worthwhile to look at whether sharing de-identified public health data has been held to be legal by court decisions. Few courts in the United States have had the chance to deal with this issue, but they "ultimately based their decision on a fact-based determination of whether the contested disclosure would place the confidentiality of personal health information at undue risk"[193]. Therefore, where the likelihood of re-identification only depended on an expert's education, training and experience but would have been very low if performed by a member of the general public, a court allowed the disclosure[194]. Conversely, the granularity of the data sought by the request combined with a "small population size, ultimately swayed [another] court to rule against disclosure"[195]. Therefore, it looks like courts "will not forbid disclosures absent real evidence that information can be readily used to re-identify information"[196]. This seems to support the argument that "de-identification science […] will remain an effective and legal means to maintain the confidentiality of personal health information" as long as it meets this threshold[197].

All in all, making general statements as to the actual likelihood of re-identification is probably not going to lead us anywhere. It is increasingly clear that "for most personal data, deidentification may be like absolute zero for temperature: a state that can be approached but never achieved"[198]. Yet, this does not mean that deidentification loses all of its potential usefulness: it is "far more productive to figure out where [the two sides of the debate] come together"[199]. Rubinstein and Hartzog maintain that this debate, while focusing on "opposing sides taking extreme positions and making overly general claims about data release policy across all disciplines", "has greatly overshadowed successful policy outcomes"[200], such as approaches where "deidentification, consent, and tiered access work together to provide multiple layers of protection"[201]. Because the two positions limited their analyses "almost exclusively to the release-and-forget model", they "largely neglect[ed] the full gamut of SDL techniques"[202]. Indeed, the famous high-profile re-identification episodes can be seen as not sounding the death knell for anonymization, but as teaching useful lessons in order not to make the same mistakes[203].

---

must decide which metric represents a plausible attack scenario for their data sets". *Id.*

193 V. RICHARDSON, S. MILAM, AND D. CHRYSLER, *Is Sharing De-identified Data Legal? The State of Public Health Confidentiality Laws and Their Interplay with Statistical Disclosure Limitation Techniques*, *Journal of Law, Medicine & Ethics*, Spring 2015, 43 Suppl 1:83-6, at 84.

194 *Id. See* Southern Illinoisan v. Illinois Department of Public Health, 844 N.E. 2d 1 (Ill. 2006).

195 RICHARDSON ET AL., *supra* note 193, at 85. *See* Marine Shale Processors, Inc. v. State of Louisiana Dep't of Health, 572 So. 2d 280 (La. App. 1 Cir. 1990). *See also* Williams Law Firm v. Board of Supervisors, 878 So. 2d 557 (La. App. 1 Cir. 2004).

196 RICHARDSON ET AL., *supra* note 193, at 85

197 *Id.*

198 GELLMAN, *supra* note 29, at 40.

199 RUBINSTEIN & HARTZOG, *supra* note 7, at 14.

200 *Id.* at 20. The "successful policy outcome" they refer to is the "new genomic data sharing policy" introduced by the National Institute of Health in 2014. This policy "promotes the use of consent for broad sharing" but "also requires researchers to explain to prospective participants the risks of reidentification and whether or not their deidentified data will be shared through unrestricted or controlled-access repositories". *Id.* at 19. This policy seems to allow the benefits of open access, because governments, businesses, and individuals can make "sound decisions […] based on the data", while balancing "participant privacy and broad accessibility of genomic data for research purposes by combining technical and policy safeguards". *Id.* at 19-20.

201 *Id.* at 19.

202 *Id.* at 22-23.

203 *See id.* at 24.

3.2 Secondary Uses of Health Data

Healthcare has been aptly defined as a "data intensive enterprise", as "[h]ospitals, pharmacies, laboratories and other healthcare organizations generate clinical data as a by-product of service"[204]. Several benefits are considered to arise from sharing patient data for research purposes, including: accountability in results, the ability of researchers to "build on the work of others more efficiently" and "perform individual patient data meta-analyses"[205].

In order to engage in secondary uses of health data, i.e., "'reuse' of data for purposes other than direct care of the patient"[206], two legal mechanisms can be used: either consent or anonymization[207]. This has been called the "consent or anonymize approach"[208]. Because consent is very impractical to obtain, anonymization is relied on as the primary mechanism for sharing data[209]. Lawyers and scientists need to engage in striking the right balance between providing individuals with an adequate level of protection for health data and building up anonymization standards which allow research[210].

There are two main issues presented by secondary uses of health data. The first issue deals with the risk of re-identification, which also causes the possibility for data to be used in ways that the individual could not anticipate and/or appreciate. The second problem regards the fact that fully de-identified data may have been deprived of pieces of information that are useful or necessary for research[211]. Moreover, there are other challenges linked to the de-identification of unstructured data, such as text narratives[212], or medical imagery[213].

---

[204] A. GEISSBUHLER, C. SAFRAN, I. BUCHAN, ET AL., *Trustworthy reuse of health data: a transnational perspective*, 82 *Int'l J. of Med. Inform.* 2 (2013).

[205] EL EMAM ET AL., *supra* note 6, at 1.

[206] GEISSBUHLER ET AL., *supra* note 204, at 2.

[207] EL EMAM ET AL., *supra* note 6, at 1.

[208] *See* M. MOSTERT, A.L. BREDENOORD, M. BIESAART AND J. VAN DELDEN, *Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach*, *European Journal of Human Genetics* (2015), doi:10.1038/ejhg.2015.239, at 1.

[209] EL EMAM ET AL., *supra* note 6, at 1.

[210] Anonymisation is particularly valuable "as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned. However, case studies and research publications have shown how difficult it is to create a truly anonymous dataset whilst retaining as much of the underlying information as required for the task". Article 29 WP Opinion 05/2014 on anonymisation techniques, at 3.

[211] *See* S.A. TOVINO, *The Use and Disclosure of Protected Health Information For Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 *South Dakota Law Review* 447, 457 (2004) ("[…] following the publication of the de-identification safe harbor in the 2000 Final Rule, several articles appeared in medical journals arguing that the safe harbor, as written, is useless for many types of epidemiologic, health services, and other population-based research that require identification of each subject's geographical information, as well as certain dates and ages"). Some scholars disagree and maintain that research can be conducted using de-identified data. *See, e.g.,* M. HATCH, *HIPAA: Commercial Interests Win Round Two*, 86 *Minn. L. Rev.* 1481, 1492 (2002) ("Researchers I have interviewed indicate that the primary research purpose of attaching the patient identifiers is to follow a patient if he transfers from one provider to the next. Yet researchers have failed to provide examples of situations where such patient identifier information was found to meaningfully expedite conclusions concerning the efficacy of a particular treatment. There are simply too many other personal variables missing on general medical charts that impede the value of such close tracking of a patient. In other words, while a macro analysis of the efficacy of treatments of the United States population might reveal certain trends, it cannot answer with certainty whether other factors not recorded on a medical chart affect the treatment outcome. Accordingly, the use of a patient identifier to track a patient from one physician to the next is hardly necessary if only a general trend can be ascertained").

[212] NIST Internal Report 8053, at 30 ("Medical records contain significant amounts of unstructured text. In recent years, there has been an effort to develop and evaluate tools designed to remove the 18 HIPAA data

As to the first problem, the risk of re-identification is particularly a problem in the field of secondary uses of data made by business associates. "Re-identification of information that was previously believed to be de-identified constitutes a use of protected health information not described in, and violation of, a business associate contract"[214] and it is very hard for a covered entity to find out about such violations, especially because "business associate contracts do not require periodic review or renewal"[215] and "the description of permitted uses and disclosures is broad"[216]. This "open[s] up an individual's data to uses that the individual does not anticipate and for which the individual may not be in agreement"[217]. Therefore, the National Commission on Vital and Health Statistics recommended in 2007 that "covered entities specify the limits of health data use in their business associate contracts"[218]. In particular, covered entities should include terms that describe what HIPAA-de-identified data may be used for and to whom they are supplied. They should also ensure that an equivalent contract exists between the business associate and all of its agents to create a chain of trust through all organizations that may have access to such data[219]. Furthermore, it reminded that the HIPAA definition of de-identification is the "only permitted means to de-identify protected health information"[220].

The second and very tricky issue deals with the statement that – as a scholar wrote in an influential paper – "[d]ata can be either useful or perfectly anonymous but never both"[221]. Indeed, some criticisms have been raised from the side of the researchers about the new GDPR, where "the combination of strict consent requirements and limited research exemptions will severely restrict medical research"[222]. Similarly, others maintain that whenever a dataset is de-identified according to the HIPAA framework it becomes unusable for research[223], both because it is hard to get access to such data and because of its poor quality[224]. More specifically, some have suggested reducing the number of identifiers to be removed from a dataset that is meant to be used in research, because, for example, "general areas of origin, residence, and work may be essential to epidemiological

---

elements from free-format text (e.g., narrative intake reports) using natural language processing techniques. The two primary techniques explored have been rule-based systems and statistical systems. Rule-based systems tend to work well for specific kinds of text but may not work well when applied to new domains. Statistical tools generally perform less accurately than rule-based systems and require labeled training data, but are easier to repurpose to new domains"). *See id.* at 30-32.

213 *Id.* at 35. Medical imagery must "be de-identified prior to being shared", but "[i]nformation that may identify an individual can be present in either the header or in the pixels". *Id.* There are provisions related to the DICOM (Digital Imaging and Communications in Medicine) format in order to "designat[e] whether or not identifying information is present in either the header or pixel area of an image and [to] indicat[e] whether a file has been deidentified". *Id.* at 35-36. However, the DICOM standard "does not specify the actual algorithms or techniques for de-identification", which "would be specific to each imaging modality and are active research areas". *Id.* at 36.

214 Nat'l Comm. on Vital & Health Statistics, *supra* note 171, at 28.

215 *Id.*

216 *Id.*

217 *Id.*

218 *Id.* at 30.

219 *Id.*

220 *Id.* at 37 (stating that the removal of 17 identifiers omitting the eighteenth catch-all is not enough under the safe harbor definition of re-identification).

221 OHM, *supra* note 5, at 1704. *See also* J. BRICKELL & V. SHMATIKOV, *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, The 14th ACM SIGKDD Int'l Conference on Knowledge Discovery & Data Mining 70 (August 2008).

222 MOSTERT ET AL., *supra* note 208, at 1.

223 Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, *supra* note 123, at 40, 175.

224 *Id.* at 231-33.

and other studies of topics such as disease incidence"[225]. Clearly, "de-identification comes at a cost to the scientific accuracy and quality of the healthcare decisions that will be made based on research using de-identified data"[226]. It looks like "[n]o legislation can establish meaningful standards for the creation of deidentified data that has full value for legitimate secondary users"[227].

Since "the search for ways forward within the consent or anonymise paradigm becomes increasingly difficult in a data-intensive medical research context"[228], we might need to look for more creative solutions. As we will discuss in the next paragraph, mere reliance on anonymization is misplaced: we need to couple this technique with other kinds of guarantees. For example, if a lower number of identifiers needed to be removed under the HIPAA Privacy Rule, this could be coupled with assurances from the research entity that it "will not use or disclose the information for purposes other than research and will not identify or contact the individuals who are subjects of the information" [229]. Furthermore, many scholars have noticed that "obtaining meaningful consent or irreversibly anonymising data is impracticable or impossible for a great deal of data-intensive medical research"[230]. Thus, a possible solution can be represented by research exemptions, which create "another legal basis than consent for the processing of sensitive personal data for medical research purposes"[231].

As we have seen in Chapter I, there are already some exceptions with respect to projects that would be impossible to carry out with anonymized data. In these instances, the Council of Europe Recommendation R(97)5 allows projects "carried out for legitimate purposes" to use personal data in three different scenarios[232]. We have also seen how the Italian DPA establishes similar rules for when research must be carried out that requires some degree of re-identifiability[233]. Also, according to the new GDPR, "Union or Member State law may provide for derogations [from some rights] in so far as […] such derogations are necessary for the fulfilment of [the] purposes"[234].

According to Article 9, an exception to the general ban on the processing of health data is established when "processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) based on Union or Member State law which shall be proportionate to

---

[225] *Id.* at 175.

[226] BARTH-JONES, *supra* note 176, at 12. Barth-Jones highlights that "some popular de-identification methods, such as "k-anonymity methods," can unnecessarily, and often undetectably, degrade the accuracy of de-identified data for multivariate statistical analyses". *Id.*

[227] GELLMAN, *supra* note 29, at 47 ("That objective cannot be reached now and may be impossible to achieve generally. There will always be a tradeoff of some sort, involving the degree of identifiability of the data, the usability of the data, the privacy of the data subjects, and the cost of the deidentification process. Technology can sometimes lessen these tradeoffs, but it cannot eliminate them all the time.").

[228] MOSTERT ET AL., *supra* note 208, at 3.

[229] Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, *supra* note 123, at 175-76. *See* 67 Fed. Reg. 53181, 53234 (2002).

[230] MOSTERT ET AL., *supra* note 208, at 3.

[231] *Id.*

[232] Council of Europe, Committee of Ministers (1997), *Recommendation R(97)5 to member states on the protection of medical data*, 13 February 1997, Art. 12. Such three scenarios are: (1) the data subject has provided his or her consent; (2) disclosure of data for a scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, as long as the data subject has not expressly opposed disclosure, and it would be impracticable to contact the data subject, and the interests of the research project justify the authorization; (3) the scientific research is provided for by law and constitutes a necessary measure for public health reasons. *See* Chapter I, Paragraph 2.1.

[233] *See* Paragraph 2.1.3.

