Trento Law and Technology Research Group

Research Paper n. 23

Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context

Paolo Guarda | July/2015

ISBN: 978-88-8443-627-6

ABSTRACT

This article is aimed at describing the most relevant issues around computerised processing of health data with specific reference to telemedicine modules within the European Union. The regulatory framework in this area is complex and varied, and often disorienting. Therefore, the application and reconstructive approach of this work tries to fill a gap in the literature by providing a first systematisation of the topic. The main issues of the digitisation of health data are taken into account, with particular attention to telemedicine and so-called patient empowerment. There is a specific focus on the analysis of the application scenarios and legal requirements, in terms of privacy and security, of a telemedicine service. The European legal framework, and specifically the legal frameworks of certain selected countries (Germany, France, Austria and Italy), is presented. Ultimately, the minimum requirements to be implemented in a telemedicine scenario, along with possible technical solutions compliant with these requirements, are discussed and presented.

CONTENTS

KEYWORDS

Data Protection – Privacy – Security –E-health - Telemedicine

ABOUT THE AUTHOR

Paolo Guarda (email: paolo.guarda@unitn.it - Personal Web Page: http://www.lawtech.jus.unitn.it/index.php/people/paolo-guarda), PhD in Comparative Private Law, is Post-doc Researcher of Private and Comparative Private Law at the University of Trento (Italy) – Faculty of Law – The Trento Law and Technology Research Group. He teaches "Information Technologies Law" and "Comparative ICT Law" and is the author of several articles about issues related to Digital Age Law (Privacy, Copyright, Technology Transfer, etc.).

Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context*

Paolo Guarda

1. Introduction

E-health is a major innovation that can improve healthcare and strengthen the quality and effectiveness of the services offered. It could guarantee substantial productivity gains and in the future will allow the construction of advanced citizen-centred health systems.

For several decades, the European Union has been promoting research programmes on the subject. Numerous results of these efforts have already been tested and put into practice.[1]

* Research fellow at the Faculty of Law – University of Trento and lecturer in Information Technologies Law (paolo.guarda@unitn.it). I acknowledge my debt to the Trento Unit of the project 'NATHCARE' (Networking Alpine Health for Continuity of Care), co-funded by the 'Alpine Space Programme 2007-2013' (www.nathcareproject.eu): the Autonomous Province of Trento (project partner) and its collaborator, Bruno Kessler Foundation (FBK); in particular I would like to thank Giandomenico Nollo, Michela Dalmartello and Claudio Eccher. I would like also to thank Dr. Rossana Ducato for her support and valuable feedback. All errors remain my own.

[1] See, for example, the epSOS project (Smart Open Services for European Patients), focusing on the interoperability of electronic health records (www.epsos.eu). See also the already mentioned NATHCARE Project aimed at designing, consolidating and validating a 'local healthcare community'-based model embracing all players in the care system with the aim of securing a sustainable and improved organisational adaptation of healthcare services. Furthermore, e-health is one of the pillars of the Digital Agenda within the

Therefore, Europe plays a fundamental role in the use of digital technologies for the purpose of basic healthcare. This phenomenon reflects a global trend, as health systems have to deal with the new challenges of a supranational scope.[2]

First of all, there is a growing demand for health and social services, as determined by a progressive aging of the world population - especially in Western countries - and by higher income and educational levels than in the past, which changes the approach, even cognitive, of citizen-users to health service (this issue represents a crucial point for a telemedicine project). Then, we may register a significant evolution of the demand itself. Technological 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). Furthermore, the evolution of the supply system is characterised by the difficulty for public authorities to match investment in technology with investment for the construction of complex organisational reforms and for the need to

---

strategy 'Europe2020' (http://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century).

[2] See Luca Buccoliero, Claudio Caccia, Greta Nasi, e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità (McGraw-Hill, Milano 2005) 1-3; Paolo Guarda, Fascicolo sanitario elettronico e protezione dei dati personali (Università di Trento, Trento 2011) 9-12 (also available at: http://eprints.biblio.unitn.it/archive/00002212/).

provide the best possible medical care on a limited budget. Finally, the increasing mobility of patients and staff is pushing users and medical professionals to move on a national and international level, giving rise to a sort of 'hospital shopping'.

From this point of view, the computerisation of the health service is seen as a kind of useful recipe to raise the level of services on the one hand, and to lower the cost of the system on the other. The significant technological advances in telecommunications, IT and biomedical and diagnostic technologies in the health sector have resulted in a positive interaction among these fields of human (and technological) knowledge. Information and Communication Technology (ICT) innovation brought indeed, on the one hand, a significant improvement in terms of time saving, service quality and health benefits, and, on the other, a more efficient use of resources.[3]

This essay is aimed at analysing the problems arising due to the complex and varied, and often, disorienting regulatory framework. Thus, the proposed application-reconstructive work is fundamental and fills a gap in the literature by providing a first systematisation of the issue.

---

[3] For further analysis see Basit Chaudhry and others, 'Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care' (2006) 144 Ann Intern Med 742; Doug Thompson and others, 'Reducing Clinical Costs with an EHR' (2010) 64 Healthcare Financial Management, 64, 10, 2010, 106; M.B. Buntin, and others, 'The Benefits Of Health Information Technology: A Review Of The Recent Literature Shows Predominantly Positive Results' (2011) 30 Health Affairs 464; L.A. Flier, 'Health Information Technology in the Era of Care Delivery Reform. To What End?' (2012) 307 JAMA: The Journal of the American Medical Association 2593.

Following this introduction, a first section will be devoted to outlining the different phenomena with particular reference to the digitisation of health data, telemedicine and, above all, so-called Patient empowerment (par. 2). Then, a specific part will be focused on the analysis of the application scenario and the legal requirements of reference, in terms of privacy and security, that a telemedicine service should implement. The European legal framework, and specifically the legal frameworks of certain selected countries, will be presented: Germany, France, Austria and Italy (par. 3). These countries were selected since they represent a sufficient overview of regulations designed to implement the rules of privacy in the context of telemedicine in Europe. The analysis will represent a useful test, at least with reference to the security rules to adopt. We will explore the issue with an in-depth analysis of the Italian legal framework, which could be considered a paradigmatic model from the practical and implementation point of view: e-health projects have already started to be sufficiently developed and many legal requirements have already been tested. Finally, the minimum requirements for implementing such a scenario (par. 4), along with possible technical solutions compliant with these requirements, will be presented.

2. Patient empowerment, digitisation of health data, and telemedicine

2.1 Premise

A crucial issue in the e-health sector is the new role of the patient. As in all areas of human life where the introduction of digital technologies ensures the emergence of new types of social relations, in the health sector, too, the patient is required to acquire a certain level of literacy to be able to participate proactively in the choices relating to the care processes affecting her. The challenge here is how to give expression to this need, coordinating and incorporating within a digital infrastructure those legal principles that in the physical context are intended to ensure citizens' security and freedom.[4]

Thus, the patient is interested in a more careful monitoring of personal data concerning her and circulating through communication networks. The advent of digital technologies led to the growth in the importance given to the citizen/patient within the information society. The e-health platforms are a perfect example of

[4] For further analysis see, among others, J.P. Tarte, C.C. Bogiages, 'Patient centered care delivery and the role of information systems' (1992) 13 Comput. Health 44; Douglas S. Wakefield and others, 'Understanding patient-centered care in the context of total quality management and continuous quality improvement' (1994) 20 Jt Comm J Qual Improv 152; Nancy Calabretta, 'Consumer-driven, patient-centered healthcare in the age of electronic information' (2002) 90 J. Med Libr Assoc 32; Karen Davis, Stephen C. Schoenbaum, Anne-Marie Audet, 'A 2020 Vision of Patient-Centered Primary Care' (2005) 20 Journal of General Internal Medicine 953.

this tendency that leads to conceiving the entire infrastructure not around the data controllers/managers, but around the interests expressed by the individual/patient. On this line of argument, the principle of self-determination is no more than the legal manifestation of these needs.

Taking into account a digital infrastructure that is able to process health data within our specific scenario, all the above considerations mean that the choices of what information to enter into the system, the levels of sharing and the various techniques for hiding information are managed directly by the patient through the instrument of consent, which, in an increasingly modular and complex way, carries out the will of the user within the information technology (IT) infrastructure. Thus, in addition to the needs of healthcare professionals to access patient data to carry out the care process, there is a clear interest on the part of the individual to finally have a voice in the care process, and to acquire a direct role as 'manager' of the database that contains her health information, with truly innovative powers of access and modification compared to traditional ones.

To complete the overview, a critical aspect of these new systems must be mentioned: the risk that this innovation trigger a process of dehumanisation of the patient-physician relationship. This social relation has been built over the centuries according to a ritualised structure, which is expressed in a range of behaviours where doctor and patient interact in a social pattern that leads them

to share information, knowledge, problems and concerns. The patient, in the real world, physically goes in front of her physician to externalise her symptoms, looking for a cure for the ills that afflict her. The physician receives this 'outburst' and, in light of the information gathered and her own knowledge, shall carry out the correct process of diagnosis and treatment, according to dynamics as old as medicine itself.[5] 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. The trust between doctor and patient is built on the basis of a mutual exchange of information, which is the background of effective knowledge sharing between the two parties, regardless of the medium used, whether or not paper documents are used or files are transmitted online. The question again is 'cultural'. It is even more necessary that the implementation of these new digital systems correspond to an adequate computer literacy, for both healthcare operators and users. The greatest damage occurs, in fact, when one someone does not have adequate knowledge of the tool they are using. The effective work to provide information to patients/users and to train healthcare providers about new services, will be used to facilitate new forms of collaboration. These will be

[5] As affirmed in Guarda (fn 2) 120-2. See also Byron J. Good, Medicine, Rationality and Experience: An Anthropological Perspective (Cambridge University Press, Cambridge 1994); Jan Howards, Anselm Strauss, Humanizing Healthcare (New York, 1997); Arushi Sinha, 'An Overview of Telemedicine: The Virtual Gaze of Healthcare in the Next Century' (2000) 14 Medical Anthropology Quarterly 291-309 (also available at: http://www.jstor.org/stable/649500).

different from those resulting from human (physical) relations, which are very often subject to behavioural patterns crystallised from habits[6].