[234] GDPR – Consolidated text, Art. 83.2 and 83.3.

the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"[235]. The Parliament during the negotiations had adopted a stricter approach whereby national law could provide a research exemption from consent for research serving a high public interest[236], but the broader position of the Council prevailed[237]. Pursuant to Recital 40, consent to further processing of the data is not necessary if "the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest"[238].

Whenever a research exemption from consent is provided, a very important issue is that of "which appropriate safeguards should be put in place"[239]. The new GDPR requires that "[p]rocessing of personal data for […] research purposes […] be subject to […] appropriate safeguards", which should "ensure the respect of the principle of data minimisation", and "[w]henever these purposes can be fulfilled by further processing of data which does not permit or not any longer permit the identification of data subjects these purposes shall be fulfilled in this manner"[240]. It also specifies that the safeguards may include pseudonymization as long as it allows for the achievement of the purposes[241]. However, this leaves room for an exemption whenever the safeguards do not allow the fulfillment of the purposes. The approach adopted by the Parliament – now abandoned -- had required pseudonymisation under the highest technical standards[242], but it has been "argued though that a strict interpretation of this requirement [would have] possibly render[ed] most data useless for epidemiological research"[243].

---

[235] *Id.* Art. 9(2)(i).
[236] GDPR – EP Resolution, Art. 81(2)(a).
[237] GDPR – Council General Approach, Art. 9(2)(i).
[238] GDPR – Consolidated text, Recital 40. Similarly, according to Recital 42b, "[t]he processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject".
[239] MOSTERT ET AL., *supra* note 208, at 3.
[240] GDPR – Consolidated text, Art. 83.1 and Recital 125 ("The processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. These safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfill those purposes by processing data which does not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards to the processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with respect to other relevant legislation such as on clinical trials").
[241] GDPR – Consolidated text, Art. 83.1.
[242] GDPR – EP Resolution, Art. 81.
[243] MOSTERT ET AL., *supra* note 208, at 3.

It looks like the new GDPR "leave[s] considerable room for a more detailed regulation on a national level", which means that "it will be largely up to the EU member states to determine the appropriate conditions of research exemptions"[244]. This diverse implementation "may impede the exchange of sensitive personal data for research across national borders"[245].

Other alternative legal bases to consent dealing with technological or organizational or governance measures have been proposed[246], as we have also seen in Chapter II. For example, we could think of authorization by an ethics committee or specific limitations to access and use[247]. Even one scholar who proposes research exemptions as the way forward suggests that there should be "an independent necessity and proportionality test, for instance by an […] ethics committee"[248]. Indeed, since we cannot rely on anonymization *per se*, "proportionate technical and governance measures should be incorporated in the design of data-intensive medical research projects and infrastructures"[249]. This is also meant to "allow individuals and the public to access clear information about the use of their data and their rights concerning this usage", especially "where technological complexity makes it difficult for individuals to find out which personal data are used, for what purpose and by whom" [250]. For instance, "these measures could include the use of IT and participant interfaces to provide individuals with sufficient information and control over their data, and to stimulate participation by relevant stakeholders"[251].

Also, we can now think again of the proposal we analyzed in Paragraph 4.3 of Chapter II dealing with the use of EHR data for research. Hoffman and Podgurski proposed drawing a distinction between interventional and record-based studies and subjecting the data in record-based studies to safeguards other than informed consent[252]. Such safeguards include the adoption of identity concealment techniques, additional oversight performed by an ethics board, and enhanced notification and education[253]. This kind of approach is very interesting inasmuch as it can be adapted to the different circumstances and focuses on risk assessment, thereby enhancing the importance of human judgment.

The issues relating to secondary uses of health data show some of the shortcomings of the current view on anonymization, which overlooks both the need to keep data useful enough for research through a case-by-case evaluation and the need to be aware of the risk of re-identification, which asks for further safeguards around anonymized data used for research.

4. Adhering to Reality

The "first law of privacy policy" is that "there is no silver bullet"[254]. The field of anonymization, as we have seen, suffers from a lack of awareness of this basic principle. The attempt to build up nearly automatic standards and bright-line rules needs to surrender

---

244 *Id.*
245 *Id.* at 4.
246 MOSTERT ET AL., *supra* note 208, at 3.
247 *Id.*
248 *Id.* at 4.
249 *Id.*
250 *Id.*
251 *Id.*
252 HOFFMAN & PODGURSKI, *supra* note 114, at 90, 124.
253 *See id.* at 128-41.
254 RUBINSTEIN & HARTZOG, *supra* note 7, at 53.

to the complexity of reality. For instance, the Center for Democracy & Technology (CDT) underlines that the Privacy Rule only devised one anonymization option, whereas a "broader spectrum of . . . options would meet the needs of different contexts and assure the data is accessed or disclosed in the least identifiable form possible for any given purpose"[255]. This is just an example of how the attempt to create precise, unbending rules should leave room for nuanced, complex standards. Furthermore, anonymity should no longer be thought of as something absolute, but rather as one of the available tools that can be used to protect privacy[256]. Policymakers and scholars need to engage in the endeavor of creating legal frameworks that are as adherent to the complexity of things as possible. It is likely that "anonymization" as we have been referring to it has died, as the "expectations of near-perfection"[257] that this term creates cannot be met. What, then, is the way forward for anonymization policy?

4.1 On a Spectrum

Data are usually regarded as either "personal" or "anonymous". Personal, i.e., identifiable data, fall within the scope of data protection laws, whereas successfully anonymized data are unprotected. This approach is clearly "outmoded"[258]. First of all, it is said to have a "view of personal data as a static concept, referring to "an individual," [while it] fails to account for the fact that data that are ostensibly not about "an individual," such as metadata, social grid analysis, or stylometry (analysis of writing style), may have unambiguous privacy impact"[259]. Furthermore, and more importantly, more and more voices of the privacy policy community are criticizing this "binary scale" and propose assessing the identifiability of data "on a spectrum", i.e., considering not only technical de-identification, but also legal and administrative safeguards that may decrease the risk of re-identification[260]. This mindset "adjusts practically to the reality that while contemporary mathematical capabilities may theoretically enable re-identification to occur, their impact can functionally and effectively be constrained by legal and organizational measures"[261]. The relationship between personal data and anonymous data is now dynamic and reversible: the concept of personal data is more and more like an "ever-lasting category"[262].

---

[255] Center for Democracy & Technology, *Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data* 2 (2009).

[256] *See* MASCETTI ET AL., *supra* note 2, at 106 (The "legal notion of anonymity, as defined in the legislation on data protection, cannot be seen as a right in itself. Instead, anonymity should be considered as a "tool" that can be used to safeguard the protection of personal data. […] Indeed, although most of the scientific contribution tackle the problem of guaranteeing privacy through anonymity, it has also been recognized that privacy protection can also be achieved without anonymity").

[257] RUBINSTEIN & HARTZOG, *supra* note 7, at 48 ("…rhetoric is a key aspect of this debate and the terms "anonymous" and "anonymization" should be used very sparingly and with due attention to precision").

[258] TENE, *supra* note 47, at 1242.

[259] *Id.* at 1242-43 (citing A. NARAYANAN ET AL., *On the Feasibility of Internet-Scale Author Identification*, in *Proceedings of the 2012 IEEE Symposium on Security and Privacy* 300 (May 22, 2012), available at: http://www.cs.berkeley.edu/~dawnsong/papers/2012%20On%20the%20Feasibility%20of%20Internet-Scale%20Author%20Identification.pdf; Letter from Salil Vadhan et al., Professor, Harvard Univ., to The Dep't of Health & Human Servs., Office of the Sec'y, & Food & Drug Admin. (Oct. 26, 2011), available at http://dataprivacylab.org/projects/irb/Vadhan.pdf).

[260] TENE & WOLF, *supra* note 50, at 5 (citing SCHWARTZ & SOLOVE, *supra* note 3). See also, for more insights on alternative proposals, TENE, *supra* note 47, at 1243-45.

[261] TENE & WOLF, *supra* note 50, at 3.

[262] DE AZEVEDO CUNHA ET AL., *supra* note 42, at 655 ("…il rapporto tra dato personale e dato anonimo è ormai dinamico e reversibile, dal momento che esistono modi per prolungare l'esistenza del dato personale (tramite l'uso secondario di questi dati, compatibile con il principio della finalità) e modi per far ritornare il

There are several different approaches within this position. Some scholars propose viewing identifiability of personal information "as a continuum"[263], without thinking of categories. Another study identified "five discrete levels" within the "continuum of identifiability": (1) "clearly identifiable" data, (2) "masked data", (3) masked data where both the quasi-identifiers and the identifying variables are obfuscated, (4) microdata or data appearing in tabular form (also called "managed" since "the data custodian can manage the risk of re-identification"), and (5) clearly non-identifiable data[264]. Schwartz and Solove proposed separating data in three categories: identified, identifiable and non-identifiable, as "[r]ather than a hard "on-off" switch, this approach allows for legal safeguards for both identified and identifiable information"[265]. According to these two scholars, "information refers to an identified person when it singles out a specific individual from others"[266]. The second category ("identifiable" data) refers to "when specific identification, while possible, is not a significantly probable event", i.e "there is some non-remote possibility of future identification"[267]. In Schwartz and Solove's model, "identifiable data should be shifted to the *identified* category when there is a significant probability that a party will make the linkage or linkages necessary to identify a person": this probability needs to be assessed using a "contextual" test, which "should consider factors such as the lifetime for which information is to be stored, the likelihood of future development of relevant technology, and parties' incentives to link identifiable data to a specific person"[268]. Third, "non-identifiable information carries only a remote risk of identification", looking at "the means reasonably likely to be used for identification"[269]. Nevertheless, these three categories form a spectrum and "do not have hard boundaries"[270].

Rubinstein and Hartzog propose a modified version of Schwartz and Solove's framework, where "public release of data sets" is treated "as an overriding factor in assigning data sets to categories 1, 2 or 3"[271]. Thus, within this proposal, "regulators should create a default presumption that publicly released data sets are identifiable", even if common identifiers have been removed, and such presumption can be overcome if the data controller "meets process-based data release requirements"[272] as discussed in paragraph 4.3.

There are varying opinions but clearly, although re-identification is often mistakenly thought of as a "binary construct", i.e., we think of information as being either identifiable or not, it is more accurate to say that "a continuum of identifiability exists, with some datasets being quite easy to re-identify with minimal resources and skill, and others requiring considerable time, effort, cost, and skill to re-identify"[273]. Therefore, "[d]ata custodians should view de-identification as a risk-management exercise", since the goal "[is not] minimizing re-identification risk to its lowest possible level, but choosing a risk that the custodian is willing to take for a particular disclosure […] and managing it", by "making

---

dato anonimo nel campo dei dati per- sonali (tramite i nuovi e sofisticati processi di re-identificazione). In questo modo, più che una "ever-expanding category," il concetto di dato personale può anche diventare una "ever-lasting category," fatto che sicuramente lancerà in futuro delle importanti sfide alla privacy").

263 GELLMAN, *supra* note 29, at 40.

264 EL EMAM, *supra* note 50, at 64-65.

265 SCHWARTZ & SOLOVE, *supra* note 3, at 1877.

266 *Id.*

267 *Id.* at 1878.

268 *Id.*

269 *Id.*

270 *Id.* at 1877.

271 RUBINSTEIN & HARTZOG, *supra* note 7, at 53.

272 *Id.*

273 EL EMAM, *supra* note 50, at 64.

trade-offs among de-identification, procedural constraints and contractual obligations"[274]. In order to meaningfully manage such risk, data custodians need to, among other things, "establish concrete guidelines for setting thresholds" depending on the specific circumstances, and employ optimization techniques "that will balance information loss with re-identification risk"[275].

4.2 Anonymized Data Need Further Safeguards

Anonymized data falls outside the scope of legal protection, yet "there is an expectation that the anonymised data will be used only for purposes that are legitimate, in a manner that would not surprise the patients, and not in a discriminatory or stigmatising manner"[276]. Indeed, this expectation relies on something other than the complete absence of a re-identification risk, because many studies have shown how it is rather naïve to believe that de-identification performed so as not to deprive data of its value is also able to exclude that, via the interaction with other databases, re-identification will ever be feasible. Some degree of risk needs to be accepted or at least acknowledged. At the same time, this means that even anonymized data needs to be surrounded by further protections in order to fulfill such expectations that the data will not be employed to commit abuses. Approaches such as the one adopted by the FTC are arguably promising, as we have said, but "sound data release policy requires more nuance as well as attention to techniques other than deidentification"[277]. Indeed, deidentification techniques should be seen as "only part of a larger approach to protecting the privacy and confidentiality of data subjects known as *statistical disclosure limitation* (SDL)"[278]. SDL refers to the techniques that have been developed "for disseminating official statistics and other data for research purposes while protecting […] privacy"[279].

Looking at research studies, "it would be irresponsible to allow any member of the public to access de-identified EHRs without any oversight", because "data miners would gain many targets for re-identification, and they could expend as much time and computational power as they have available"[280]. Therefore, even when research projects use de-identified data, they should be subject to "continuing reviews" in order "to ensure that investigators are safeguarding privacy with appropriate security measures and are engaging in valid research activities rather than misusing data"[281].

In addition, the awareness of the re-identification risk led to the development of other layers of protection based on "privacy ethics", e.g., the implementation of "governance mechanisms that oversee the development and use of the models"[282]. In practice, a privacy ethics council "within a data controller or data processor would advise the business about whether the model and its uses are discriminatory, stigmatizing, creepy,

---

274 K. EL EMAM, *Heuristics for De-identifying Health Data*, *IEEE Security & Privacy* 6(4):58-61 (2008), p. 60.
275 *Id.*
276 EL EMAM ET AL., *supra* note 6, at 1.
277 RUBINSTEIN & HARTZOG, *supra* note 7, at 4.
278 *Id.* at 14.
279 *Id.* at 15.
280 HOFFMAN & PODGURSKI, *supra* note 114, at 136 ("Even with a low success rate, they may be able to re-identify a large number of EHRs. For example, if data miners had access to a database of de-identified EHRs for every person in the United States (over 311 million people) and they de-identified records with a 0.10% success rate, they would be able to de-identify EHRs of over 311,000 people.").
281 *Id.*
282 K. EL EMAM, C. ALVAREZ, *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, 5 *Int'l Data Privacy Law* 73-87 (2015), at 6.

or surprising"[283]. The evaluation could be based on some criteria including: the "relationship between the purposes for which the data have been collected and the purposes for model-based decision-making", the "context in which the data have been collected and the reasonable expectations of the data subjects as to their further use", the "nature of the data and the impact of the model-based decisions on the data subjects", and the "safeguards applied by the controller to ensure fairness in decision-making and to present any undue impact on the data subjects"[284]. In some instances, conditions of use accompanying the anonymized data may be another useful tool, since the application of these criteria is subjective and predicting all the possible decisions that can be made with an anonymized dataset is impossible[285].

Another attempt to deal with the re-identification risk has been represented by advocating for the implementation of a trustworthy process for handling health data, as discussed within the 2012 European Summit on Trustworthy Reuse of Health Data. Together with employing the best available techniques, there is another element which unavoidably plays a role: trust, which has been defined as "the cornerstone of data sharing and reuse"[286] and which is largely based on transparency and the ability of data subjects to know how their data is being processed. In order to implement a trustworthy process, according to the findings of the 2012 European Summit, three components are needed: a technological component, a research component, and an exploitation component[287]. The first deals with "the design and implementation of IT tools and services able to guarantee data quality and data security, as well as to provide interoperability, adaptability and scalability"; the second one concerns "the evidence that can be derived from a reuse of data"; the last regards "goals of the data reuse, which may include a variety of purposes, from clinical research, epidemiology and surveillance to post-marketing analysis"[288].

The solution presented by a 2010 paper by Robert Gellman consists in a "legislative-based contractual solution for the sharing of deidentified personal information while providing protections for privacy"[289]. This proposal does not aim at being "a universal guarantee of privacy", but just at "provid[ing] another tool to support the sharing of personal data while addressing the privacy interests of the data subjects"[290]. According to this approach, "a data discloser and a data recipient […] enter into a voluntary contract that defines responsibilities and offer remedies to aggrieved individuals"[291]. Gellman proposes the implementation of a statute that "defines the terms of data disclosure and rights for the data subjects", in order "to strike a balance between the interests of all parties: the data disclosers, the data users, and the data subjects"[292]. The suggested legislation would "only apply to those who choose to accept its terms and penalties through a data agreement"[293]. The obligations imposed on the data recipients would be: a prohibition "from reidentifying or attempting to reidentify [the data] under the threat of civil and criminal penalties", as well as a requirement "to maintain technical, administrative, and other safeguards against

---

283 *Id.*
284 *Id.*
285 *Id.*
286 GEISSBUHLER ET AL., *supra* note 204, at 5.
287 *Id.* at 6.
288 *Id.*
289 GELLMAN, *supra* note 29, at 35.
290 *Id.*
291 *Id.*
292 *Id.* at 47.
293 *Id.* at 48.

reidentification"[294]. This would allow data recipients to "offer potential disclosers more assurance that a data transfer will not create liabilities", and would create "uniform rules, new protections, and enforcement methods"[295]. Within this "voluntary approach", "those who want the benefits [can choose to] accept the obligations"[296]. Arguably, this would tackle "[t]oday's lack of clear definitions, deidentification procedures, and legal certainty", by "provid[ing] greater certainty about the potential liabilities, and allow[ing] individual data subjects to enforce their privacy interests when data has been reidentified"[297].

Indeed, the deidentification debate should move to building up a policy based on the full range of data controls and safeguards. A sound data release policy should not "commit to one particular data control, such as contracts", but "the full range of control options should be utilized in conjunction with data treatment techniques, organizational support, and mindful framing"[298]. Arguably, "the more rigorous and robust the data treatment, the less potent the data controls need to be" and *vice versa*, in "a sort of inverse-ratio rule"[299].

4.3 "From Output To Process"[300]

The recent paper written by Rubinstein and Hartzog "propose a policy-driven and comprehensive process-based framework for minimizing the risk of reidentification and sensitive attribute disclosure"[301]. They choose to focus "on process rather than output" because they recognize "that there is no perfect anonymity"[302]. This seems extremely reasonable inasmuch as we already adopt this approach when we try to protect human rights in other fields: for instance, the focus on "due process of law" shows how we try to build up a fair process, acknowledging that this is as close as we can get to achieving justice. The protection of privacy as a human right can thus adopt the same approach as we discover that the attempts to achieve perfect anonymity are farfetched. It looks like "a careful reading of the privacy scholarship […] reveals a rough consensus that can be used to develop data release policy around the concept of minimizing risk"[303]. The paper shows how it would be unwise to rely solely on harm, on transparency, or on permission[304]. First of all, "harm is a contentious concept in privacy law" as it is very hard to assess and detect[305]. Secondly, it is also unwise to focus only on transparency and disclosures because "[c]onsumers only have a limited ability to make meaningful decisions regarding their own privacy due to the incredible volume, impenetrability and interconnectedness of data collection and transfers"[306]. Thirdly, as we have seen, informed consent in the field of medical research also creates several problems, as it is "regularly meaningless", therefore "it

---

294 *Id.* at 48-49.
295 *Id.* at 49.
296 *Id.*
297 *Id.* at 54.
298 RUBINSTEIN & HARTZOG, *supra* note 7, at 36.
299 *Id.* at 37-38.
300 *Id.* at 44.
301 *Id.* at 4.
302 *Id.* at 5.
303 *Id.* at 21.
304 *Id.* at 26-27.
305 *Id.* at 26 ("Many privacy harms are incremental or difficult to quantify or articulate", thus "they fall through the cracks of harm-based privacy regimes with high injury thresholds." Furthermore, "harms related to insufficient anonymization can also be very difficult to detect, because reidentification usually remains hidden unless a researcher or adversary claims credit for a successful attack").
306 *Id.* at 27.

should not be over-leveraged"[307]. As a consequence, the paper proposes that "[i]nstead of focusing on the ultimate goal of anonymization, the law could be designed around the processes necessary to lower the risk of reidentification and sensitive attribute disclosure"[308]. This would mean shifting the focus from output to process, due to the awareness that "perfect anonymization is a myth"[309]. Thus, the two scholars propose that a "more sustainable approach" would try "to ensure that data custodians follow appropriate processes for minimizing risk"[310]. This change would make data release policy look more like data security policy, as it would share with it some interesting advantages[311]. Data security is, first of all, "conceived of as a process of continually identifying risk, minimizing data collection and retention, [and] implementing administrative, technical, and physical safeguards"[312]. This process-based regime is more suitable for data release policy than the output-based regime employed in tort law and its causation issues[313]. Furthermore, data release policy should be similar to data security policy in its contextual approach, "because sound deidentification is similarly contingent upon a large number of factors"[314]. Indeed, "a 'one size fits all' standard for data release policy will not be effective", especially considering how quickly the field advances[315]. Furthermore, the most meaningful approach to data release is a risk tolerant one, as this "will help move us past the debate over the perfection (or lack thereof) of anonymization"[316]. This focus on the need for nuanced and realistic standards in the field of anonymization is really the approach we have been trying to support for the whole of this study.

Again mirroring data security policy, Rubinstein and Hartzog propose deferring to industry standards in order to allow "data release policy [to] be nimble, which in turn requires a relative lack of specificity"[317]. This approach leaves enough "breathing space to organizations where it is difficult to prescribe with precision the optimal protections in a given context" and "helps ensure that rules […] remain grounded in reality and up-to-date"[318]. However, in order to ensure "[c]ertain minimal protections for people", a "co-regulatory approach" is more advisable, so that regulators can "step[ ] in when industry standards fail to deliver that minimum standard of care"[319].

Looking more specifically at the HIPAA standard for anonymization that we have analyzed above, it "could move closer to process-based data releases in several different ways"[320]. For instance, the safe harbor method "could be modified to require technological, organizational, and contractual mechanisms for limiting access to deidentified data sets as

---

307 *Id. See* D.J. SOLOVE, *Privacy Self-Management and the Consent Dilemma*, 126 *Harv. L. Rev.* 1879 (2013).
308 RUBINSTEIN & HARTZOG, *supra* note 7, at 27.
309 *Id.* at 28.
310 *Id.*
311 *Id.* at 28-29.
312 *Id.* at 30.
313 *Id.* at 31.
314 *Id.* at 32. Such factors include: "different motivations for attacks, different approaches for computing reidentification risk, the different standards that have been used to describe the abilities of the "attacker", the variety of harms that can result from the use or distribution of de-identified data, the effort that the organization can spend performing and testing the deidentification process, the utility desired for the de-identified data, the ability to use other controls that can minimize risk, and the likelihood that an attacker will attempt to reidentify the data, and amount of effort the attacker might be willing to expend". *Id.*
315 *Id.* at 33.
316 *Id.* at 34.
317 *Id.* at 41.
318 *Id.*
319 *Id.* at 42.
320 *Id.* at 46.

well as deidentification"[321]. In order to comply with HIPAA, companies could be required to show the implementation of "a comprehensive data release program"[322]. Generally speaking, the focus should not be on "mechanically removing a pre-set list of identifiers", but on the implementation of risk-minimizing procedures based on threat modeling[323]. Threat models would then be "used to calculate risk as soundly and accurately as possible" and "guide companies toward the implementation of deidentification safeguards or use of other SDL methods"[324].

Indeed, privacy policy is an inherently multidisciplinary field and we should aim at bridging the gaps between policy, law, and technology. Thus, it is wise to adopt a "holistic approach" which includes "not just data flow controls but also organizational structure, education, and more careful deidentification rhetoric", using "the full spectrum of SDL techniques"[325] as we have described in the previous paragraph. The shift to a risk-based process would create incentives "to embrace the full spectrum of SDL methods and to combine deidentification techniques with access controls to protect data", and would avoid promises regarding perfect anonymity, which would be replaced by "appropriate assurances based on reasonable security measures"[326]. Indeed, "[i]f companies do not promise perfection and people do not expect it, then deidentification policy will be more likely to reflect reality"[327].

4.4 Risk Factors

We will now try to identify the different risk factors "to be balanced in determining how protecting a company must be when releasing a data set"[328].

What is the likelihood of successful re-identification? — Data controllers should focus on the concrete means that would be necessary to reverse the anonymization technique, looking in particular at the cost and the skills needed to implement them to assess their likelihood[329]. For example, the Article 29 Working Party advises balancing the data controller's anonymization effort and costs against "the increasing low-cost availability of technical means to identify individuals in datasets, the increasing public availability of other datasets . . . and the many examples of incomplete anonymisation entailing subsequent adverse, sometimes irreparable, effects on data subjects"[330]. The ICO Code of Practice remarks that sometimes the risk of re-identification is clear, such as when the combination of publicly available data with the 'anonymized' data can lead to re-identification, but usually there is no such bright-line guidance[331]. Another element bearing on the re-identification risk is the volume of data, as "[s]ome large data sets have a high degree of unicity, which makes it easier to launch reidentification attacks"[332]. Furthermore, the sensitivity of the data also

---

321 *Id.*
322 *Id.*
323 *Id.*
324 *Id.*
325 *Id.* at 35.
326 *Id.* at 47.
327 *Id.* at 49.
328 *Id.* at 38.
329 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 8-9.
330 *Id.*, at 9.
331 UK ICO Code, at 21.
332 RUBINSTEIN & HARTZOG, *supra* note 7, at 38.

plays a pivotal role, as "[s]ome information, like health and financial information, is more sensitive and thus more likely to be targeted by attackers"[333].

Who is going to receive the data? — There are three increasingly risky types of recipients of data: 1) internal recipients, 2) trusted recipients, and 3) the general public[334]. With respect to trusted recipients, "there might exist several tiers […], with increasing protections tied to less-trustworthy recipients"[335]. Releases to the general public are "inherently problematic and require the greatest amount of protections"[336]. Indeed, data controllers should carefully consider the different disclosure options, because the "publication of anonymised data to the world at large" and "limited access" entail very different degrees of risk[337] and ask for the imposition of different obligations[338].

Interestingly, the Article 29 Working Party advises looking at all the means likely reasonably to be used by any person (and not just by the data recipient)[339]. The UK Information Commissioner's Office provides some practical suggestions useful to assess the re-identification risk, according to which a data controller should, for instance, use the so-called 'motivated intruder' test[340]. In other words, a useful approach may be that of inquiring into whether a person with no prior knowledge who wants to identify the individual would be able to do so, assuming that he is reasonably competent, has access to Internet, libraries and public documents and would, for instance, ask questions to people who may have additional knowledge.[341] This test is said to strike a good balance because it strives to consider the perspective of the average person rather than that of people with very high technical knowledge or completely lacking in research skills.[342] Some practices are suggested in order to employ this test: carrying out web searches, searching the archives of newspapers to look for connections with crime map data, using social networks to inquire into potential connections to user's profiles, using the electoral register and library resources[343]. Furthermore, according to the UK ICO Code, a data controller should consider the possibility of individuals with prior knowledge (e.g., family members, doctors…*etc.*), looking in particular at whether this other individual would learn anything

---

333 *Id.*

334 *Id.*

335 *Id.* at 39.