2.2 European Union regulatory framework

European legislators - with Directives 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector)[7] – have set the main rules regarding personal data processing within the European Union[8]. Devoting some *ad hoc* rules to the problem of health data,

[6] Before the digital age, health data processing was not such a problematic issue. It was based on a strictly fiduciary relationship between the patient (rectius: data subject) and the physician, who in most cases was the 'General Practitioner (GP)'. Everything was then recorded on paper, or simply spoken. The advent and widespread diffusion of computers has led to an upsurge of new problems and demand for protection. Digital technology has provided the extraordinary ability to access large amounts of aggregated data very quickly; on the other hand, it has also made possible the creation of big databases to which more and more people – even though limited in number and specifically identified - may have access. This has greatly increased the risks associated with the treatment of these data, their unlawful circulation and dissemination, and the capability to affect the dignity and the fundamental freedoms and rights of the individual data subject. See E. Topol, The Creative Destruction of Medicine. How the Digital Revolution Will Create Better Healthcare (Basic Books, New York 2012); Umberto Izzo, 'Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina (2000) Danno e resp. 807; Sinha (fn 5).

[7] As amended by Directive 2009/136/EC.

[8] With reference to European data protection law, see Horwitz J. Morton, 'Data Protection and Privacy' (1996) 18 EIPR 558; Lee A. Bygrave, Data Protection Law. Approaching Its Rationale, Logic and Limits (Kluwer Law International,

the EU highlighted the specificity and the dangers that the operations relating to this particular category of data may show. These directives have been adopted within the national legal systems.

Regarding the specific area of digitised health data management, we have to refer also to several international documents that are pushing the implementation of EHR. Above all, we must cite the 'Working Document on the processing of personal data relating to health in electronic health records (EHR)', adopted on 15 February 2007 by Article 29 Data Protection Working Party (hereinafter: Working Document). This document aims to provide guidance on the interpretation of the applicable legal framework of data protection for EHR systems and to establish some general principles. It also aims at setting out the data protection preconditions for establishing a nationwide EHR system, as well as the applicable safeguards.[9] This kind of infrastructure raises many critical issues in relation to the legislation on the protection of personal data, which have been managed by national legislators and

---

The Hague – London - New York 2002); Paolo Guarda, 'Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks' (2008) Ciberspazio e dir 65 (also available at: http://eprints.biblio.unitn.it/archive/00001524/); Ian J. Lloyd, Information technology law (Oxford University Press, Oxford 2008) 1 ff.

[9] A definition of this new instrument has been proposed by the already mentioned Working Group: 'A comprehensive medical record 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'.

Data Protection Authorities.[10]

Coming back to the main issue of this essay, it is worth mentioning that in dealing with these evolving phenomena - causing deep structural and organisational changes in the healthcare system - national governments and regional authorities have created strategic plans in order to manage the transition and to encourage the spread of ICT within the medical field. But first of all the European Union has played its part by financing similar projects.

Referring only to the last decade, on 22 September 2002, a 'Community action programme in the field of public health (2003-2008)' was approved by Decision no. 1786/2002/EC of the European Parliament and of the Council. This programme, in addition to the traditional objectives focused on information and knowledge of healthcare, on the ability of rapid and coordinated intervention by the European Union, and on disease prevention, provided for the possibility of using ICT in order to enhance the

[10] For instance, the Italian Data Protection Authority (Garante per la protezione dei dati personali) intervened by enacting some guidelines on the implementation of an EHR system by a General Provision ('Guidelines on the Electronic Health Record and the Health File – 16 July 2009', hereinafter: GL EHR). The Data Protection Authority intervened again on a related aspect concerning, in particular, the activity of online examination records: 'Guidelines on Online Examination Records - 19 November 2009', hereinafter: GL Records). Also the inter-institutional working group on EHR, involving, under the coordination of the Ministry of Health, internal and external experts of the Ministry, as well as representatives of the regions designated and other institutional actors, has developed a reference model whose final results have been described in the 'Guidelines on electronic health records' approved by the State-Regions Conference on 10 February 2011 (see http://www.salute.gov.it/imgs/C_17_pubblicazioni_1465_allegato.pdf) .

quality of healthcare across Europe. In 2004 the European Commission adopted a plan, called 'eHealth Action Plan 2004', where the adoption of ICT in the healthcare sector was aimed at keeping costs stable or lower, shortening waiting times and decreasing margins of error. Furthermore, one of the three pillars of the 'i2010 - A European Information Society for growth and employment' is the promotion of 'inclusion, improvement of public services and quality of life' through ICT[11]. Without making any pretense at completeness, it is worth mentioning a series of recommendations and communications of the European Commission aimed at promoting the implementation and development of e-health: the 'White Paper' of the Commission 'Together for Health: A Strategic Approach for the EU 2008-2013', Brussels, 23 October 2007; the Commission Recommendation of 2 July 2008, on border interoperability of electronic health records (COM (2008) 3282); the Communication of the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions of 4 November 2008 on telemedicine for the benefit of patients, healthcare systems and society (COM (2008) 689). Finally, we should at least mention the epSOS (Smart Open Services for European Patients) project, which was launched in July 2008 and aimed at achieving an electronic exchange of health data at a

[11] See the Web site: http://ec.europa.eu/ health-eu/index_it.htm. See also eHealth Task Force Report, 'Redesigning health in Europe for 2020' (2012) http://www.president.ee/images/stories/pdf/ehtf-report2012.pdf.

European level, in compliance with the regulatory framework and existing information systems in the countries participating in the initiative.[12]

Lastly, the European Commission's eHealth Action Plan 2012-2020 provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research on personalised medicine of the future. This means providing smarter, safer and patient-centred health services. Given the fast growing uptake of tablets and smartphones, the Action Plan also includes a special focus on mobile health (mHealth).[13] The eHealth Action Plan is a communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.[14]

Finally, it is worth mentioning Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. It makes provisions aimed at clarifying patients' rights with regard to accessing cross-border healthcare services; guaranteeing the safety,

---

[12] See http://www.epsos.eu/epsos-home.html.

[13] A Green Paper on Mobile Health (mHealth) was published by the European Commission on 10 April 2014. The objective of this Paper is to launch a broad stakeholder consultation on existing barriers and issues related to mHealth deployment and help identify the right way forward to unlock the mHealth potential. The consultation was open from 10 April to 3 July 2014 (available at: http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth).

[14] See http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=1252.

quality and efficiency of care that they will receive in another EU Member State; promoting cooperation between Member States on healthcare matters.[15]

In order to support a systematic use of telemedicine, the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions enacted a Communication on telemedicine for the benefit of patients, healthcare systems and society (COM (2008) 689). This Communication had a direct impact within

[15] The same happened at the national level. For instance, with regard to the Italian context, the system of e-health is characterised by a national strategic framework and several important interventions at a local level. We need to quote the previous 'National Health Plan 2003-2005', by which the Italian Government identified the overall goals of health for Italy, in the light of changes in the national political and social scenario. Therefore, in October 2004, the Presidency of the Council of Ministers activated an organisational tool called 'Tavolo di lavoro permanente per la sanità elettronica' in order to coordinate and support the implementation of the National Health Plan. At the local level, for some years the health system of the Autonomous Province of Trento has been developing an integrated model of innovation and development involving the expansion and integration of existing information services, the development of projects in the field of telemedicine and homecare, the reorganisation of organisational and managerial processes, and the rethinking and reorganisation of production and management of 'health documents'. 'TREC – Cartella Clinica del Cittadino' addresses these principles (see https://trec.trentinosalute.net/). It aims at promoting a platform of e-care and supporting citizens in the management of their health and care, as well as the social and health institutions in supplying new service models. The TREC platform offers an innovative approach, whereby the patient plays an integral part in the management system of information. According to this view, every interaction of the patient with the new system for managing health records may imply the creation of new data, which are stored on an infrastructure designed and managed by the Provincial Healthcare Provider (this results in the creation of a so-called Personal Health Record (PHR)).

on a national level.[16]

In conclusion to this introductory paragraph, it is useful to try to provide the reader with possible definitions of the more general phenomenon examined in this paper. Thus, telemedicine may be defined as:

> 'The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities' (WHO, 1997-1998).

The European Commission provides its own version instead:

> 'The provision of healthcare services, through the use of ICT,

[16] For instance, in order to implement its provisions, a special technical table on telemedicine was established in Italy at the 'Consiglio Superiore di Sanità' on 24 February 2011. The scope of the table was to provide appropriate national guidelines, aimed at outlining a policy framework for prioritising areas for the application of telemedicine, analysing models, processes and methods of integration of telemedicine services in clinical practice, defining taxonomies and classifications, as well as aspects of the legal and regulatory profiles and economic sustainability of the services and benefits of telemedicine. The aforementioned technical board completed its work on 10 July 2012, and the 'Consiglio Superiore di Sanità' has since approved the 'National Guidelines on Telemedicine'. The document, the Permanent Conference for relations between the State, regions, autonomous provinces of Trento and Bolzano approved by the State on the 20 February 2014, has provided guidelines for the definition of common technical-organisational measures to support the development of telemedicine at a national level.

> in situations where the health professional and the patient (or two health professionals) are not in the same location. It involves secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients' (EU Commission, 2008).