336 *Id.* For example, Tene and Wolf have proposed that "[w]here data are shared publicly or made freely available to transferees, technical safeguards such as differential privacy […] be applied". TENE & WOLF, *supra* note 50, at 7. *See* C. DWORK, *Differential Privacy*, in 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006).

337 UK ICO Code, *supra* note 16, at 37.

338 TENE & WOLF, *supra* note 50, at 5 ("Different obligations should be imposed depending on whether the intended recipients of data are the public at large, contractually bound service providers or business associates, researchers subject to institutional review boards, or internal employees").

339 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 9. This triggers an important consequence: whenever the data controller retains the original identifiable data at event-level and hands over part of this data, maybe after masking the identifiable data, the resulting dataset is still considered personal data in the European framework. The dataset is only considered anonymous if the data controller aggregates the data to a level where the individual events are no longer identifiable and if the original raw data is deleted. *Id.*

340 UK ICO Code, at 22.

341 *Id.* at 22-23. The ICO Code of Practice specifies that the intruder is assumed not to have specialist knowledge such as hacking skills, and he is assumed not to break the law in his identification attempt. *Id.* at 23.

342 *See id.*

343 *Id.* at 23-24.

new and at what information he is likely to possess already and trying to avoid making assumptions that are not always warranted (e.g., we cannot presume complete openness in family relationships)[344]. However, it is better to start the risk assessment from recorded information and established fact, as opposed to personal knowledge, which, as much as it could lead to identification, is very hard to substantiate and connect to re-identification with a sufficient degree of plausibility[345]. Also, a data controller should assess whether the individuals who are likely to be able to carry out re-identification are also likely to actually do it, as some may have reasons to avoid it (e.g., doctors' ethical obligations)[346].

In order to figure out if an organization can be considered a "trusted" recipient, its privacy program can be evaluated, looking at whether it "collect[s] and store[s] data in a way that minimizes the risk of reidentification and sensitive attribute disclosure" and "it offer[s] privacy training to its employees, segment[s] the virtual and physical storage of data, implement[s] company policies regarding deidentification, and set[s] a tone within the organization regarding data minimization and anonymization as important privacy protections"[347].

What use will be made of the data? — Clearly there are some uses that are riskier or more problematic, such as "commercial or discriminatory purposes", which create a greater need for protections "given the potential harm and motivations by attackers to identify people or sensitive attributes" [348]. On the other hand, it has been argued that "protections should be lowered if the data is to be used for a significant public good or to help people avoid serious harm"[349]. In order to make this assessment, data controllers can also look at the needs of the organization receiving the anonymized information[350].

What data treatment techniques have been implemented? — The re-identification risk can vary "according to the ways data is manipulated through the use of de-identification and SDL techniques to protect data subjects"[351]. Also, the risk is much greater if the data set includes non-anonymized portions: data controllers should "take into account the identification potential of the non-anonymised portion of a dataset (if any), especially when combined with the anonymised portion, plus of possible correlations between attributes (e.g. between geographical location and wealth level data)"[352].

What data access controls have been applied? — The risk of reidentification is lower if "SDL and other access controls are utilized to limit who can access data and how they can access it"[353]. For instance, companies can choose to disclose data only to trusted recipients through contractual agreements whereby the data recipient agrees "to protect the data and refrain from attempting reidentification"[354].

---

344 *Id.* at 24-25.
345 *Id.* at 26.
346 *Id.* at 25.
347 RUBINSTEIN & HARTZOG, *supra* note 7, at 39.
348 *Id.* at 40. *See also* Article 29 WP Opinion 05/2014 on anonymisation techniques, at 25 (stating that data controllers should clearly set out the purposes to be achieved through the anonymised data set, because they play a crucial role in the determination of the identification risk).
349 RUBINSTEIN & HARTZOG, *supra* note 7, at 40.
350 *See* UK ICO Code, at 17.
351 RUBINSTEIN & HARTZOG, *supra* note 7, at 40.
352 Article 29 WP Opinion 05/2014 on anonymisation techniques, at 24.
353 RUBINSTEIN & HARTZOG, *supra* note 7, at 40.
354 *Id.*

What are the data subject's expectations? Has the data subject provided his or her consent? — Indeed, if consent is "meaningful" and "properly obtained", it "can mitigate the need to offer robust protections"[355]. Furthermore, consumer expectations should be at least met, in order for protections to avoid being deceptive[356].

5. Comparative Conclusions

This analysis of the role of anonymization with respect to health data and of the existing legal standards leads to some important conclusions. We need to abandon the illusion of perfection when building up legal standards and come up with novel, complex solutions that take into account all the different nuances of the world around us. "The myth of perfection persists because it is potent", but "[w]e should abandon the ideal of the sublime in cyberlaw"[357]. Focusing on achieving perfectly defined, automatic standards constitutes a distraction from what really matters. As we have seen in the previous chapters, efficiency is not a goal but is a means to pursue other goals. Also, accepting imperfection and risk is in fact what allows us to be realistic, as privacy law and policy is inherently human, especially when it deals with health data. If health data protection aims at protecting information concerning a human activity through a human activity, the hope to achieve perfect, flawless solutions is merely speculative. Indeed, "the imperfect – the flawed – is often both effective and even desirable as an outcome of legal regulation"[358].

First of all, the dichotomy between protected, identifiable data and unprotected, anonymized data needs to be given a second thought. Both the European and the U.S. legal systems rely on this basic distinction, while retaining some other differences. However, thinking of identifiability as a spectrum is more accurate, and more importantly, it provides better insight into the need for striking a balance on a case-by-case basis. Indeed, each data re-use may present the need for a different degree of specificity of the data and for a different amount of protection for the data subject. As this switch to conceiving identifiability as a continuum is hoped for by a large number of commentators, it is disappointing to see how the proposed General Data Protection Regulation does not adopt this change of heart.

Secondly, we should stop "expecting the impossible" by overlooking the existence of re-identification risk. The issue of anonymization should be re-framed and be transformed into a search for ways to protect privacy that are tailored to the circumstances. The concept of "anonymization" as we have been commonly using it "simply over-promise[s]", as it "create[s] expectations of near-perfection and lull[s] people into a false sense of security"[359]. Even data that have been de-identified pursuant to the legal standards are not immune from privacy risks in today's interconnected world. We should accept the fact that re-identification risk cannot be brought to zero, especially if data need to be kept useful for research. Thus, anonymization in the field of health data cannot be dealt with only by optimizing techniques and scientific tools. Additional layers of protection need to be implemented that do not rely on technical measures. An example is represented by contractual obligations, such as an agreement between a data discloser and a data recipient. Furthermore, we can think more generally of the compliance with ethical frameworks surrounding the processing and re-use of highly sensitive data such as health records,

---

355 *Id.* at 41.
356 *Id.*
357 BAMBAUER, *supra* note 1.
358 *Id.*
359 RUBINSTEIN & HARTZOG, *supra* note 7, at 48.

ultimately based on the respect for human dignity. Defending the human person should be the ultimate goal of the health data protection policy, and the establishment of meaningful protections including anonymization should pursue this overarching end. Similar to what we do with other human rights in other sectors, we should accept the complexity of reality and abandon the focus on the (impossible) achievement of perfect outcomes. Rather, we should aim at designing a set of nuanced and tailored measures amounting to a complex privacy-protective process, which can be adapted to all the different needs.

Conclusions

There are two goals that should be pursued in the field of health data privacy: the protection of human dignity and the promotion of a data protection culture based on such human values. This is true of privacy law as a whole but is even more crucial in the processing and treatment of health data inasmuch as they express our weaknesses. We could probably regard our diseases as our "inefficiencies", but using the "efficiency" language sounds forced and merciless when referring to human beings. Indeed, this shows once again how the goals we pursue in this field should not be spelled out in terms of efficiency, but rather in terms of dignity and adherence to the complexity of reality.

The pursuit of flawless, bright-line rules is both deceptive and misleading. All realities that relate to human beings are featured by some degree of imperfection, and law should not make deceptive promises of perfection. Nevertheless, we have seen how health data protection has been fraught with overly simplistic, superficial standards, which fail to take into account the different nuances. To think of the issues as black or white is naïve as it fails to take into account the inherent intricacy of reality. "For technology truly to augment reality, its designers and engineers should get a better idea of the complex practices that our reality is composed of"[1]. A more sound policy consists in accepting and treasuring inefficiency, because cracks are "how the light gets in"[2]. As much as we all struggle to accept our weaknesses, the best way to provide adequate protection for the data that express them does not consist in pursuing perfectly efficient systems, but rather in designing rules that take into account the nuances pertaining to anything that relates to human beings. Hence, law should not disregard the many different aspects within each of these issues. Rather, data controllers should perform a deeper, subtler analysis based on their understanding of what is really at stake, without relying on any oversimplified standard. The old dichotomies should be abandoned and there should be a switch to a risk-analytic approach.

The analysis of the legislation in Europe and in the United States in Chapter I leads to the awareness that the crux of the problem is to protect health data privacy and uphold the value of the human person while allowing for efficient and smooth transactions. The adoption of bright-line rules that create incentives to formally comply with the standards has proven to be insufficient. Thus, in order for this balance to be adequately struck, the law should design more nuanced standards, which generate incentives to regularly perform a risk assessment and contribute to the creation of a data protection culture. Arguably, the "Data Protection Impact Assessment" introduced by the new GDPR goes in this direction. The risk-analytic procedures should be constantly updated and tailored to the circumstances.

The consent of the data subject is one of the instances where processing of health data is allowed and is the basis for the creation of electronic health records in most systems. However, one should not rely on consent as a silver bullet. The GDPR will strengthen the provisions on consent, but lack of information, biases and power imbalance undermine the patient's ability to make meaningful choices. Furthermore, the pursuit of the so-called patient empowerment should not shadow the fact that the patient cannot be fully in charge of her own health, as her position of weakness requires some guidance. This is

[1] E. MOROZOV, *To Save Everything Click Here: The Folly of Technological Solutionism*, 2014, at 13.
[2] LEONARD COHEN, "*Anthem*" (song), *The Future*, Columbia 1992.

one of the reasons why it is crucial to remember that the delivery of health care is based on the human relationship between patient and physician.

Turning to Chapter II, the implementation of electronic health record systems is another example of the tendency of our era to pursue efficiency and overlook the competing interests. Any effort to welcome technology in the delivery of health care without forgetting that healing is an activity performed by human beings for human beings should be highly appreciated. It is necessary to strike the right balance between the use of technology and the ability to treat health care as a human activity and patients as human beings rather than as stacks of data.

Another superficial distinction that we should abandon in the realm of health data is the dichotomy between personal and anonymous data. Chapter III has shown that, as advocated by many scholars, this binary choice should be replaced by a more nuanced range of different situations based on the risk of re-identification. The new EU Regulation disappointingly fails to adopt this new approach and retains the outdated distinction. Switching to conceiving identifiability as a spectrum better shows the need for case-by-case evaluations, as each situation may require a different degree of data quality and a different amount of privacy protection. Furthermore, the issue of anonymization should no longer be framed as the pursuit of a result, because such result is impossible to achieve given the ever-present re-identification risk and the growing chances of data aggregation. It is more reasonable to think of anonymization as part of a broader effort to protect privacy and combine it with other layers of protection, such as contractual obligations or ethical frameworks.

Thus, the field of health data protection very clearly shows some of the flaws of the way our society perceives efficiency as a goal and technology as an autonomous force. The peculiarities of health data require overly simplistic approaches to be replaced by a deeper and subtler understanding of the complex and multifaceted structure of the issues surrounding health data protection. The myth of perfection should be abandoned, as it lures us into disregarding what really matters. It is necessary to accept inefficiency because it is impossible to eradicate. Since health data protection aims at safeguarding data concerning an intrinsically human activity the hope to achieve flawless solutions is no more than speculative. This work goes as far as maintaining that inefficiency should not only be accepted, but also treasured and valued, as it allows for laws and policies to be fully adherent to reality. The impossibility to achieve perfect outcomes is a precious reminder, as it constantly forces data controllers, policymakers and the society at large to carefully assess the reasons for protecting privacy in order to design new standards. In the field of health data privacy, cracks are "how the light gets in" because they keep us from fully forgetting that, as the European Data Protection Directive aptly highlights, data processing systems are designed to serve man.

Legislation and Case Law

Council of Europe

COUNCIL OF EUROPE, Committee of Ministers (1997), *Recommendation R(97)5 to member states on the protection of medical data*, 13 February 1997

COUNCIL OF EUROPE, *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, 1997, available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm>

COUNCIL OF EUROPE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

COUNCIL OF EUROPE, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5

EUROPEAN COURT OF HUMAN RIGHTS, *Amann v. Switzerland*, No. 27798/95, 2000-II Eur. Ct. H.R.

European Union

Charter of Fundamental Rights of the European Union, December 7, 2000, O.J., No. C 364, 2000

Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. C 115/47

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), 2000 O.J. (L 178) 1 (July 17, 2000)

Directive 2001/20/EC on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, OJ 2001 L 121/34

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 O.J. (L 201) 37 (July 31, 2002)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

EUROPEAN COMMISSION, *Decision 2000/520/EC pursuant to European Parliament and Council Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, OJ 2000 No. L215/7

EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

EUROPEAN PARLIAMENT, *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>

Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), December 15, 2015, available at <http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf>

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306

EUROPEAN COURT OF JUSTICE, Judgment of 6 November 2003, Case C-101/01 - *Bodil Lindqvist*

EUROPEAN COURT OF JUSTICE, Judgment of 6 October 2015 in Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, EU:C:2015:650

EU Member States

France – Healthcare Insurance Act no. 2004-810 of 13 August 2004

Italy – Constitution of the Italian Republic, available at <https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf>

Italy – Decree of the President of the Council of Ministers of September 29, 2015, no. 179 (published in Italy's Official Journal no. 263 dated November 11, 2015).