Telemedicine is not an alternative treatment that replaces the traditional doctor-patient relationship. Rather it is a tool that is complementary to it, enhancing the delivery of health services and reducing inherent limitations, primarily due to distance.[17]

2.2.1 Notes on future EU privacy regulations

The EU scenario on privacy is under review. On 25th January 2012 the European Commission presented a package of proposals for the modernisation of the European data protection framework, consisting of: a Communication outlining the strategy of the reform, a Regulation intended to replace Directive

[17] It is now worth at least mentioning the possible use of cloud computing in the healthcare sector. The adoption of cloud technologies helps reduce the fixed costs of purchasing computer tools (hardware and software), as well as the costs of maintenance and upgrade, allowing for direct investment only for obtaining a desired service, and in a flexible manner and only when needed. We must think about the cloud not only for archiving or storage of health data, but also for the use of powerful healthcare applications within the cloud (for example for EHR management) or for the development of these applications on special platforms in the cloud (see 'Opinion 05/2012 on Cloud Computing', adopted on 1 July 2012, by the Article 29 Data Protection Working Party). These kinds of scenario will raise several critical issues related to privacy and security of the processing of personal and health data.

95/46/EC, and a Directive to take the place of the Framework Decision 2008/977/GAI on the protection of data processed in the framework of police and judicial cooperation in criminal matters.[18] Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 28 EU Member States have implemented the 1995 rules in different ways, resulting in divergences in their enforcement. The initiative will help to reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.[19]

We do not know precisely when this regulatory intervention will come into force. The debate on the text seems to be very much alive. Here is a by no means exhaustive list of the major changes in the proposed regulation:

- the fundamental definitions will remain in force, but with some significant additions (for instance, genetic data, health data, biometric data);
- EU law will also apply to the processing of personal data carried out outside the EU, whether relating to supply of

[18] See the http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[19] On the proposed General Data Protection Regulation, see Paul de Hert, Vagelis Papakonstantinou, 'The proposed data protection regulation replacing directive 95/46/ec: a sound system for the protection of individuals' (2012) 28 Computer law & security review 130; Francoise Gilbert, 'Proposed EU Data Protection Regulation: the Good, the Bad and the Unknown (2012) 15 Journal of Internet Law 1.

goods or services to EU citizens or such as to allow monitoring of the behaviour of EU citizens;

- the right of data subject to 'data portability' will be established (eg in case you wish to transfer your data from one social network to another), but also the 'right to be forgotten', ie to decide which information may continue to circulate (especially online) after a certain period of time, under certain circumstances (for example, to comply with legal obligations, to ensure the exercise of freedom of expression, to allow historical research);
- the obligation for holders to notify of the processing of personal data will be removed and replaced by that of appointing a 'data protection officer' (in charge of data protection, according to the terminology of Directive 95 /46) for all public entities and for private ones with more than a certain number of employees;
- the concept of 'privacy impact assessment' would be introduced in addition to the general principle of 'privacy by design' (ie the provision of measures to protect data already at the design stage of a product or a software);
- an obligation will be introduced for all data controllers to notify the competent authority of any violations of personal data ('personal data breaches');

- more specifically powers (including sanctions) and the independence requirements of the national data protection authorities will be established; the opinion of these authorities will be essential if one intends to adopt regulatory instruments, including laws, which could affect the protection of personal data.

2.*3 Developing a telemedicine application*

Telemedicine applications usually start as experimental research projects to test a new model of care, based on the collaboration of healthcare professionals supported by digital technology, in which patients could assume a pivotal role. In the long term, these e-health projects should be able to exceed the threshold of experimentation, since, as a product that might be adopted in a stable and lasting way in a real national social-health service with concrete features, rules and limits, it has to respect the same rules. The e-health application will be even more appreciated if it will be able to fit into the existing framework and communicate with the systems already in use. This process requires time and should be approached with care and caution, given the technical difficulties and, in particular, the legal risks in implementing solutions that do not address high security standards of patient privacy.

The in-depth knowledge of the processes that you intend to

computerise is an essential factor in this development. ICT applications should not, in fact, simply 'replicate' in a non-paper context a mere copy of existing ones; but rather, in order to allow them to maximise their potential, it is desirable firstly to 'rethink' the process that you intend to apply, trying to improve it as far as possible. For this reason, the description of the care process you are going follow using digital technologies becomes crucial in building the technical and legal architectures.

In this context, it is therefore desirable to approach the solution to the problem with techniques that can correctly map existing ones and allow for a more effective system to be designed. The so called 'Business Process Reengineering' (BPR), for example, is a technique that involves studying the process that one wishes to innovate.[20] The BPR technique is divided into three phases: the first one, in which one defines the scope of the intervention; the second one, in which one surveys the processes and diagnosis of the ways in which the activities are carried out, taking into account the current state (so-called *as-is*); and a third phase of redesign. The main purpose of this analysis is to understand in detail how a task is actually performed at a given time, who carries it out, what are the internal relations among agents, and which organisation supports the activity.

All these considerations are quite important when you

[20] See Michael Hammer, The reengineering Revolution (Harper Collins, New York 1995).

approach the problem from the point of view of privacy, and you try to structure the information flows correctly.[21]

The compliance with European and national data protection regulation while designing and implementing an e-health system is no trivial matter. Building up a telemedicine system, in all its aspects (medical, technological, ethical, economic), implementing it in its hardware and software components, checking the results from the medical point of view, and only then asking whether it is in accordance with privacy regulations is an error that must be avoided. The same European regulation on data protection will introduce the new concepts of 'privacy by design' and 'privacy impact assessment', which will mean that those who create a product or software must necessarily design them together with the security measures that should be applied, and then with full knowledge of the potential hazards and risks, which must be addressed or, preferably, avoided from the start. Hence the importance of structuring immediately the e-health platform in a manner consistent with the principles of the privacy laws in force in a given legal system.

A further element of difficulty in this context is the fact that the regulatory framework in the field of e-health is inherently dynamic and therefore subject to periodic and ongoing

[21] A platform should be already outlined in its fundamental elements before being built. After the pilot test phase, you should be able to improve the care process itself, which, in the digitisation phase, may have shown some critical aspects and/or weaknesses.

additions/modifications by the various Legislators.[22]

3. European and National Legal Frameworks with reference to Privacy and Security Issues: an Overview

3.1 The European Union legal framework

As we pointed out previously, the legal framework on privacy and security issues relating to EU data protection is essentially represented by Directive 95/46/EC and Directive 2002/58/EC. These acts established the main rules in relation to personal data processing.

Data protection discipline in the EU lays down the main rules on how data processing shall be performed. We can summarise privacy principles as follows:

- *Fair and Lawful Processing*: the collection and processing of personal data shall neither unreasonably intrude upon the data subjects' privacy nor unreasonably interfere with their autonomy and integrity, and shall be compliant with the overall legal framework.

[22] To confirm this, the European Commission has launched a call for tender (n° EAHC/2013/Health/06) with the overall objective of preparing an overview of the national laws on Electronic Health Records in EU Member States and their interaction with the provision of cross-border eHealth services of Article 11 and Article 14 of Directive 2011/24/EU. The deadline to submit tenders was 7 June 2013. See http://ec.europa.eu/eahc/health/tenders_H06_2013.html.

- *Consent*: personal data shall be collected and processed only if the data subjects have given their explicit consent to data processing.
- *Specification of Purpose*: personal data shall be collected for specified, lawful and legitimate purposes and not processed in ways that are incompatible with the purposes for which the data have been collected.
- *Minimality*: the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
- *Minimal Disclosure*: the disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.
- *Information Quality:* personal data shall be accurate, relevant, and complete with respect to the purposes for which they are collected and processed.
- *Data Subject Control:* the data subject shall be able to check and influence the processing of his/her personal data.
- *Sensitivity:* the processing of personal data, which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data.

- *Information Security:* personal data shall be processed in a way that guarantees a level of security appropriate to the risks presented by the processing and the nature of the data.

Within this context, security issues are essential with respect to the processing of personal data and, in particular, medical data. The security requirements embody the substantive protection of the person concerned. The safety of treatments carried out by electronic means is essentially based on the following requirements: limited access, traceability and audit system, unintelligible data (and anonymity when possible).

In relation to that, at the EU level the main reference is art. 17 Directive 95/46/EC:[23]

> '1. Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

[23] See also art. 4 of the Directive 2002/58/EC, and art. 30 of the proposal of the General Data Protection Regulation.

2. The Member States shall provide that the controller must, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures (...).'

Several Member States have included these principles in their national laws.

3.2 A comparative survey

In the following pages we propose a by no means exhaustive series of informative paragraphs with reference to the regulation of a few major European countries: Germany, France, Austria and Italy.[24] More space and in-depth analysis will be devoted to the Italian legal system since the Italian transposition of the rules established at the European level could be presented as paradigmatic and restrictive one.[25]

3.2.1 Germany

The general legal framework is contained in the Federal

[24] The content of the comparative paragraphs is taken up, adapted and reformulated by the Deliverable drafted within the research activity carried out in the abovementioned 'Legal framework for NATHCARE Project' (2014).

[25] See, for example, the omission of the parameter of implementation costs of the security measures, provided by art. 17 of Directive 95/46/EC, and absent, instead, in the Italian Data Protection Code.

Data Protection Act (BDSG, Bundesdatenschutzgesetz).[26] Some specific definition refinements as well as organisational and implementation regulations for public authorities are included in several data protection acts of each State (regarding Bavaria, for instance: BayDSG, Bayerisches Datenschutzgesetz). Some States have dedicated an *ad hoc* regulation to healthcare providers (GDSG NRW, Gesundheitsdatenschutzgesetz NRW). Some other States rely on federal law and additionally provide sections in their hospital functioning acts (for example in Bavaria §27 Data Protection of the Bayerisches Krankenhausgesetz). These laws aim at protecting personal and, in particular, highly confidential health-related data of individuals against unlawful access, processing and transfer and at guaranteeing the right to informational self-determination in the medical treatment context.