Italy – Decree-law of October 18, 2012, no. 179 (converted into law by L. of December 17, 2012, no. 221 and published in Italy's Official Journal no. 294, dated December 18, 2012)

Italy – Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003 (as translated at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932)

Italy – Royal Decree no. 1631 of 30 September 1938, Presidential Decree No. 128 of 27 March 1969, Decree of the Department of Health of 5 August 1977

United States

American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

Exec. Order No. 13,335, 69 Fed. Reg. 24059 (April 30, 2004)

Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 301-99 (2012))

Health Information Technology for Economic and Clinical Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.)

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 5-42 U.S.C.)

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. part 160 and 164)

Texas Hospital Licensing Law (Tex. Health & Safety Code Ann. § 241.152(a))

Texas Medical Practice Act (Tex. Occ. Code Ann. § 159.002(a)-(b))

Bayne v. Provost, 359 F. Supp. 2d 234 (N.D.N.Y. 2005).

Holman v. Rasak, 785 N.W.2d 98, 109 (Mich. 2009)

Holmes v. Nightingale, 158 P.3d 1039 (Okla. 2007)

Law v. Zuckerman, 307 F. Supp. 2d 705 (D. Md. 2004)

Marine Shale Processors, Inc. v. State of Louisiana Dep't of Health, 572 So. 2d 280 (La. App. 1 Cir. 1990)

Nixon v. Administrator of General Services, 433 U.S. 425 (1977)

Smith v. Rafalin, 800 N.Y.S.2d 357 (N.Y. Sup. Ct. Mar. 24, 2005)

Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011)

South Carolina Medical Association v. Thompson (4th Cir. 2003) 327 F.3d 346 (4th Cir. 2003)

Southern Illinoisan v. Illinois Department of Public Health, 844 N.E. 2d 1 (Ill. 2006)

State ex rel. *Proctor v. Messina*, 320 S.W.3d 145 (Mo. 2010) (*en banc*)

United States v. Westinghouse Electric Corp., 638 F.2d 570, 578 (3rd Cir. 1980)

Whalen v. Roe, 429 U.S. 589 (1977)

Williams Law Firm v. Board of Supervisors, 878 So. 2d 557 (La. App. 1 Cir. 2004)

Soft Law and Policy

European Union

COUNCIL OF THE EUROPEAN UNION, Interinstitutional File: 2012/001 (COD), 11 June 2015, available at <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>

EUROPEAN COMMISSION - *Press release, Agreement on Commission's EU data protection reform will boost Digital Single Market*, Brussels, 15 December 2015, available at <http://europa.eu/rapid/press-release_IP-15-6321_en.htm>

EUROPEAN COMMISSION – *Press release, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, Strasbourg, 2 February 2016, available at: <http://europa.eu/rapid/press-release_IP-16-216_en.htm>

EUROPEAN COMMISSION, *'e-Health – making healthcare better for European citizens: an action plan for a European e-Health Area'*, COM (2004) 356 final, 30 April 2004

EUROPEAN COMMISSION, *A digital agenda for Europe*, 26 August 2010, COM(2010)245

EUROPEAN COMMISSION, *Communication "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century"*, COM(2012)736 final

EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*, COM(2008) 689, Brussels, November 4, 2008

EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, COM(2015) 566 final (November 6, 2015)

EUROPEAN COMMISSION, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, (November 27, 2013)

EUROPEAN COMMISSION, *Europe 2020—A strategy for smart, sustainable and inclusive growth*, COM(2010)2020

EUROPEAN COMMISSION, *Factsheet on the "Right to be Forgotten" ruling*, available at <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>

EUROPEAN COMMISSION, Green Paper on mobile health, 10 April 2014, COM(2014) 219 final, complemented by a Staff Working Document (SWD(2014) 135 final)

EUROPEAN COMMISSION, MEMO/13/923 (October 22, 2013), available at <http://europa.eu/rapid/press-release_MEMO-13-923_it.htm>

EUROPEAN COMMISSION, MEMO/14/186, March 12, 2014, available at <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>

EUROPEAN COMMISSION, *Recommendation on cross-border interoperability of electronic health record systems*, COM(2008) 3282, Brussels, July 2, 2008

EUROPEAN COMMISSION, *White paper - Together for Health: A Strategic Approach for the EU 2008-2013*, COM(2007) 630 final, Brussels, October 23, 2007

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 1/2015 – Mobile Health – Reconciling technological innovation with data protection*, May 21, 2015

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the proposal for a Regulation of the European Parliament and of the Council on European Statistics*, COM(2007) 625 final (2008), OJ C 308, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008XX1203(01)>

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the proposal for a Regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work*, COM(2007) 46 final, available at <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-09-05_Statistics_health_data_EN.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Annex – health data in apps and devices* (Feb. 5, 2015), available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP 216 (April 10, 2014), available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136 (June 20, 2007), available at <http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/opinion_04-2007_personal_data_/Opinion_04-2007_personal_data_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 02/2013 on apps on smart devices*, 00461/13/EN WP 202 (February 27, 2013), available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196 (July 1, 2012), available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Statement of the Article 29 Working Party on the consequences of the Schrems Judgment*, Brussels, 3 February 2016, available at <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document on the processing of personal data relating to health in electronic health records (EHR)*, 00323/07/EN WP 131 (February 15, 2007), available at

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf>

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (WP 153)*, 24 June 2008

EUROPEAN UNION ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114)*, 25 November 2005

Handbook on European data protection law (2014), available at <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law>

Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services – Final report and recommendations, July 23, 2014, available at <http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf>

Special Eurobarometer 359 – "Attitudes on Data Protection and Electronic Identity in the European Union" (2011), available at <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>

EU Member States

England – DEPARTMENT OF HEALTH, *Policy Paper – Personalised health and care 2020: a framework for action*, November 13, 2014, available at <https://www.gov.uk/government/publications/personalised-health-and-care-2020/using-data-and-technology-to-transform-outcomes-for-patients-and-citizens>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Authorisation No. 2/2014 Concerning Processing of Data Suitable for Disclosing Health* (published in Italy's Official Journal No. 301 of 30 December 2014)

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Authorisation No. 9/2014 - General Authorisation to Process Personal Data for Scientific Research Purposes* (published in Italy's Official Journal No. 301 of 30 December 2014)

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Decision *"Lavoro: buste paga e dati che rivelano lo stato di salute del dipendente"*, June 18, 2009, available at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1640331>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Decision "*Lo scontrino fiscale "parlante" per l'acquisto di farmaci"*, April 29, 2009, available at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1611565>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Dossier sanitario: prescrizioni per il sistema informativo delle prestazioni sanitarie erogate da un'Azienda sanitaria*, October 22, 2015, available at

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4449114>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, General Authorisation No. 8/2014 for the Processing of Genetic Data (published in Italy's Official Journal No. 301 of 30 December 2014)

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guidelines for Data Processing within the Framework of Clinical Drug Trials* - 24 July 2008, as published in the Official Journal of the Italian Republic (no. 190 dated 14 August 2008)

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guidelines on the Electronic Health Record and the Health File*, July 16, 2009 (published in Italy's Official Journal no. 178, dated 3 August 2009), available at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guidelines on Online Examination Records*, November 19, 2009 (published in Italy's Official Journal no. 288, dated December 11, 2009), available at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634292>

Italy – GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guidelines on the "Dossier sanitario"*, June 4, 2015, available at <http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+-+Allegato+A.pdf>

Italy – MINISTRY OF HEALTH, *Il Fascicolo Sanitario Elettronico – Linee guida nazionali*, November 11, 2010, available at <http://www.salute.gov.it/imgs/C_17_pubblicazioni_1465_allegato.pdf>

UK – INFORMATION COMMISSIONER'S OFFICE, *Anonymisation: Managing Data Protection Risk Code of Practice* (2012), available at <https://ico.org.uk/media/1061/anonymisation-code.pdf >

United States

CENTERS FOR MEDICARE & MEDICAID SERVICES, *An Introduction to the Medicare EHR Incentive Program for Eligible Professionals*, available at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf>

CENTERS FOR MEDICARE & MEDICAID SERVICES, *Certified EHR Technology* (Oct. 11, 2011), available at <http://www.cms.gov/EHRIncentivePrograms/25_Certification.asp>

CENTERS FOR MEDICARE & MEDICAID SERVICES, CMS.gov, *EHR Incentive Programs*, available at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms/>

CENTERS FOR MEDICARE & MEDICAID SERVICES, CMS.gov, *Medicare and Medicaid EHR Incentive Program Basics*, available at <http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html>

CENTERS FOR MEDICARE & MEDICAID SERVICES, Office of Public Affairs, *CMS EHR Meaningful Use Overview*, available at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html>

DEPARTMENT OF HEALTH & HUMAN SERVICES, *Health Information Privacy: Breaches Affecting 500 or More Individuals*, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

DEPARTMENT OF HEALTH & HUMAN SERVICES, HHS Website, "*Federal Policy for the Protection of Human Subjects ('Common Rule')*", available at <http://www.hhs.gov/ohrp/humansubjects/commonrule/>

DEPARTMENT OF HEALTH & HUMAN SERVICES, HHS Website, "*The Common Rule*", available at <http://www.hhs.gov/ohrp/humansubjects/>

DEPARTMENT OF HEALTH & HUMAN SERVICES, *Summary of the HIPAA Privacy Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>

EXECUTIVE OFFICE OF THE PRESIDENT – PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, *Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: the Path Forward,* December 2010, available at <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf>

FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era with Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>

GOOGLE OFFICIAL BLOG, *An update on Google Health and Google PowerMeter*, June 24, 2011, available at <http://googleblog.blogspot.it/2011/06/update-on-google-health-and-google.html?m=1>

Institute of Medicine (US), Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule (SHARYL J. NASS, LAURA A. LEVIT & LAWRENCE O. GOSTIN eds., National Academies Press 2009), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, available at <http://www.ncbi.nlm.nih.gov/books/NBK9578/>

NAT'L COMM. ON VITAL & HEALTH STATISTICS, U.S. Dep't of Health and Human Servs., *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data* (2007), available at <http://www.ncvhs.hhs.gov/071221lt.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), E. MCCALLISTER, T. GRANCE AND K. SCARFONE, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-122 (2010), available at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Internal Report 8053, De-Identification of Personal Information* (2015), available at <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *NIST Cloud Computing Program* (Jan. 28, 2014), available at <http://csrc.nist.gov/groups/SNS/cloud-computing/>

NIH PUBLICATION NUMBER 04-5489, *Research Repositories, Databases, and the HIPAA Privacy Rule (2004*), available at <http://privacyruleandresearch.nih.gov/research_repositories.asp>

PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *Report to the President Realizing the Full Potential of Health Information Technology to Improve Health Care for Americans: The Path Forward* (2010), available at <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf>

THE WHITE HOUSE, *Transforming Health Care: The President's Health Information Technology Plan*, April 2004, available at <http://georgewbush-whitehouse.archives.gov/infocus/technology/economic:policy200404/chap3.html >

U.S. FOOD & DRUG ADMIN., *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff* (Sept. 25, 2013)

Bibliography

ABET F., *Il ruolo delle tecnologie per una sanità moderna: la telemedicina*, in *Informatica & Documentazione*, 2007, 51

ACCIAI R. (ed.), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004

ACCIAI R., *La tutela della privacy ed il s.s.n.*, in *Ragiusan*, 2003, fasc. 225/226, 20

ALEXIN Z., *Does fair anonymization exist?*, *International Review of Law, Computers & Technology*, Vol. 28, No.1, 21 (2014)

BAICE P., *La cartella clinica tra diritto di riservatezza e diritto di accesso*, *Ragiusan* n. 280/290, Sez. 1, 2008

BAMBAUER D.E., *The Myth of Perfection*, 2 *Wake Forest L. Rev.* 22 (2012)

BARTH-JONES D.C., *The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now* (2012), available at <http://ssrn.com/abstract=2076397>

BAUMAN Z. & LYON D., *Liquid Surveillance*, 2013

BENITEZ K. & MALIN B., *Evaluating re-identification risks with respect to the HIPAA privacy rule*, 17 *J. Am. Med. Inform. Assoc.* 169-177 (2010), available at <http://jamia.bmj.com/content/17/2/169.full.pdf+html>

BERG J., *The E-Health Revolution and the Necessary Evolution of Informed Consent*, 11 *Indiana Health Law Review* 589 (2014)

BIANCA C.M., BUSNELLI F.D. (eds.), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003 n. 196 ("Codice Privacy")*, Padova, 2007

BIASIOTTI A., Codi*ce della privacy e misure minime di sicurezza: d.lgs. 196/2003*, II ed., Roma, 2004

BLUMENTHAL D. AND TAVENNER M., *The "Meaningful Use" Regulation for Electronic Health Records*, 363 *New England Journal of Medicine* 501 (2010)

BOMASH K., *Privacy and Public Health in the Information Age: Electronic Health Records and the Minnesota Health Records Act*, 10 *Minn. J.L. Sci. & Tech.* 117 (2009)

BOS L. MARSH A., CARROLL D., GUPTA S., REES M., *Patient 2.0 Empowerment*, in H. ARABNIA, A. MARS (EDS.), *Proceedings of the 2008 International Conference on Semantic Web & Web Services* SWWS08 (2008)

BRENNA E., *La valutazione economica delle tecnologie in sanità con particolare riferimento all'area della telemedicina*, in *Sanità pubbl.*, 2001, 89

BRENNAN P, SAFRAN C., *Report of conference track 3: patient empowerment*, 69 *International Journal of Medical Informatics* 301 (2003)

BRICKELL J. & SHMATIKOV V., *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, The 14th ACM SIGKDD Int'l Conference on Knowledge Discovery & Data Mining 70 (August 2008).