Within the German legal system there is not a specific telemedicine act. Thus the general legal framework described above

[26] For general information on telemedicine in Germany see Karl Jähn, Anja Gärtig-Daugs, Eckhard Nagel, 'Telemedicine and e-Health' (2005) 11 Telemed J E Health 146-50 (also available at: http://online.liebertpub.com/doi/pdf/10.1089/tmj.2005.11.146); Ali Sunyaev (ed.), Healthcare Telematics in Germany. Design and Application of a Security Analysis Method (Gabler, Germany 2011); Tobias Dehling, Ali Sunyaev, 'Information Security of Patient-Centered Services Utilising the German Nationwide Health Information Technology Infrastructure, in Proceedings of the 3rd USENIX Workshop on Health Security and Privacy (HealthSec'12) (May 2014) https://www.usenix.org/system/files/conference/healthsec12/healthsec12-final9.pdf; Id., 'Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure' (2014) 24 Electronic Markets 89-99.

provides for the legal constraints to be implemented in e-health solutions. The main purpose of e-health and telemedicine applications is to optimise access to medical, mostly patient-related, information and to enable the flow of information inside the healthcare system and along the medical treatment chain.

Most of the legal constraints in data processing and mandatory organisational and technical requirements also result from traditional medical confidentiality (§203 Strafgesetzbuch, StGB and §9 Musterberufsordnung für Ärzte, MBO). Medical confidentiality is applicable to any aspect of medical treatment and must be respected by anyone directly or indirectly involved in patient care.

As a general rule, written consent is necessary for collecting and processing personal health-related data (§4 BDSG, § 630d of the German Civil Code (Bürgerliches Gesetzbuch, BGB)). Then, the patient has to be informed prior to asking for consent, about the purpose and the extent of the data collection as well as about the individuals, groups of individuals or institutions that will have access to these data or will receive the patient data for further processing (art. 15 of BayDSG). There is also an implicit consent given by a patient who is treated in a hospital to involve other specialists or any physician of the same department and to forward or grant access to non-anonymous parts of her EHR to other hospital specialists for a second opinion.

The patient also has the right to obtain information on who

is allowed to access the stored information, or on who has already accessed this information. She may also decide to whom to grant access to her medical records.

In the telemedicine context, the patient must agree before data is transferred or provided to other medical professionals involved in her treatment and the data subset must also be directly linked to the treatment episode or to a defined health condition of the patient.

Furthermore the patient has the right to access the documents containing objective medical information that are stored in her patient record and also request deletion, if no legal requirements demand the long term archiving of these documents.

Regarding securing sensitive data, a telemedicine platform shall provide safe channels of communication and secure storing of data according to current technical standards (see, for instance, art. 7 of BayDSG). This includes the extensive use of encryption technologies on all layers starting from the network communication and ending up at the storage of patient-related data and documents. In addition to securing data storage and flows, the whole server, network and building infrastructure has to be designed and managed in conformance with current data protection laws and standards. Furthermore, access restriction policies for servers and data storage systems and for the application itself, a detailed audit trail, backup strategies, firewalls and intrusion detection systems, and a secure operating system are all issues to be addressed by the

security architecture.

The platform must ensure the authenticity of the identity of all users according to current technical best practices, with reference to regional or national strategies and also in line with the technical means provided at a regional or national level. The authentication can be achieved by using personal certificates usually stored on health professional and social-services/insurance smartcards, forwarding access data by separate channels (token generator, SMS, e-mail, paper-based TAN list), password-protected access, and access for registered IP addresses only. The authorisation to access patient documents should be regulated on a fine-grained level, limiting access only to health professionals who directly provide medical services to the patient for a defined medical problem and only as long the problem persists. With the consent of the patient, access rights can be extended.

For compliance with data protection regulation, the system must provide auditing functionalities, required for: documenting, tracing and detecting cases or attempts of abuse; providing information about the transactions relating to the data and documents of the patient; documenting access to the system. The integrity of the stored data must be ensured.

3.2.2 France

France has a highly centralised system: the majority of political and administrative authorities are located in Paris. In 1982,

however, a trend toward decentralisation began, which led to the delegation of powers to the Regions. The population of France is approximately 62 million inhabitants. The healthcare system is pluralistic: private and public bodies co-exist. Patients choose their GPs and have free access to different types of hospitals.[27]

The e-Health projects are developed by different actors, both regionally and locally. At the national level a mapping of all of these initiatives has been carried out. Among these, the following are of significant interest:

- *SESAM-Vitale*: it was introduced at the end of the 1990s and interconnects more than 223,000 healthcare professionals in the National Health System. The system is based on three elements:
    - *Carte Vitale*, a chip card that contains simple administrative information (health insurance details

[27] As references for this part, see E-Health ERA, 'Fact sheet France' (March 2007) http://www.ehealth-era.org/database/documents/factsheets/France.pdf; euser, 'eHealth Country Brief: France' (2005) http://www.euser-eu.org/eUSER_eHealthCountryBrief.asp?CaseID=2220&CaseTitleID=1061&MenuID=118; Violette Peigné, 'Il trattamento dei dati sanitari in Italia e Francia tra convergenze e divergenze' (2008) Diritto dell'Internet 296; Michael Gagneux, 'Pour un dossier Patient virtule et partagé et une stregie nationale des systèmes d'information de santé' (23 April 2008) http://www.d-m-p.org/docs/Rapport_DMP_mission_Gagneux.pdf; EHR Implement, 'WP5 – National reports of EHR implementation – France' (28 May 2009) http://www.ehr-implement.eu/download.cfm?downloadfile=A684205D-1143-DEB7-74D3FF51299F09E6&typename=dmFile&fieldname=filename; Commission Nationale de l'Informatique et des Libertés, 'Measures for the privacy risk treatment' (translation of June 2012 edition) http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf.

and beneficiaries), recently replaced by the new Vitale 2;

- *Carte de Professionnel de Santé* (CPS), a microprocessor smart card used by GPs, created in 1993 (later expanded through the Ordonnances Juppé of April 1996 to organise a secure infrastructure for electronic health information systems); the included features are: identification, authentication and electronic signature of health personnel;
- *Réseau santé social* (RSS), the health network for distributing data streams and encouraging communication between health professionals and health insurance funds.

- Health website (http://www.sante.fr), developed under the direction of the Directorate General of the Ministry of Health, which has as its principal objective the promotion of information from the public agencies with regard to issues of public health;
- Different applications and platforms in the field of telemedicine are already used in some regions; at a national level we find the '*Dossier Médical Personnel*' (DMP).

The DMP is an ambitious project started in 2004 with Law No 2004-810 of 13 August 2004 on '*Assurance maladie*' (the DMP is

stated in art. L. 161-36-1 of the Code de la Sécurité sociale)[28]. The reform has not respected the deadline (1 July 2004) due to the size of the project that affects 60 million patients, and also because of limited computerisation among health professionals. The project to date is not yet fully complete.

The purpose of data processing carried out by the DMP consists in ensuring better coordination, quality and continuity of health service. Another purpose, more of a political nature, is obviously to reduce healthcare expenses.

The DMP consists of a storage system of health data for each beneficiary of the compulsory health insurance system. It is under the direct control of the patient. It contains:

- data that allows the identification of the patient (name, surname, date of birth, login to the opening and operation of the files) and information identifying the professional;
- data of GPs (previous medical history of specialist consultations, allergies, vaccinations, etc);
- data on the treatment (results of examinations, records of preventive and therapeutic measures, ongoing illnesses, treatments in progress, etc);
- data on prevention (individual risk factors, reports, quotes, etc);
- data on clinical findings (radiography, scanner).

[28] See <http://www.d-m-p.org/index.php> accessed 24 June 2014.

The inclusion of new data, their amendment or deletion is subject to the patient's consent. Healthcare workers have access to the system through the simultaneous use of two smart cards: the CPS and the Vitale-2. For personal use, patients can access the DMP online through the national portal: access is managed through login and password. The information is entered into the system only by authorised healthcare professionals. Each piece of information is dated and signed, and its author identified. There is also a special section devoted to information that the patient can add about her health (all documents are marked using the IHE-XDS standard).

Data retention is supervised by the patient, who must choose a special service provider called '*hérbegeur*', which may be a natural person or legal entity approved in advance through a process led by a special committee (of which there are currently six). The link between patient and *hérbegeur* is regulated by a *hébergement* contract (the *hébergement* has an obligation to ensure the security and confidentiality of data in compliance with the provisions of the Act and is bound by professional secrecy).

The patient who directly controls the DMP benefits from free access to all data via Internet, even without the intervention of a healthcare professional. She also has access to the system log files in order to know exactly which data has been accessed, by whom and when.[29]

[29] The patient's consent is required for accessing and administrating the DMP, as an expression of the self-determination principle. We must however take into

The patient does not have the ability to modify the content of medical DMP (*rectius*, entered and signed by health professionals data). The patient has the right to *masquage*: this is the right to withhold, even temporarily, access to information.[30]

There is currently no general legislative framework that establishes the sharing of personal data in the medico-social sector. However the legislation in both these contexts emphasises the need for coordination of stakeholders, in particular with information systems.

Pursuant to article L. 1110-4 of Code de la Santé publique, modified by Law no.2009-879 of Loi de 21 juillet 2009 Hôpital, patients, santé, territoires (HPST), anyone cared for by a professional, a business, a health network or any other organisation involved in prevention and care has the right to respect for her private life and confidentiality of her information. The right to privacy of patient health information offers a double (legal and

consideration that, in cases of emergency, a special procedure is provided, called 'Brise de glace' ('breaking of the glass'), which allows access to the DMP when it is impossible for the patient to give consent. This represents an ex-post control, since the patient knows exactly who has accessed, when and why.

[30] This right is adjusted to the reality of the doctor-patient relationship and takes into account the fact that the patient reveals the information in a manner proportional to the degree of this confidence: the greater the confidence, the more detailed the information. This possibility has raised many criticisms. Healthcare professionals claim that they could not be held responsible for the fact that it was not the correct procedure or treatment if they were not in a position to know that the data to which they had access were incomplete. Potential risks abound, in particular where the more sensitive (and therefore more likely to be hidden) information happens to also be most important for patient care (especially if the masking is carried out by a patient not sufficiently aware of the risks).

technical) protection and covers both the sharing and exchange of health information.

Pursuant to Article L. 1111-14 of Code de la Santé publique, sharing health data between health professionals is subject to the approval of the patient, regardless of the mode of exercise. It is therefore compulsory to inform the patient and to have her free and clear consent. If the patient cannot express her consent (or is a child or a protected adult), the health professional must ask for the consent of her family or legal representative. In the case of emergency, patient consent is not required (from article L.1111-1 to article L1111-9 of Code de la Santé publique).