BRISCH K.M. AND HAUPT C.E., *Information Technology Meets Healthcare: The Present and Future of German and European E-Health Initiatives*, 12 *DePaul J. Health Care L.* 105 (2009)

Bryan Cave LLP Global Data Privacy and Security Team, *Business Associates At A Glance: Responsibilities And Liabilities* (2015), available at <http://bryancavedatamatters.com/wp-content/uploads/2015/12/Final-Business-Associates_At-A-Glance.pdf>

Bryan Cave LLP Global Data Privacy and Security Team*, Healthcare Data Breach Enforcements and Fines At A Glance* (2015), available at <http://bryancavedatamatters.com/healthcare-data-breach-enforcements-and-fines-at-a-glance/>

Bryan Cave LLP Global Data Privacy and Security Team*, Healthcare Data Breach State-Level Enforcements and Fines At A Glance* (2015), available at <http://www.bryancavedatamatters.com/state-level-enforcement-and-fines-for-health-data-breaches-at-a-glance/>

Bryan Cave LLP Global Data Privacy and Security Team, *Privacy Shield: Safe Harbor 2.0?*, February 3, 2016, available at <https://www.bryancave.com/en/thought-leadership/privacy-shield-safe-harbor-2-0.html>

Bryan Cave LLP Global Data Privacy and Security Team, *The Causes of Healthcare Breaches At A Glance* (2015), available at <http://bryancavedatamatters.com/the-causes-of-healthcare-breaches-at-a-glance/>

Bryan Cave LLP Global Data Privacy and Security Team, *Privacy Shield: Safe Harbor 2.0?*, February 3, 2016, available at <https://www.bryancave.com/en/thought-leadership/privacy-shield-safe-harbor-2-0.html>

BUCCOLIERO L., CACCIA C., NASI G., *E-he@lth. Percorsi di implementazione dei sistemi informativi in sanità*, Milano 2005

BUNTIN M.B. ET AL., *The Benefits Of Health Information Technology: A Review Of The Recent Literature Shows Predominantly Positive Results*, in 30 He*alth Affairs*, 2011, 464

BYGRAVE L.A., *Data Privacy Law: An International Perspective*, Oxford University Press, 2014

BYGRAVE L.A., *Data Protection Law. Approaching Its Rationale, Logic and Limits,* Kluwer Law International, 2002.

CACCIA C., *Sanità digitale: quale futuro. Considerazioni per una speranza di successo*, *Rivista elettronica di Diritto, Economia, Management,* n. 3, 2014

CAGGIA F., *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *Il codice del trattamento dei dati personali*, Torino, 2007

CALDARELLA J., *Privacy and Security of Personal Health Records Maintained By Online Health Services*, 20 *Alb. L.J. Sci. & Tech.* 203 (2010)

CALLENS S., *Telemedicine and the E-Commerce Directive*, 9 *European Journal of Health Law* 93 (2002)

CALLENS S., *The EU legal framework on e-health*, in E. MOSSIALOS, G. PERMANAND, R. BAETEN, T. HERVEY (EDS.), *Health Systems Governance in Europe – The Role of EU Law and Policy*, Cambridge University Press, 2010

CANGELOSI G., *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in *Dir. famiglia*, 2007

CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (eds.), *Il codice dei dati personali. Temi e problemi*, Milano, 2004

CAREY P., *Data Protection Law. A Practical Guide to UK and EU Law*, Oxford University Press, 2nd edition, 2004

CARTER P., *HIPAA Compliance Handbook*, Gaithersburg, - Alphen, 2014

CASINI M., SARTEA C., *La consulenza genetica in Italia: problemi, regole di consenso informato, trattamento dei dati genetici e privacy*, in *Medicina e morale*, 2009, 1121

CASONATO C., *Il consenso informato. Profili di diritto comparato*, in C. CASONATO, T.E. FROSINI, T. GROPPI (eds.), *Diritto pubblico comparato ed europeo*, 2009, 1052

CASSANO G., FADDA S. (eds.), *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy d.lgs. 30 giugno 2003, n. 196*, Milano, 2004

CAVO G.M., *La cartella clinica e la tutela della riservatezza del malato*, in *Sanità Pubblica e Privata*, fasc. 2 (2011)

CENTER FOR DEMOCRACY & TECHNOLOGY, *Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data* (2009), available at <https://www.cdt.org/files/pdfs/20090625_deidentify.pdf>

Center for Democracy & Technology, *Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data* 2 (2009).

CHAUDHRY B. ET AL., *Systematic Review: Impact of Health Information Technology on Quality, Efficiency and Costs of Medical Care*, in 144 *Ann. Intern. Med.*, 2006, 742

CHEN C., GARRIDO T., CHOCK D., OKAWA G., LIANG L., *The Kaiser Permanente Electronic Health Record: Transforming And Streamlining Modalities of Care*, 28 *Health Affairs*, 2009, 2 , 323

CIACCI G., *Privacy e sanità*, Roma, 2005

CIAMPI C., *La Sicurezza dei Dati Personali Sanitari*, in *Rivista elettronica di Diritto, Economia, Management*, n. 3, 2014

CIRILLO G.P. (ed.), *Il Codice sulla protezione dei dati personali*, Milano, 2004

CLINE J., *Privacy Matters: When Is Personal Data Truly De-Identified?*, COMPUTERWORLD (July 24, 2009), available at <http://www.computerworld.com/s/article/9135898/Privacy_matters_When_is_personal_data_truly_de_identified_>

COHEN B., *Regulating Data Mining Post-*Sorrell: *Using HIPAA To Restrict Marketing Uses of Patients' Private Medical Information*, 47 *Wake Forest Law Review* 1141 (2012)

Comments of the Electronic Privacy Information Center (EPIC) to the Federal Trade Commission, "Health Breach Notification Rulemaking," Project No. R911002 (2009), available at <https://www.ftc.gov/sites/default/files/documents/public_comments/health-breach-notification-rulemaking-541358-00125/541358-00125.pdf>

COPPIETERS Y. & LEVEQUE A., *Ethics, privacy and the legal framework governing medical data: opportunities or threats for biomedical and public health research*, 71 *Archives Of Pub. Health*, no. 15, 2013

CORLEY S.O., *Protection for Psychotherapy Notes Under the HIPAA Privacy Rule: As Private As A Hospital Gown*, 22 *Health Matrix: Journal of Law-Medicine* 489 (2002)

CORTEZ N., *The Mobile Health Revolution?*, 47 *U.C.D. L. Rev.* 1173 (2014)

CRIGGER B.J., *e-Medicine: Policy to Shape the Future of Health Care*, 36 *The Hastings Center Report* 12 (2006)

CUFFARO V., D'ORAZIO R. & RICCIUTO V. (eds.), *Il codice del trattamento dei dati personali*, Torino, 2007

DE AZEVEDO CUNHA, M.V., DONEDA, D., ANDRADE, N., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriori finalità: sfide alla* privacy, *Ciberspazio e diritto* 2010, Vol. 11, n. 4, 641 (2010)

DE HERT P. & GUTWIRTH S., *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action,* in S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?*, Springer, 2009

DE HERT P. & PAPAKONSTANTINOU V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, 28 *Computer Law & Security Review* 130 (2012)

DEVORE A.C., *Cloud Computing: Privacy Storm on the Horizon?*, 20 Alb. L.J. Sci. & Tech. 365 (2010)

DEVRIES W.T., *Protecting Privacy in the Digital Age*, 18 *Berkeley Tech. L.J.* 283 (2003)

DI CIOMMO F., *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002

DI IORIO C.T. & CARINCI F., *Privacy and Health Care Information Systems: Where Is The Balance?*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

DIMASI L., *Il trattamento dei dati personali in sanità e la circolazione delle informazioni nell'era dell'informatizzazione*, in *Sanità Pubblica e Privata*, 2011, fasc. 4, 28-43

DINUR I. & NISSIM K., *Revealing Information While Preserving Privacy*, in Proc. 22nd ACM Symp. On Principles Database Sys. 202 (2003), available at <http://portal.acm.org/citation.cfm?id=773173)>

DUMORTIER J. AND VERHENNEMAN G., *Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

DUMORTIER, J. & VERHENNEMAN, G., *Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the U.S.*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (eds.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

DUQUENOY P., MEKAWIE N.M. AND SPRINGETT M., *Patients, Trust and Ethics in Information Privacy in eHealth*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

EDELSTEIN L., *The Hippocratic Oath: Text, Translation, and Interpretation*, in R.M. VEATCH, *Cross-cultural Perspectives in Medical Ethics*, 2000

EGGERS D., *The Circle* (2013)

EL EMAM K., ALVAREZ C.*, A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques,* 5 Int'l Data Privacy Law 73-87 (2015), available at <http://idpl.oxfordjournals.org/content/early/2014/12/12/idpl.ipu033.abstract>

EL EMAM K., *Heuristics for De-identifying Health Data, IEEE Security & Privacy* 6(4):58-61 (2008), available at < http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4588232>

EL EMAM K., *Risk-based de-identification of health data*, *IEEE Security & Privacy* 2010, 8:64-67, available at <http://www.privacyanalytics.ca/wp-content/uploads/2013/12/riskdeid.pdf>

EL EMAM K., RODGERS S., MALIN B., *Anonymising and sharing individual patient data*, *BMJ* 2015; 350 :h1139, available at < http://www.bmj.com/content/350/bmj.h1139>

FILAURO C., *Telemedicina, cartella clinica elettronica e tutela della* privacy, *Danno e resp.* 5, 2011

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli 2012

FLAHERTY J.L., *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 *Am. J.L. & Med.* 416 (2014)

FLEMING G., *HIPAA-Cratic or HIPAA-Critical: U.S. Privacy Protections Should Be Guaranteed By Covered Entities Working Abroad*, 98 *Minnesota Law Review* 2375 (2014)

FLIER L.A., *Health information technology in the era of care delivery reform. To what end?*, in *JAMA*, 2012, 307, 24, 2593

FLORIO A., *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in *Ciberspazio e dir.*, 2010, 111

FRANCIS L., *Privacy and Health Information: The United States and the European Union*, 103 *Kentucky Law Journal* 419 (2015)

FRANCIS L.P., *When Patients Interact with EHRs: Problems of Privacy and Confidentiality*, 12 *Hous. J. Health Law & Policy* 171 (2012)

GARTEE R., *Electronic Health Records. Understanding and Using Computerized Medical Records*, Upper Saddle River - New Jersey, 2007

GEISSBUHLER A., SAFRAN C., BUCHAN I., ET AL., *Trustworthy reuse of health data: a transnational perspective*, in *International Journal of Medical Informatics*, vol. 82, issue 1, 2013, p. 1-9, available at <http://www.sciencedirect.com/science/article/pii/S138650561200202X>

GELLMAN R., *The Deidentification Dilemma: A Legislative and Contractual Proposal,* 21 Fordham Intell. Prop. Media & Ent. L.J. 33 (2011), available at <http://ir.lawnet.fordham.edu/iplj/vol21/iss1/2>

GEORGE C., WHITEHOUSE D. AND DUQUENOY P., *Assessing Legal, Ethical and Governance Challenges in eHealth*, in C. GEORGE, D. WHITEHOUSE AND P. DUQUENOY (EDS.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

GERING S.R., Electronic Health Records: How to Avoid Digital Disaster, 16 *Mich. St. U. J. Med. & L.* 297 (2012)

GILBERT F., *European Data Protection 2.0: New Compliance Requirements in Sight – What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 *Santa Clara Computer & High Tech. L.J.* 815 (2012).

GILBERT F., *Proposed EU Data Protection Regulation: The Good, The Bad, And The Unknown*, 15 *Journal of Internet Law* 1 (2012)

GOLLE P., *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 *ACM Workshop on Privacy in the Elec. Soc'y* 77 (2006), available at <https://crypto.stanford.edu/~pgolle/papers/census.pdf>

GOSTIN L., *Health Information Privacy*, in *Georgetown Law Faculty Publications and Other Works*, 1995

GOSTIN L.O. & HODGE, JR. J.G., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 *Minn. L. Rev.* 1439 (2002)

GRADY A, *Electronic Health Records: How The United States Can Learn From The French Dossier Medical Personnel*, 30 *Wis. Int'l L.J.* 374, 377 (2013).

GREENLEAF G., *'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?*, 29 *Computer Law & Security Review* 430 (2013)

GUARDA P., DUCATO R., *Profili giuridici dei Personal Health Records: l'autogestione dei dati sanitari da parte del paziente tra privacy e tutela della salute*, 3 *Rivista Critica del Diritto Privato* 389 (2014)

GUARDA P., *Fascicolo Sanitario Elettronico e protezione dei dati personali*, Università degli Studi di Trento, 2011

GUARDA P., *Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context*, Trento Law and Technology Research Group, Research Paper n. 23 (July 2015), available at

<https://iris.unitn.it/retrieve/handle/11572/109729/14864/Guarda_LawTechRP_23_2.pdf>

HALL M.A., *Property, Privacy and the Pursuit of Integrated Electronic Medical Records*, Wake Forest Univ. Legal Studies Paper No. 1334963

HATCH M., *HIPAA: Commercial Interests Win Round Two*, 86 *Minn. L. Rev.* 1481 (2002)

HÄYRY M., CHADWICK R., ARNASON V., ARNASON G. (eds.), *The ethics and governance of human genetic databases, European perspectives*, University Press, Cambridge, 2007

HELM A.M. & GEORGATOS D., *Privacy and mHealth: How Mobile Health "Apps" Fit Into A Privacy Framework Not Limited To HIPAA*, 64 *Syracuse L. Rev.* 131 (2014)

HERVEY T.K. & MCHALE J.V., *Health Law and the European Union*, Cambridge University Press, 2004

HILL K., *Adventures in Self-Surveillance, a.k.a. The Quantified Self, a.k.a. Extreme Naval-Gazing*, *Forbes* (Apr. 7, 2011)

HILLER J., MCMULLEN M.S., CHUMNEY W.M., BAUMER D.L., *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*, 17 *B.U. J. Sci. & Tech. L.* 1 (2011)

HODGE J.G. ET AL., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 *JAMA* 1466 (1999)

HOFFMAN S. & PODGURSKI A., *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 *Berkeley Tech. L.J.* 1523 (2009)

HOFFMAN S. & PODGURSKI A., *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, Working Paper 06-15, September 2006

HOFFMAN S. & PODGURSKI A., *Meaningful Use and Certification of Health Information Technology: What About Safety?*, Faculty Publications. Paper 3 (2011), available at <http://scholarlycommons.law.case.edu/faculty_publications/3>

HOFFMAN S. AND PODGURSKI A., *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 *S. M. U. L. Rev.* 85 (2012)

HOOVER B.K. & BRADSHAW M., *Not So Hip?: The Expanded Burdens on and Consequences to Law Firms as Business Associates Under HITECH Modifications to HIPAA*, 13 *Rich. J. L. & Pub. Int.* 313 (2010)

HOUSEH M., BORYCKI E., KUSHNIRUK A., *Empowering patients through social media: the benefits and challenges*, 20 *Health Informatics J.* 50 (2014)

Interview to Antonello Soro (Garante per la protezione dei dati personali), RaiNews 24, October 20, 2015, available at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4345229>

IZZO U. & GUARDA P., *Sanità Elettronica, Tutela Dei Dati Personali E Digital Divide Generazionale / E-Health, Data Protection And Generational Digital Divide*, Trento Law and Technology Research Group - Research Paper Series (2010), available at <http://eprints.biblio.unitn.it/archive/00001921/>

IZZO U. AND DUCATO R., *The Privacy of Minors within Patient-Centered e-Health Systems*, Trento Law and Technology Research Group, Research Paper n. 21, June 2014

IZZO U., *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, in *Danno e resp.*, 8-9, 807-18 (2000)

KELLEHER D., *A new Safe Harbor? Yes, it's possible* (Jan. 12, 2016), available at <https://iapp.org/news/a/173906/>

KLEINKE J.D., *Dot-Gov: Market Failure and the Creation of a National Health Information Technology System*, 24 *Health Aff.* 1246 (2005)

KLOSEK J., *Exploring The Barriers to The More Widespread Adoption of Electronic Health Records*, 25 *Notre Dame J. L. Ethics & Public Policy* 429 (2011)

KULYNYCH J. & KORN D., *Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule*, 28 *Am. J. L. & Med* 309 (2002)

KUNER C., *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Privacy & Security Law Report, 11 PVLR 06, 02/06/2012. Copyright 2012 by The Bureau of National Affairs, Inc., available at <http://amcham.dk/files/editor/Data_privacy_-_Kuner_EU_regulation_article.pdf>

LAFKY D., *The Safe Harbor Method of De-Identification: An Empirical Test, Department of Health and Human Services*, Office of the National Coordinator for Health Information Technology, October 8, 2009, available at <http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf>

LAMARQUE E., *Privacy e salute*, in M.G. LOSANO (ed.), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni. Roma-Bari*, 2001

LATIFI R. (ED.), *Current principles and practices of telemedicine and e-health*, Amsterdam 2008

LOSANO M.G. (ed.), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001

LYNSKEY O., *From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis*, in S. GUTWIRTH ET AL. (eds.), *European Data Protection: Coming of Age*, Springer, 2013

MAGNUSSON R.S., *The Changing Legal and Conceptual Shape of Health Care Privacy*, 32 *J. L. Med. & Ethics* 680 (2004)

MARCOTTE L., SEIDMAN J., TRUDEL K., BERWICK D.M., BLUMENTHAL D., MOSTASHARI F. AND JAIN S.H., *Achieving Meaningful Use of Health Information Technology: A Guide for Physicians to the EHR Incentive Programs*, *Archives of Internal Medicine* 172 (9):731–6 (2012)

MASCALZONI D. (ed.), *Ethics, Law and Governance of Biobanking. National, European and International Approaches*, Springer 2015.

MASCETTI S., MONREALE A., RICCI A. AND GERINO A., *Anonymity: A Comparison Between the Legal and Computer Science Perspectives*, in S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer 2013

MASSON V., *Le dossiér medical personnel fait peau neuve*, Le Figaro, October 16, 2015, available at <http://www.lefigaro.fr/conjoncture/2015/10/16/20002-20151016ARTFIG00097-le-dossier-medical-personnel-fait-peau-neuve.php>

MCCARTHY C.P., *Paging Dr. Google: Personal Health Records and Patient Privacy*, 51 *William & Mary L. Rev.* 2243 (2010)

MCCUBBIN C.N., *Legal and Ethico-legal Issues in E-healthcare Research Projects in the UK*, 62 *Social Science & Medicine* 2768 (2006)

MONDUCCI J., PASETTI G., *Il trattamento dei dati sanitari e genetici*, in J. MONDUCCI, G. SARTOR (eds.), *Il Codice in materia di protezione dei dati personali. Commento sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004

MOROZOV E., *To Save Everything, Click Here: The Folly of Technological Solutionism* (2013)

MOSTERT M., BREDENOORD A.L., BIESAART M. AND VAN DELDEN J., *Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach*, *European Journal of Human Genetics* (2015), doi:10.1038/ejhg.2015.239

NARAYANAN A. & SHMATIKOV V., *De-Anonymizing Social Networks*, in *Proc. 2009 30th IEEE Symp. On Security & Privacy 173*

NARAYANAN A. & SHMATIKOV V., *Myths and Fallacies of "Personally Identifiable Information"*, 53 Commc'n ACM 24, 26 (June 2010)

NARAYANAN A. & SHMATIKOV V., *Robust De-Anonymization of Large Sparse Datasets*, 2008 *IEEE Symp. on Sec. and Privacy* 111, Feb. 5, 2008

NARDONE A., TRIASSI M., *Profili organizzativi e giuridici della telemedicina nel quadro delle risorse tecnologiche in sanità*, in *Sanità pubblica e privata*, 2003, 27

NIGER S., *Il diritto alla protezione dei dati personali*, in J. MONDUCCI, G. SARTOR (eds.), *Il Codice in materia di protezione dei dati personali. Commento sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004

OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 *UCLA L. Rev.* 1701 (2010), available at <http://ssrn.com/abstract=1450006>

OHM P., *Sensitive Information*, 88 *S. Cal. L. Rev.* (forthcoming 2015)

ORTALI A., *Utilizzo dell'ICT (Information Communication Technology) in sanità*, *Rivista elettronica di Diritto, Economia, Management*, n. 3, 2014

PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano 2008

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002

PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003

PASCUZZI G., *Il diritto dell'era digitale*, II ed., Bologna, 2010

PASCUZZI G., IZZO U., MACILOTTI M. (eds.), *Comparative Issues in the Governance of Research Biobanks*, Springer 2013

PASQUALE F. & ADAMS RAGONE T., *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 *Stan. Tech. L. Rev.* 595 (2014)

PEIGNÉ V., *Il Fascicolo Sanitario Elettronico, Verso Una "Trasparenza Sanitaria" Della Persona – Electronic Health Records: Towards An "Health Transparency" Of The Individual*, 6 *Riv. It. Medicina Legale* 1519 (2011)

PEIGNÉ V., *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e divergenze*, in *Diritto dell'Internet*, 2008, 3, 296

PERRI P., *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Giuffrè, Milano, 2007

PIZZETTI F., *Sette anni di protezione dati in Italia: un bilancio e uno sguardo sul futuro*, Torino, Giappichelli, 2012

PLANK K.C., *Cloud Providers Often Are Business Associates Under HIPAA, Officials Say*, 22 *Health L. Rep.* (BNA) 858 (June 6, 2013)

POSTER M.J., *HIPAA Confusion: How the Privacy Rule Authorizes "Informal" Discovery*, 44 *University of Baltimore Law Review* 491 (2015)

POULLET Y., *The Directive 95/46/EC: Ten years after*, 22 *Computer Law & Security Report* 206 (2006)

PREITE G., *L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente*, 3 *Rivista Elettronica di Diritto, Economia, Management* 106 (2014)

REICHEL J. & LIND, A., *The New General Data Protection Regulation – Where Are We Are and Where Might We Be Heading?*, in D. MASCALZONI (ed.), *Ethics, Law and Governance of Biobanking. National, European and International Approaches*, Springer, 2015

RICHARDSON V., MILAM S. AND CHRYSLER D., *Is Sharing De-identified Data Legal? The State of Public Health Confidentiality Laws and Their Interplay with Statistical Disclosure Limitation Techniques*, *Journal of Law, Medicine & Ethics*, Spring 2015, 43 Suppl 1:83-6.

RIVKIN-HAAS E., *Electronic Medical Records and the Challenge to Privacy: How the United States and Canada Are Responding*, 34 *Hastings International & Comparative Law Review* 177 (2011)

ROACH W.H., *Medical Records and the Law*, Sudbury, 2008

RODOTÀ S., *Data Protection as a Fundamental Right*, in S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?*, Springer, 2009

RODOTÀ S., *Libertà, opportunità, democrazia, informazione, Relazione introduttiva al Convegno "Internet e privacy – quali regole?"*, May 8 1998

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 600

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normative: il nuovo codice sulla privacy, in Europa e diritto privato*, 2004

ROTH J., *The mHealth Conundrum: Smartphones & Mobile Medical Apps – How Much FDA Medical Device Regulation is Required?*, 15 *North Carolina Journal of Law & Technology* 359 (2014)

ROTHSTEIN M.A., *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, New Haven, 1997

ROTHSTEIN M.A., *HIPAA Privacy Rule 2.0*, *The Journal of Law, Medicine and Ethics* 41(2), 525 (2013)

RUBINSTEIN I.S. AND HARTZOG W., *Anonymization and Risk*, New York University School of Law, Public Law & Legal Theory Research Paper Series, Working Paper No. 15-36 (2015)

RYAN J., *The Uncertain Future: Privacy and Security in Cloud Computing*, 54 *Santa Clara L. Rev.* 497 (2014)

RYNNING E., *Public Trust and Privacy in Shared Electronic Health Records*, 14 *European Journal of Health Law* 105 (2007)

SALEEM T., *Implementation of HER/EPR in England: a model for developing countries*, in *Journal of Health Informatics in Developing Countries*, 2009 vol. 3, n. 1

SANTANIELLO G. (ed.), *La protezione dei dati personali*, in G. SANTANIELLO (ed.), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005, 131

SCHMIDT E. AND COHEN J., *The New Digital Age: Reshaping the Future of People, Nations and Business*, Knopf 2013

SCHULTE IN DEN BÄUMEN, T., PACI, D., IBARRETA, D., *Data Protection in Biobanks – A European challenge for the long-term sustainability of Biobanking*, in *Revista de Derecho y Genoma Humano*, 31, 2009

SCHWARTZ P., *Questioning the Quantitative Imperative: Decision Aids, Prevention, and the Ethics of Disclosure*, 41 *Hastings Ctr. Rep.* 30 (2011)

SCHWARTZ P., SOLOVE D., *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. Rev. 1814 (2011), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366>

SGRECCIA E., *Non archiviare l'impegno per l'umanizzazione della medicina*, *Medicina e Morale*, 1986, fasc. 2, 267-270

SHEFFNER D.J., State ex rel. Proctor v. Messina *and* Ex Parte *Communications Under the HIPAA Privacy Rule: The "Judicial Proceedings" Split*, 39 *Southern Illinois University Law Journal* 71 (2014)

SHIH A. ET AL., *Commonwealth Fund, Organizing the U.S. Health are Delivery System For High Performance* ix (2008)

SICA S., STANZIONE P. (eds.), *La nuova disciplina sulla privacy: commento al d.lgs. 30 giugno 2003, n. 196*, Bologna, 2004

SINHA A., *An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century*, in *Medical Anthropology Quarterly*, New Series, vol. 14, n. 3 (Sep. 2000)

SOLOVE D.J., *A Taxonomy of Privacy*, 154 *U. Pa. L. Rev.* 477 (2006)

SOLOVE D.J., *Privacy Self-Management and the Consent Dilemma*, 126 *Harv. L. Rev.* 1879 (2013)

SOLOVE D.J., ROTENBERG M. & SCHWARTZ P.M., *Information Privacy Law,* 2nd edition, Aspen 2006

SOMA J.T., RYNERSON S.D. & KITAEV E., *Privacy Law in a Nutshell*, 2nd edition, West Academic Publishing 2014

SOMAN A.K., *Cloud-based Solutions for Healthcare IT* (2011)

STACCINI P., DANIEL C., DART T., AND BOUHADDOU O., *Sharing Data and Medical Records*, in A. VENOT, A. BURGUN AND C. QUANTIN (EDS.), *Medical Informatics, e-Health. Fundamentals and Applications*, Springer 2014

STANBERRY B., *The legal and ethical aspects of telemedicine: data protection, security and European law*, 4 *Journal of Telemedicine and Telecare*, 18 (1998)

STEFANINI E., *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Cedam, Padova, 2008

STENBECK M. & ALLEBECK P., *Do the planned changes to European data protection threaten or facilitate important health research?*, *Eur. J. Public. Health* 2011, 21(6): 682-3

SUTER P., SUTER W.N., JOHNSTON D., *Theory-based telehealth and patient empowerment*, 14 *Popul. Health. Manag.* 87 (2011)

SWAN M., *Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen*, 2 *J. Personalized Med.* 93 (2012)

SWEENEY L., *Simple Demographics Often Identify People Uniquely* 2, Carnegie Mellon Univ., Working Paper No. 3, 2000.