The hosting platform, whose role it is to store and archive personal health data, is meant to ensure compliance with the requirements of confidentiality, security and sustainability of these data. Article L.1111-8 of Code de la Santé publique and Decree No. 2006-6 of 4 January 2006 set the legal constraints relating to hosting of personal health data. As a consequence, this is a requirement for health professionals to meet a set of standards of security and confidentiality when storing health data on their own information systems.

To share medical information hosted in France, the telemedicine provider has to ensure a high level of security concerning the control of data integrity (Article R.4127-73 of Code de la Santé publique, revised in 2003), meaning data are consistent and correct.

The platform must provide safe channels of communication according to current technical standards (encryption, firewall) and safe storage of directory data.

Privacy regulation requires the use of the health professional card (CPS) for access, exchange and sharing of health data of a personal nature. CPSs are produced and distributed by the National Agency in charge of Health Information Systems (ASIP Santé), which authenticates the carriers and tracks their actions.

A data processing manager must be identified according to Article 3 of Loi de 6 janvier 1978 n° 78-17 (pertaining to data protection, IT, files and freedom) with the task of managing a list of participating health professionals and assessing the quality of health professionals.

All activities running in a telemedicine system must be logged. The platform should log incoming and outgoing communication. Each activity should include ongoing training of the health professionals involved (Article R.4127-73 of Code de la Santé publique revised in 2003).

3.2.3 Austria

The rights regarding the use of any personal data are set out in the Austrian Data Protection Act (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)).[31]

[31] As general references for this part, see Thomas Mairinger and others, 'The legal situation of telemedicine in Austria' (1997) 3 J Telemed Telecare September 154-

Specifically, every person has a set of rights, as the right to confidentiality, to disclosure of stored personal data, to correct untrue information, and to have unjustly used data removed.

The Austrian telematics act (Bundesgesetz betreffend Datensicherheitsmaßnahmen beim elektronischen Verkehr mit Gesundheitsdaten und Einrichtung eines Informationsmanagement (Gesundheitstelematikgesetz - GTelG)) provides for a centralised specialist directory. However, any person (even practitioners) can agree to have a set of data stored in a telemedicine platform.

According to the Austrian Data Protection Act, sensitive personal data can be processed only: a) if the data subject provides informed consent (which can be revoked at any time by the patient, making any further data exchange unlawful); b) if the data is needed to save the life of the patient and consent cannot be obtained; c) if data is used for health protection, medical diagnostics, healthcare and treatment or management of health services, and only if the data is being used by medical professionals or other persons who are bound to professional secrecy.

Data confidentiality has to be ensured by using networks for transmission that are encrypted and only a closed group of authenticated users can access, or by protocols and measures

7; Wolfgang Dorda and others, 'Introducing the Electronic Health Record in Austria', (2005) 116 Studies in health technology and informatics 119-24 (also available at http://www.meduniwien.ac.at/msi/mias/papers/Dorda2005a.pdf).

ensuring the complete encryption of health data.[32] Data integrity has to be ensured using electronic signatures based on qualified certificates or by ensuring that data cannot be changed without leaving traces.

The identity and role of the healthcare provider receiving the data have to be assured using electronic signatures based on qualified certificates or the eHealth directory. If it is not possible to reach the standards mentioned above for identity, roles and integrity, healthcare providers have to at least mutually confirm identities and roles via personal contact (protocolled) or via telephonic contact (protocolled) or via contractual clauses regarding electronic contact or via the eHealth directory. There are no specific regulations on patient identification in health telematics in Austria. However, it is going to be up to the due diligence of the treating physician to make sure that the identification of the patient is ensured.

According to §14 of the Data Protection Act, the use of sensitive data has to be adequately (ie within the technical possibilities) registered, especially (but not limited to) any changes, queries and transmissions.

3.2.4 Italy

Within the Italian legal system, the point of reference is

[32] Implementing Advanced Encryption Standard (AES) [FIPS197] or TripleDES [ANSI X9.52] in CBC or CTR Modus [NIST 800-38A].

Legislative Decree 30 June 2003, n. 196 'Codice in materia di protezione dei dati personali' (IDPC), which actually implemented the European Directives[33]. This regulatory action dedicated a specific discipline to this issue. In particular, art. 4, par. 1, lett. d, of Italian Data Protection Code defines so called 'sensitive data' as follows:

> 'personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life'.

In order to process such information a stricter and more protective discipline has been provided, since its collection, communication and dissemination may present the data subject to which they pertain with several serious risks of discrimination. The Code provides also a specific regulation on the treatment of health data in Part II, Title V 'Processing of personal data in the healthcare sector', arts. 75-94.

[33] For a further analysis see Roberto Pardolesi (ed.), Diritto alla riservatezza e circolazione dei dati personali (Giuffré, Milano 2003) 1 ff.; Juri Monducci, Giovanni Sartor, Il Codice in materia di protezione dei dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196 (Cedam, Padova 2004); Francesco Cardarelli, Salvatore Sica, Vincenzo Zeno Zencovich (eds.), Il codice dei dati personali. Temi e problemi (Giuffré, Milano 2004) 11 ff.

Consent and Information Notice

'Consent' is a pivotal concept and represents a sort of gateway to treatment. European legislators, as we know, have opted for a very protective model for citizens' rights based on the opt-in system (prior consent to treatment). The processing of health data (sensitive data by definition) is subject to rules and more stringent requirements. According to art. 23, par. 1 IDPC, the processing of personal data shall only be allowed if the data subject gives her express consent. It has to be given

> 'freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13' (art. 23, par. 2, IDPC).

The consent shall, thus, always be accompanied by the specific 'Information Notice', which shall disclose all the information required by art. 13 and describe the terms of service, emphasising its voluntary nature, without any effect on the possibility of accessing medical care. In this notice, the right of the data subject, set by art. 7 IDPC, must be displayed. In addition to the elements required by art. 13, the information notice shall highlight in detail the processing operations carried out for scientific purposes, within the framework of telemedicine services, or through the use of modern technologies, including telemedicine and telecare, or to supply other goods or services to the data subject via electronic communication networks (see arts. 78 and 79 IDCP).

Regarding the processing of sensitive data, art. 26, par. 1 establishes a particular discipline:

> 'Sensitive data may only be processed with the data subject's written consent and the Data Protection Authority's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations.'[34]

Within the health sector, art. 76, par. 1, of IDPC provides a specific regulation:

> 'Health professionals and public healthcare bodies may process personal data disclosing health, also within the framework of activities in the substantial public interest pursuant to Section 85,
>
> a) with the data subject's consent, also without being authorised by the Garante, if the processing concerns data and operations that are indispensable to safeguard the data subject's bodily integrity and health,
>
> b) also without the data subject's consent, based on the Garante's prior authorisation, if the purposes referred to under a) concern either a third party or the community as a whole'. [35]

---

[34] See 'General Authorisation n. 2/2013 - Authorisation to the processing of data disclosing health and sex life - December 27', 2013, adopted by Italian Data Protection Authority.

[35] The Garante per la protezione dei dati personali is the Italian Data Protection Authority, an independent authority set up in 1997 to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure

Consent is required in appropriate forms at the time of the first useful contact with the healthcare provider. With regards to the way the consent is expressed, the article 81 mentions two possibilities:

- consent to process one's sensitive data (disclosing health conditions) can be expressed in a unique declaration, which can be oral or written;
- in the case of an oral declaration, the healthcare professional or public healthcare authority takes note of the expressed consent and of the delivery to the interested person of the General Privacy Informative Note.

Article 82, however, states that the Information Notice and the consent on the processing of one's personal data can take place also after the delivery of the healthcare treatment, without delay, only in the following cases:

- emergencies or cases involving public hygiene;
- physical impediment, lack of legal capacity, or incapacity to distinguish right and wrong, when 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;

---

respect for individuals' dignity.

- impending and irretrievable danger for the data subject's health or bodily integrity;
- when the delivery of the necessary medical treatment can be negatively affected in terms of its timeliness or effectiveness by the need to obtain the data subject's prior consent.

Within the specific scenario of digital treatment by an e-health platform, consent must necessarily have the following elements. Although it can be shown together with the consent provided for the data processing for care purpose, it must be autonomous, collected *ad hoc*, and specific to the digital treatment. It is worth emphasising that in its basic setting this kind of digital application must involve an opt-in system, in line with the structure of the legislation on the protection of personal data: this choice, however, needs to be modulated with reference to the specific data that fit inside the information system. The logical consequence of that is the collection of autonomous consent and several specific consents, separate from the one required for the processing of data collected for specific purposes of care.

It is clear that the multiplication of consents, in line with a strong concept of self-determination by the patient, necessarily leads to the possibility that this personal choice actually be managed by the patient through interfaces that can allow her to express or withdraw it in relation to levels of modular access (for example, in differentiated data bases) by several data controllers; the system must keep track of the operated options.

Finally, it must be mentioned that the data subject may at any time withdraw her consent to the processing. After the withdrawal it will not be possible for parties other than those who generated the health data to access to them. Consequently, sharing of the patient data among health professionals will stop.

Notification of processing

The notification is a statement through which a public or private entity informs the Data Protection Authority of the processing of personal data it intends to perform. The notification, implementing Article 18 of European directive 95/46/EC, is governed by articles 37 (list of treatments to be notified), 38 (notification mechanisms) and 39 (communication of obligations) IDPC.

The Italian Data Protection Authority, with the Decision of 31 March 2004 relating to the cases to be removed from the notification requirement, with the Opinion of 23 April 2004 concerning clarification on the treatment to be notified, and the Opinion of 26 April 2004 on the notifications within the health sector, has established the limits of application of article 37.

As regards our scenario, the notification must be submitted if the treatment involves:

> 'data disclosing health and sex life processed for the purposes of assisted reproduction, provision of healthcare services via electronic networks in connection with data banks and/or the

supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, HIV-positivity, organ and tissue transplantation and monitoring of healthcare expenditure' (art. 37, par. 1, lett. b).

Thus, the electronic provisions of healthcare services, made in connection with databases, need to be noted. This implies that the treatments in which the physician uses a data bank, even electronically, but does not provide the online medical service, having a direct (and physical) relationship with the patient at her own clinic, are not subject to the obligation of notification.[36]

The notification of processing operations shall have to be submitted to the Authority in advance of the processing and only once, regardless of the number of operations to be performed and the duration of the processing, and may concern one or more processing operations for related purposes. A notification shall only be effective if it is transmitted via the Data Protection Authority's Website[37] by using the form containing the request to provide all the pieces of information listed in art. 38, par. 2.

Securing sensitive data and technical security measures

A proper health data treatment should require, given the delicacy of the content, the adoption of security measures of

[36] Thinking of the future implementation of an e-health platform, we should take into account the nature of the medical provision. Only if the electronic system will replace the traditional one, will the notification be compulsory.
[37] https://web.garanteprivacy.it/rgt/NotificaTelematica.php.

technical nature.

The security measures provided by the IDPC are classified as 'suitable and preventative' security measures and 'minimum' security measures. The IDPC dedicates Title V to the regulation of data and systems security, devoting Chapter I to security measures in general and Chapter II to minimum security measures. The regulation is contained in articles 31 and following, in 'Technical Specifications Concerning Minimum Security Measures (Annex B)', and in article 3 on 'Data Minimisation Principle'.

Article 31 ('Security Requirements') states:

> 'Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventive security measures, the risk of their destruction or loss, whether by accident or not, of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.'

Namely, the rule states that the implementation of 'suitable preventative security measures' has to conform to the following three elements: a) technological advance of security; b) the types of processed data; c) the kind of data process.

Furthermore, these security measures have not been standardised, since they are impossible to establish, as they change

constantly depending on technological developments. From a purely technical point of view, we are talking about anti-virus software, back-up procedures, and also physical measures, including burglar or fire alarms installed in the offices where data are stored.

Chapter II of the IDPC provides at art. 33 a precise definition of the 'minimum' security measures that data controllers have to implement, in the framework of the more general requirements as established by art. 31, in order to assure a minimum level of personal data protection. Every person who wants to carry out personal data processing is obliged to adopt a generic protection duty and to implement further minimum measures. Actually, they affect substantially the organisation and the methods of data collection, introducing directly binding precepts whose non-observance is (criminally) sanctioned.

Article 33 ('Minimum Security Measures') states:

> 'Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant to this Chapter in order to ensure a minimum level of personal data protection.'

Regarding the processing of personal data by electronic means, it shall only be allowed if the minimum security measures below are adopted, in accordance with the arrangements laid down

in the technical specifications as in Annex B (art. 34):[38]

- *computerised authentication*;
- *implementation of procedures for managing authentication credentials*:[39]
    - authentication credentials shall consist of an ID code for the person in charge of the processing associated with a secret password that shall only be known to this person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password (Annex B, p. 2);
    - one or more authentication credentials shall be assigned to or associated with each person in charge of the processing (Annex B, p. 3);

[38] The non-compliance with the minimum security measure requirements is punished by detention for up to two years or by a fine of between 10,000 and 50,000 Euro (art. 169).

[39] Regarding access to network services provided by public administrations, see art. 64, par. 2, Legislative Decree 7 March 2005, n. 82 (eGovernment Code) that establishes that: '2. Public Services can provide access to network services they deliver that require digital identification also by means other than electronic identity card and the national services card, provided that such tools allow the identification of the person requesting the service. Access to the electronic identity card and national services card is still permitted regardless of the access mode defined by individual administrations'.

- the instructions provided to the persons in charge of the processing shall require the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care (Annex B, p. 4);
- where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used and at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months (Annex B, p. 5);
- an ID code, if used, may not be assigned to another person in charge of the processing even at a different time (Annex B, p. 6);
- authentication credentials shall be deactivated if they have not been used for at least six months, except

for those that have been authorised exclusively for technical management purposes (Annex B, p. 7);

- authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data (Annex B, p. 8);
- the persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions (Annex B, p. 9);
- when data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes relating to system operations and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing,

without delay, as to the activities carried out (Annex B, p. 10);

- *use of an authorisation system that can allow the user access to specific resources to pinpoint the authorisation profile*
    - when authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used (Annex B, p. 12);
    - authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to the start of processing in such a way as to only enable access to the data that are necessary to perform processing operations (Annex B, p. 13);
- *regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance of electronic means*
    - within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be

drawn up by homogeneous categories of tasks and corresponding authorisation profiles (Annex B, p. 15);

- *protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software*
    - personal data shall be protected against the risk of intrusion and the effects of programs as per Article 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months (Annex B, p. 16);
    - the regular update of computer programs aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months (Annex B, p. 17);
- *implementation of procedures for safe keeping backup copies and restoring data and system availability (ie back-up copies)*
    - organisational and technical instructions shall be issued such as to require at least weekly data back-ups (Annex B, p. 18);
    - in case of sensitive data: if either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be

compatible with data subjects' rights and not in excess of seven days (Annex B, p. 23);

- *implementation of encryption techniques or identification codes for specific processing operations performed by healthcare bodies in respect of data disclosing health and sex life.*

Finally, article 3 IDPC states the so-called 'data minimisation principle':

> 'Information 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'.

This principle represents the general clause guiding the specific rules provided by Title V and it requires data controllers to adopt organisational measures to minimise the use of personal and identification data[40]. That goal can be reached using anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity. In relation to the implementation, this provision requests something new and very expensive. It implies remarkable investment in computer and information resources (the information systems must be reconsidered in order to be able to

[40] See Giovanni Buttarelli, 'sub Art. 3. Principio di necessità nel trattamento dei dati', in Cesare Massimo Bianca, Francesco Donato Busnelli (eds.), La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 (Cedam, Padova 2007) 32 ff.

incorporate and manage what the provision sets out) and in terms of human resources.

In the following subsections some detailed information on security issues profiled in a telemedicine application scenario will be provided.

The construction of a healthcare database

The construction of a health database is very delicate in terms of compliance with privacy regulation and technical solution.

The IDPC sets out a number of rules in this regard.

Article 22, par. 6, establishes that sensitive data contained in databases and kept with the aid of 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.'

The scope is to provide a database containing health information, in which the patient to whom these data refer is recognisable only when necessary.

Paragraph 7 of art. 22 adds:

> 'Data disclosing health and sex life shall be kept separate from any other personal data that is processed for purposes for which they are not required. Said data shall be processed in

accordance with the provisions laid down in paragraph 6 also if they are contained in lists, registers or data banks that are kept without the help of electronic means'.

These precautions, as seen above, are also reasserted at art. 34, par. 1, letter. h).

Therefore, when creating computerised databases containing health data, encryption techniques or identification codes should be adopted in order to permit the separation of health information by name or identification number of the patient and the health information (the object of particular protection) from other personal data relating to the patient. The matching between the identification data and the health data (and thus the recognition of the patient) should only occur as a result of further voluntary and conscious operation by the health professional of decryption or entering identification code.

Furthermore, point 24 of Annex B establishes that:

'Healthcare bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been

specifically authorised to access them. Containers equipped with locks or equivalent devices must be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.'

All this requires an *ad hoc* design of the database that will be created around the physical separation between identification data and disclosing health status data. The identification data can be encrypted at the database level using advanced encryption techniques: this solution will keep anonymous health data in the event of unauthorised access to the database.

Finally, Annex B provides two final requirements on removable media: a) the organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing (Annex B, p. 21); the removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be reconstructed by any technical means (Annex B, p. 22).

Authentication and authorisation system

The main requirements that need to be implemented when

you are processing personal and sensitive data with respect to the adoption of computerised authentication and authorisation systems are listed above.

With respect to our scenario, the implementation of strong authentication systems appears to be a crucial point. It is required by the particular category of data that are processed and by the specific features of the platform treatment itself. This system shall ensure that access to the system is granted only to those who really are entitled to process the data and prevent, therefore, that (unauthorised) third parties have access and process sensitive data.

Then, the system of authorisation has to be modulated and handled properly and perfectly in accordance with the permission levels that from a legal point of view allow different care professionals to access data and the operations required. To do this, you need to map carefully the information process and determine who can do what, having as reference the care process involving the patient. Evidently, the 'Case Manager(s)' will have the highest level of permission in the system; other healthcare professionals will have a level of permission modulated on their actual activities and needs.

Finally, as regards patient identification procedures, the use of devices for verifying the (digital) identity of users is strongly recommended, before authorising access to resources in the various domains. Thus, in addition to the usual logins and passwords, a smart card should be delivered to patients in order to achieve high levels of security standards (ie strong authentication).

Traceability and audit system: the augmenting tools of technology

Another crucial requirement is the implementation of a system that can guarantee the traceability of accesses and activities carried on and audit log systems for controlling database accesses and detect abnormalities.[41]

The need for a uniform mechanism to reconstruct the 'situations of accountability' with respect to the generation of each single data made available on the system must be emphasised. It should be noted that an audit system, able to track user activity and to determine *ex post* any responsibility, represents a key point of any future e-health system. Although the probative value of the log file is the subject of debate, it is tempting to say that in this case technology offers the possibility of interpreting the requirements of protection with a level of effectiveness unattainable in the pre-digital era. A system capable of generating a warning message (for example, via e-mail) that alerts the patient to the fact that his/her data has been accessed, and by whom, is far from chimerical.[42] This will represent a formidable tool of control for patients, ensuring

[41] See the 'Security Measures' established at par. 10 of 'Guidelines on the Electronic Health Record and the Health File, 16 July 2009' of Italian Data Protection Authority, provided for the specific EHR domain.