SWEENEY L., *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, available at <http://dataprivacylab.org/projects/identifiability/paper1.pdf>

SWIRE P.P. & STEINFELD L.B., *Security and Privacy After September 11: The Health Care Example*, 86 *Minn. L. Rev.* 1515, 1526-27 (2002)

SZEREJKO J.D., *Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security*, 47 *Conn. L. Rev.* 1103 (2015)

TENE O. & POLONETSKY J., *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 *Nw.J. Tech. & Intell. Prop.* 239 (2013)

TENE O. & WOLF C., *Future of Privacy Forum – White Paper. The Definition of Personal Data: Seeing the Complete Spectrum* (2013), available at < http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-De-Id-January-201311.pdf>

TENE O., *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 *Ohio St. L.J.* 1217 (2013), available at < http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/17-Tene.pdf>

TERRY N.P. & FRANCIS L.P., *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 *U. Illinois Law Review* 681 (2007)

TERRY N.P., *A Medical Ghost in the E-Health Machine*, 14 *Health Matrix* 225-29 (2004)

TERRY N.P., *Certification and Meaningful Use: Reframing Adoption of Electronic Health Record as a Quality Imperative*, 8 *Ind. Health L. Rev.* 45 (2011)

TERRY N.P., *E-Health: Perspective and Promise*, 46 *St. Louis U. L.J.* 1 (2002)

TERRY N.P., *Electronic health records: International, structural and legal perspectives*, 12 *Journal of Legal Medicine* No. 1 (2004)

TERRY N.P., *What's Wrong With Health Privacy?*, 5 *J. Health & Biomedical L.* 1 (2009)

THE ECONOMIST, *Medicine goes digital. A special report on health care and technology*, April 18, 2009, available at <http://www.economist.com/sites/default/files/special-reports-pdfs/13447102.pdf>

THE ECONOMIST, *The Quantified Self: Counting Every Moment* (Mar. 3, 2012).

THOMPSON D. ET AL., *Reducing Clinical Costs with an EHR*, in 64 *Healthcare Financial Management*, 2010, 106

TOVINO S.A., *The Use and Disclosure of Protected Health Information For Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 *South Dakota Law Review* 447 (2004)

TURK M., *Electronic Health Records. How to Suture the Gap Between Privacy And Efficient Delivery of Healthcare*, 80 *Brook. L. Rev.* 565 (2015)

VARANI E., *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario. Dalla Carta dei diritti fondamentali dell'Unione Europea al decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 2005

WADHAM J., *Human Rights and Privacy – The Balance*, speech given at Cambridge (Mar. 2000), available at <http://www.liberty-human-rights.org.uk/mhrp6j.html>

WALKER J., BIEBER E.J., RICHARDS F. (eds.), *Implementing an electronic health record system*, New York, N.Y., 2006

WALLACE S. ET AL., *The legal and risk management conundrum of telemedicine, in 5 Journal of Telemedicine and Telecare*, 1999, 8

WHITE T.J. & HOFFMAN C.A., *The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 *W. Va. L. Rev.* 709 (2004)

WICKS E., *Electronic Health Records and Privacy Interests: The English Experience*, in C. GEORGE, D. WHITEHOUSE, P. DUQUENOY (eds.), *eHealth: Legal, Ethical and Governance Challenges*, Springer 2013

WILKES J.J., *The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care*, 2014 *BYU L. Rev.* 1213 (2015)

WRIGHT A., FEBLOWITZ J., SAMAL L., MCCOY A.B., SITTIG D.F., *The Medicare Electronic Health Record Incentive Program: Provider Perofrmance on Core and Menu Measures*, 49 *Health Services Research* 325 (2014)

WRIGHT A., HENKIN S., FEBLOWITZ J., MCCOY A.B., BATES D.W., SITTIG D.F., *Early Results of the Meaningful Use Program for Electronic Health Records*, in *New England Journal of Medicine*, 368, 8, 2013, 779

WU F. T., *Defining Privacy and Utility in Data Sets*, 84 *U. Colo. L. Rev.* 1117 (2013), available at <http://ssrn.com/abstract=2031808>

WU S., *A Guide to HIPAA Security and the Law*, Chicago, 2007

WU S., CHAUDHRY B., WANG J., MAGLIONE M., MOJICA W., ROTH E., *Systematic Review: Impact of Health Information Technology on Quality, Efficiency and Costs of Medical Care*, in *Annals of Internal Medicine*, 144, 10, 2006, 742

ZAMBRANO V., *Dati sanitari e tutela della sfera privata*, in *Dir. informazione e informatica*, 1999, 1

Other Sources

LEONARD COHEN, "*Anthem*" (song), *The Future*, Columbia 1992.

The Student Paper Series of the Trento Lawtech Research Group is published since Fall 2010

http://www.lawtech.jus.unitn.it/index.php/student-paper-series?start=1

Freely downloadable papers already published:

STUDENT PAPER N. 26

Big Data: Privacy and Intellectual Property in a Comparative Perspective

SARTORE, FEDERICO (2016) (a cura di Roberto Caso e Paolo Guarda), Big Data: Privacy and Intellectual Property in a Comparative Perspective, The Trento Law and Technology Research Group. Student Paper Series; 26. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-534-7

STUDENT PAPER N. 25

Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course

REMO ANDREOLLI, DALILA MACCIONI, ALBERTO MANTOVANI, CHIARA MARCHETTO, MARIASOLE MASCHIO, GIULIA MASSIMO, ALICE MATTEOTTI, MICHELE MAZZETTI, PIERA MIGNEMI, CHIARA MILANESE, GIACOMO MINGARDO, ANNA LAURA MOGETTA, AMEDEO MONTI, SARA MORANDI, BENEDETTA MUNARI, EDOARDO NADALINI, SERENA NANNI, VANIA ODORIZZI, ANTONIA PALOMBELLA, EMANUELE PASTORINO, JULIA PAU, TOMMASO PEDRAZZANI, PATRIZIA PEDRETTI, VERA PERRICONE, BEATRICE PEVARELLO, LARA PIASERE, MARTA PILOTTO, MARCO POLI, ANNA POLITO, CARLO ALBERTO PULEJO, SILVIA RICCAMBONI, ROBERTA RICCHIUTI, LORENZO RICCO, ELEONORA RIGHI, FRANCESCA RIGO, CHIARA ROMANO, ANTONIO ROSSI, ELEONORA ROTOLA, ALESSANDRO RUFFINI, DENISE

SACCO, GIULIA SAKEZI, CHIARA SALATI, MATTEO SANTOMAURO, SILVIA SARTORI, ANGELA SETTE, BIANCA STELZER, GIORGIA TRENTINI, SILVIA TROVATO, GIULIA URBANIS, MARIA CRISTINA URBANO, NICOL VECCARO, VERONICA VILLOTTI, GIULIA VISENTINI, LETIZIA ZAVATTI, ELENA ZUCCHI (2016) Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course. The Trento Law and Technology Research Group. Student Paper Series; 25. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 24

La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability

CAERAN, MIRCO (2016) La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability. The Trento Law and Technology Research Group. Student Paper Series; 24. Trento: Università degli Studi di Trento. ISBN 978-88-8443-663-4

STUDENT PAPER N. 23

La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities

CHIARUTTINI, MARIA OTTAVIA (2015) La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities. The Trento Law and Technology Research Group. Student Paper Series; 23. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 22

Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio = Technology Transfer and Regional Context: Old Problems and New Perspectives for a Sustainable Co-operation among Universitiy, Entrepreneurship and Local Economy

CALGARO, GIOVANNI (2013) Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio. The Trento Law and Technology Research Group. Student Paper Series; 22. Trento: Università degli Studi di Trento. ISBN 978-88-8443-525-5

STUDENT PAPER N. 21

La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata = Internet Service Provider liability and copyright infringement: a comparative analysis.

Imperadori, Rossella (2014) *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata.* Trento Law and Technology Research Group. Student Paper; 21 . Trento : Università degli Studi di Trento. ISBN 978-88-8443-572-9

STUDENT PAPER N. 20

Open innovation e patent: un'analisi comparata = Open innovation and patent: a comparative analysis

Ponti, Stefania (2014) *Open innovation e patent: un'analisi comparata.* The Trento Law and Technology Research Group. Student Paper Series; 20 . Trento : Università degli Studi di Trento. ISBN 978-88-8443-573-6

STUDENT PAPER N. 19

La responsabilità civile nell'attività sciistica

CAPPA, MARISA (2014) La responsabilità civile nell'attività sciistica = Ski accidents and civil liability. Trento Law and Technology Research Group. Student Paper Series, 19. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 18

Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM

TEBANO, GIANLUIGI (2014) Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM = Agricultural Biodiversity and the Protection of Farmers from patent Hold-Up: the case of GMOs.Trento Law and Technology Research Group. Student Paper Series; 18. Trento : Università degli Studi di Trento.

STUDENT PAPER N. 17

Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici

MAFFEI, STEPHANIE (2013) Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici = Producing and Eating "Bio": A Comparative Analisys of the Law of Organic Food. Trento Law and Technology Research Group. Student Paper Series; 17. Trento : Università degli Studi di Trento.

STUDENT PAPER N. 16

La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata = The Protection of Geographical Indications in the Wine Sector: A Comparative Analisys

SIMONI, CHIARA (2013) La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata. The Trento Law and Technology Research Group. Student Papers Series; 16. Trento: Università degli Studi di Trento. Facoltà di Giurisprudenza.
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/ 142

STUDENT PAPER N. 15

Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano

SALVADORI, IVAN (2013) Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano. Trento Law and Technology Research Group. Student Paper; 15. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 14

Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare

VIZZIELLO, VIVIANA (2013) Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare. Trento Law and Technology Research Group. Student Paper; 14. Trento: Università degli Studi di Trento.

STUDENT PAPER N.13

The Intellectual Property and Open Source Approaches to Biological Material

CARVALHO, ALEXANDRA (2013) The Intellectual Property and Open Source Approaches to Biological Material. Trento Law and Technology Research Group. Student Paper Series; 13. Trento: Università degli Studi di Trento.

STUDENT PAPER N.12

Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930)

TRESTINI, SILVIA (2012) Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930) = For an Archeology of Food Law: 54 Years of Case Law Collections Concerning the Safety and Quality of Food (1876-1930). The Trento Law and Technology Research Group. Student Papers Series, 12.
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
143

STUDENT PAPER N.11

Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo

PICCIN, CHIARA (2012) Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo = From the Alps to the Pyrenees: Comparative Analysis of Civil Liability for Mountain Sport Activities in Italian and Spanish Law. The Trento Law and Technology Research Group. Student Papers Series, 11

STUDENT PAPER N.10

Copynorms: Norme Sociali e Diritto d'Autore

PERRI, THOMAS (2012) Copynorms: Norme Sociali e Diritto d'Autore = Copynorms: Social Norms and Copyright. Trento Law and Technology Research Group. Students Paper Series, 10

STUDENT PAPER N. 9

L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco

ALESSANDRA ZUCCATO (2012), L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco = Exporting Wines to the United States: Rules and Contractual Practices with Specific Reference to the Case of ProseccoTrento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 9)

STUDENT PAPER N.8

Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis.

RUGGERO, BROGI (2011) Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis. Trento: Università degli Studi di Trento (TrentoLawand Technology Research Group. Student Papers Series, 8)
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
144

STUDENT PAPER N.7

Evoluzione tecnologica e mutamento del concetto di plagio nella musica

TREVISA, ANDREA (2012) Evoluzione tecnologica e mutamento del concetto di plagio nella musica = Technological evolution and change of the notion of plagiarism in music Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 7)

STUDENT PAPER N.6

Il trasferimento tecnologico università-imprese: profili giuridici ed economici

SIRAGNA, SARA (2011) Il trasferimento tecnologico università-imprese: profili giuridici ed economici = University-Enterprises Technological Transfer: Legal and Economic issues Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 6)

STUDENT PAPER N.5

Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese

GUERRINI, SUSANNA (2011) Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese = Mediation & Medical Liability: The Italian "General Approach" Compared to the Specialized Model Applied in FranceTrento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 5)

STUDENT PAPER N.4

"Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia

PODETTI, MASSIMILIANO (2011) "Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia = Gun Control and Tort Liability: A Comparison between the U.S. and Italy Trento: Università degli Studi di Trento. (Trento Law and Technology Research Group. Students Paper Series 4)
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/ 145

STUDENT PAPER N.3

Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti

TOGNI, ENRICO (2011) Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti = Smart Foods and Dietary Supplements: Regulatory and Civil Liability Issues in a Comparison between Europe and United States Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 3)

STUDENT PAPER N.2

Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia

SARTOR, MARTA (2010) Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia = The Role of Tort Law within the Family: A Comparison between Italy and France Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students
Paper Series; 2)

STUDENT PAPER N.1

Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito

RIZZETTO, FEDERICO (2010) Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito = War Technologies and Home Soldiers Injuries: The Role of Tort Law in a Comparison between the American "Agent Orange" and the Italian "Depleted Uranium" Litigations Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 1)