[42] This tool has been established for the Italian EHR. According to Article 14 of the Draft of the President of the Council of Ministers Decree 'Electronic health records in accordance with Article 12, paragraph 7, of Law Decree 179/2012 and Art. 13th, paragraph 2 quarter of Decree-Law 69/2013, all access to patient information is recorded in a special section of electronic health records and patients can access them at any time. In addition, each Region or Autonomous Province may provide a notification service, promptly informing the data subject with a text message or an e-mail about any access of his/her health data.

that data pertaining to them are always treated in accordance with the conditions of legitimacy provided by law. Information regarding access will allow the patient to check, when she wishes, the reason for the display of her data and, where appropriate, to ask for an explanation in this regard, finally enforcing what is established by Data Protection Regulation.[43]

In order to build a telemedicine module, the e-health platform shall implement a tool, which allows the patient to generate data directly in the informative system and, at the same time, monitors such activity, keeping track of each insertion and modification. This would help reconstruct at any given time the information available to the healthcare professional, regardless of the activity of the patient (we can assume the adoption of a sort of 'history' system of the entries that cannot be modified).

Governance of data processing: the difficulty of addressing the power to control the flow of health information

It must be emphasised that the correct identification of the 'responsible' subject of the treatment is a pivotal operation, and it is, indeed, crucial for the efficient and effective management of the entire process. As part of treatment in place by computerised e-health systems, generally the 'data controller' of the treatment will be identified in the local healthcare organisation, as the only subject able to put in place the strategic choices with regard to the

[43] With reference to the Italian legal system, see art. 7 IDPC.

treatment and the security measures to be implemented[44].

It is also important to identify correctly the 'data processor' (as specified and clarified previously) and to ensure that this appointment is not just another bureaucratic task, but rather a driving force for the management and implementation of the privacy policy within the various contexts in which the treatment is carried out by the data controller.

Finally, the authorisation to the treatment to the 'persons in charge' should be considered and managed wisely, in order to make it correspond to the real powers and the actual granting legitimacy of such persons/employees. As noted above, these authorisations must be fully incorporated in the digital infrastructure through systems that manage the permissions granted to the users in a manner consistent with the legal constraints and the medical expertise of the person in charge.

Legal validity and reliability of data entered into the system: an open problem

Even if it is not properly a privacy or security requirement, it should be stressed that data protection in telemedicine and e-health systems is achieved through another fundamental aspect: information management. During the design phase, it is essential to analyse the type of information that the system manages, which is

[44] Once a networked system is set up, resulting in the communication and exchange of health information, we, then, could talk about so called 'co-ownership', a question still far from being clearly delineated from a legal point of view.

the followed path within the system and how this information is then stored and maintained. Only in this way will we be able to understand what rules must be observed and what security measures should be applied.

It is necessary to have an in-depth knowledge of the legal nature of medical documents to be digitised and the related responsibilities.

The legal validity to be associated with documents generated within the system by any party has an impact also and especially with reference to the possible medical liability (and damages) that might result from an erroneous assessment of these data that could have led to misdiagnosis.[45] This issue concerns the regulation on electronic documents and electronic signatures and, therefore, the legal value that the law ascribes to such 'digitised data' entered into the system. The problem has, among other things, an obvious impact on the organisational structure of the health entity taken into account.

In this context there is a crucial need for a legislative intervention in order to clarify the levels of responsibility relating to the activities carried out in this new digital scenario. Therefore, the following analysis does not claim to be comprehensive or complete, but it is aimed, however, at presenting a clear picture of the legislation applicable in this context.

---

[45] As general references for this part, see Giovanni Pascuzzi, Il diritto dell'era digitale (3rd ed. il Mulino, Bologna 2011) 95-117; Ettore Battelli, Il valore legale dei documenti informatici (Edizioni Scientifiche Italiane, Napoli 2012).

At a European level, the point of reference is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 ('on a Community framework for electronic signatures'), which established a minimum set of rules and technical requirements with which all States must comply. Italy, like other EU Member States, has transposed the provisions contained in this Directive and come up with a set of rules.

In Italy, the discipline of electronic documents now in force is shared between the Italian Civil Code and the Digital Administration Code (DAC), approved by Legislative Decree 7 March 2005, n. 82.[46] The legislature, through the DAC, has provided an arrangement of the matter, trying to establish equivalences between the electronic documents and the 'traditional' ones, and adjusting the value in concrete and substantial evidence of different types of documents.

In an attempt to simplify a surely complex discipline, the following types of electronic document, useful in our application context,[47] can be identified and briefly defined:

1. *the electronic documents signed with simple electronic signature*;[48]

---

[46] As amended by Legislative Decree of 30 December 2010, n. 235. Together with these rules we need to take into account the discipline contained in the Presidential Decree of 28 December 2000, n. 445 (Consolidated administrative documentation) and in other minor legislative acts.

[47] You could also have the case of the electronic document with authenticated signature and the electronic official document.

[48] 'Simple electronic signature': set of data in electronic form attached to or logically associated with other electronic data, used as a method of electronic identification (art. 1, par. 1, lett. q, DAC).

2. *the electronic document signed with an advanced (but not qualified) electronic signature*;[49]
3. *the electronic document signed with a qualified*[50] *(especially digital*[51] *or equivalent) signature*;
4. *the electronic document without any kind of electronic signature.*[52]

The need for a uniform mechanism to reconstruct the 'situations of accountability,' concerning the generation of each single data made available on the system, must be emphasised.

It should be noted that an audit system that can track user activity and determine *ex post* any responsibility, represents a key point. As we have already stressed, a system capable of generating a warning message for alerting the patient about an access to his/her data is under construction. The approach behind such a control

---

[49] 'Advanced electronic signature': set of data in electronic form attached to or associated with an electronic document that allows the identification of the signatory of the document and provides the unique connection to the signatory, created through means on which the signatory can maintain an exclusive control, linked to the data to which that signature refers so as to allow detection if the same data have been subsequently modified (art. 1, par. 1, lett. q-bis, DAC).

[50] 'Qualified electronic signature': a particular type of advanced electronic signature, which is based on a qualified certificate and created by a secure device for the creation of the signature (art. 1, par. 1, lett. r, DAC).

[51] 'Digital electronic signature': a particular type of advanced electronic signature based on a qualified certificate and a system of cryptographic keys, one public and one private, related to each other, which allows the holder using the private key and the recipient using the public key, respectively, to make manifest and verify the origin and integrity of an electronic document or a set of electronic documents (art. 1, par. 1, lett. s, DAC).

[52] Pursuant to art. 20, par. 1, DAC, the electronic document created by anyone, the storage on computer support, and the transmission by electronic means comply with the technical rules set out in article 71 are valid and relevant to the effects of the law, pursuant to the provisions of the DAC.

would be more practical and realistic with respect to the attempt to define *ex ante* once and for all the various access levels.

Another critical issue is the legal validity to be associated with documents generated within the system by any party. This has an impact also and especially with reference to possible medical liability. The flip side of this issue is the following question: will the professional actors of the system, particularly GPs, but also the stakeholders responsible for HO, really trust data put into the system by the patient? They might end up making mistakes by trusting inaccurate or untrue information; or they could be accused of being wrong, if they decide not to take into account truthful data posted in the digitised systems (and therefore added to the availability of medical knowledge) directly by the patient. The digital scenario is not different and cannot be dissociated from the dynamics of trust which are expressed in the physical world. If a physician met a patient for the first time and was assailed with a mountain of documents showing a range of information on past medical history of the patient (analysis, personal annotations, recipes for taken medicines, etc), it is plausible to think that the physician would not be led to place a particular degree of confidence on this information provided by a person whom - at this early stage - he does not know. Very different is the level of trust when we have the interaction between a GP and (for instance) a chronic patient, who goes twice a week to the medical clinic, carries out daily self-measures, and forwards them to his trusted physician.

This type of interaction builds up a trusted relationship that can be easily translated into an interaction guaranteed by the digital infrastructure: this would surely lead to a more efficient and effective path of healing. This kind of relationship embodied in the activities involved in a telemedicine project.

Both in the case of an electronic document without signature and with electronic signature, the issue around which the rule is set is related to the ability of the document to be considered as a written form (regardless of evidentiary purposes).

With specific reference to point no. 4 (electronic document without any kind of electronic signature), the suitability to satisfy the requirement of written form and its probative value is freely assessed in court, in view of its objective characteristics of quality, safety, integrity and immutability (art. 20, par. 2, DAC). The main critical issue for legal purposes is the fact that the assessment of this capacity is only subsequent and depends on many circumstances, not all predictable. A similar situation characterises the case stated in point no. 1: in terms of evidence, it is freely assessed in judgement, in view of its objective characteristics of quality, safety, integrity and immutability (art. 21, par. 1, DAC). In relation to the cases stated in no. 2 and 3, these documents have the effect provided for in art. 2702 Civil Code, namely the private deed, which is full proof, until a complaint of forgery, of the origin of the statements by those who have signed, if the person against whom the writing was produced recognises the subscription, or if this is considered to be legally

recognised.[53]

Articles 22, 23 and 23-ter DAC deal with the (analogue or digital) copies of a document. Without going further in the description of all the circumstances involved, it is worth mentioning that, pursuant to art. 22, par. 3, DAC, computer-generated copies of original documents, originally created on an analogue format in compliance with the technical rules set out in art. 71, have the same probative force of the originals from which they are taken if their conformity to the original ones is not expressly disclaimed.

In conclusion, the types of documentary production recognised in the digital environment are numerous and some are being tested. From a legal, and also archival, point of view the crucial aspect refers to the ability to assess the consequences in terms of 'quality', 'safety', 'integrity' and 'immutability' of the various documentary evidence produced. For this evaluation, it is essential to examine in greater detail the internal mechanisms from which these characteristics originate.

[53] The main difference with the paper environment concerns the issue of signature repudiation: in the digital world this possibility is transformed into an obligation to prove the contrary by the owner of the device).

4. Common Feasible Privacy and Security Issues in a Telemedicine Application Scenario. A set of recommendations

4.1 Premise

In this last section, the legal principles that should characterise the implementation of a telemedicine application will be extrapolated to an appropriate level of abstraction.[54]

Although the legal systems outlined are different and varied (and they represent just a paradigmatic list of all the European Union countries), however, in all of them it is possible to outline some necessary and essential elements established in order to carry on the processing of patient medical data within a computerised structure. First of all, the need to obtain the patient's consent surely

---

[54] As general reference for this part and in order to further analyse the issues involved, see Nevena Stolba, Marko Banek, A Min Tjoa, Thomas Mueck, 'The Security Issue of Federated Data Warehouses in the Area of Evidence-Based Medicine' (2007) 15th European Conference on Information Systems, St. Gallen, Switzerland http://wit.at/people/stolba/documents/DWH%20Support%20for%20Interoperability%20of%20e-Health%20Systems.pdf; Bernd Blobel, 'Comparing approaches for advanced e-health security infrastructures' (2007) 76 Int J Med Inform 454–9; Paolo Guarda, Nicola Zannone, 'Towards the Development of Privacy-Aware Systems' (2009 51 Information and Software Technology 337-350 (also available at http://security1.win.tue.nl/~zannone/publication/guar-zann-08-IST.pdf); Karl A. Stroetmann, Joerg Artmann, Veli N. Stroetmannm, 'European countries on their journey towards national eHealth infrastructures. eHealth Strategies Report' (January 2011) http://www.ehealth-strategies.eu/report/ehealth_strategies_final_report_web.pdf; Jun Lu, Song Zhang, E-health Web Application Framework and Platform Based on The Cloud Technology Master Thesis (Spring 2013) http://www.diva-portal.org/smash/get/diva2:647835/FULLTEXT01.pdf.

represents a constant: it has to be specific and, above all, informed with respect to the particular type of treatment that the telemedicine pilot intends to put in place. In addition, highest security standards are always established for the management of health data with particular reference to the construction of the databases, the communication within the system of the medical information, the guarantee of their integrity and incorruptibility, etc. Also stressed is the importance of implementing authentication and authorisation systems fit to ensure, on the basis of particular technologies and tools, that only those who are really entitled may have access to personal data and that different permission levels correspond to each subject in a way compliant with the roles that they really play within the system itself. Finally, traceability and audit systems must be implemented in order to ensure that all the activities carried into the digitised infrastructure can be traced and, possibly, verified.

4.2 Consent and Information Notice

The pivotal issue that has to be taken into account is 'consent'. It is a sort of gateway to treatment. European legislators have opted, as we know, for a very protective model for citizens' rights based on the opt-in system (prior consent to treatment). We have also shown that the processing of health data (sensitive data by definition) is subject to rules and more stringent requirements. Consent must, therefore, be considered a prerequisite and essential to any treatment, even more when the processing means through

which it is carried out result in the creation of risks and potential problems to the security and integrity of the data themselves. Consent is regulated and modulated in partially different ways in the various legal systems. The need for it, however, is a constant. It expresses the principle of self-determination of the patient, allowing a variety of choices within the same treatment, and the platform has to be designed on the real needs and interests of the individuals according to the choices expressed in the consent. Thus, consent is the main instrument through which, in this context, the principle of self-determination is expressed.

From a technical point of view, consent to the processing of health data must generally be made in writing. This formality, even though it is easily manageable through traditional paper-based interactions at the time of the first contact between the patient and the healthcare body that provides the health service, may, however, be a critical point to solve if not properly managed also from a digital point of view. E-health platforms must be structured in such a way as to allow the patient-citizen modular management of consent (it also has to be compliant with the applicable rules for what concerns the legal - and evidential - value of electronic documents).

Once consent is duly served, it must be preceded by an Information Notice. The information notice shall outline, albeit schematically, the characteristic features of the particular processing of medical data in order to trace the essential structure and allow the

patient to be informed about the procedures and rules that will govern the processing of her health data.

Finally, it must be noted that the data subject may at any time withdraw her consent to processing. After withdrawal, it will not be possible for parties other than those who generated the health data to access to them, while access to medical records will always be granted to those who have produced them. As a consequence of that, sharing among health professionals of the patient data will stop.

We can summarise the main features of consent as follows: necessity of data subject's written consent; it must be autonomous and collected *ad hoc* for specific digital treatment; a general consent to the telemedicine treatment and possible several specific consents for specific purposes of care (blanking identified clinical data, etc.); the data subject can withdraw consent at any time.

Some information shall be delivered to the patient in order to explain the peculiarities of the data treatment and the responsibilities with respect to data directly entered into the system. The information notice, in fact, shall highlight in detail the processing operation carried out, the data controller and the terms of service, the voluntary nature of the consent, the data subject rights as established in the data protection regulation. Furthermore, it shall, also, stress the fact that the processing is carried out within the framework of telemedicine services or through the use of modern technologies or to supply other goods or services to the

data subject via electronic communication networks.

4.3. Securing sensitive data and technical security measures

The processing of sensitive data must surely involve the implementation of high technical measures to ensure data security.

The sensitivity of health data processed by a digitised system requires the adoption of specific technical measures to ensure appropriate levels of security (art. 17 Directive 95/46/EC).

A telemedicine platform has to minimise possible threats to data integrity, implementing the security measures established by law. These include, among others:

- computerised authentication system;
- implementation of procedures for managing authentication credentials;
- use of an authorisation system that can allow the user access to specific resources to pinpoint the authorisation profile;
- regular update of the specifications concerning the scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance by electronic means;
- protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software;

- implementation of procedures for safe keeping backup copies and restoring data and system availability (i.e. back-up copies);
- implementation of encryption techniques or identification codes for specific processing operations;
- data confidentiality and database encryption: the telemedicine platform must provide safe channels of communication according to current technical standards (encryption, firewall) and safe storage of directory data;
- traceability of access and operation carried out.

With respect to the physical safeguards, the data controller shall implement some measures to protect the hardware and facilities to the stored Personal Health Information (PHI). The following solutions are recommended:

- facility access controls: the limitations for physical equipment access to the facilities where the health information system is housed, to ensure that authorised personnel are allowed to access the system;
- workstation use: some specific rules for the proper use of workstations and the characteristics of the physical environment of workstations that can access PHI;
- workstation security: restrictions on access to workstations with PHI;

- device and media controls: it means the receipt and removal of the device and media which will contain the PHI into and out of the facility, for example, disposal, reuse of media, accountability, and backup and storage.

The pivotal recommendation for the management of sensitive data contained in databases states that an electronic system must implement 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.

Moreover, health data shall be kept separate from any other personal data that is processed for purposes for which they are not required.

One solution to the first recommendation is to directly encrypt the sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. This prevents anyone without the keys from using the data.

Within the e-health sector a strong authentication system is recommended, for both healthcare professionals and patients.[55] It

[55] The adoption of a 'safe' authentication system is a crucial point in the future of any digitised platform for managing health data. The Working Document on the processing of personal data relating to health in electronic health records (EHR), adopted on 15 February 2007 by Article 29 Data Protection Working Party, explicitly deals with 'Identification and authentication of patients and healthcare professionals' and stresses that 'reliable identification of patients in EHR systems is of crucial importance. If health data were used which relate to the wrong person as a result of incorrect identification of a patient the consequences would in many cases be detrimental'; and further on again, 'the special sensitivity of

can be based on, eg, one-time password (using a token or a mobile phone), or encryption chip-based devices (smart card, USB token), etc.

On the other hand, the system of authorisation has to be modulated and handled properly and perfectly in accordance with the permission levels that from a legal point of view allow stakeholders access to data and the operations required.[56]

4.4 Traceability and audit system

The implementation of a uniform mechanism for reconstructing the chain of accountability, concerning the generation of each single data in the platform is key to the system. An audit system that can track user activity and determine *ex post* any responsibility, is fundamental for ensuring a level of effectiveness unattainable in the pre-digital era. At the same time,

---

health data requires that no access is possible for unauthorised persons. Reliable access control depends on reliable identification and authentication. This makes it necessary to uniquely identify and also properly authenticate users'. The solution proposed by Working Document is represented by the use of smart cards that provide a high level of reliability and security: 'Health cards on smart card basis could contribute significantly to a proper electronic identification of patients and also to their authentication if they want to access their own EHR data'. However, regarding patient identification procedures, where permitted by law and if deemed appropriate to increase the level of user satisfaction, other kind of authentication systems may be studied and evaluated, mainly based on mobile applications.

[56] Finally, with reference to physical security, the data centre should be established in a safe place for the timely detection and prevention of emergency situations created by earthquakes, fire, water leakage or flooding, etc. Physical access controls are needed in these secure locations, such as locks, electronic key readers, or other access control mechanisms.

the provision of an *ex ante* measure, such as an automatic message warning the patient about any access to her medical records, represents a formidable tool of control for the patient ensuring that data pertaining to her are always treated in accordance with the conditions of legitimacy provided by law. The certainty given by technology, in this specific context, could help in better designing the e-health platform and ensuring a dynamic protection of patients' informational privacy.

4.5 Communication of health data in a cross-border context

Starting from the general rule, data disclosing health may not be disseminated, ie made available to an undetermined person.[57]

They may, instead, be communicated or transmitted to certain subjects (ie by the data controller to the data processor), but the transfer must be in encrypted form.[58] Taking into account, as an example, the Italian legal context, this is established by Annex B to IDPC, n. 24. In particular, in the case of transmission of data between server of data controller and client of data subject, it must be through secure communication protocols based on encryption standards for electronic data transfers, including digital certification

[57] See, for example, Section 26, par. 5 IDPC.

[58] The legal requirements for data transmission is satisfied by using the Transport Layer Security (TLS). TLS is a cryptographic protocol which is designed to provide communication security over the Internet. See Tim Dierks, Eric Rescorla, 'The Transport Layer Security (TLS) Protocol' (August 2008), Version 1.2 http://tools.ietf.org/html/rfc5246.

of the systems delivering network-based services (https SSL - Secure Socket Layer - protocols). The file containing the examination record(s) will have to be protected so as to prevent unlawful and/or unwanted acquisition of the information by other entities other than the relevant addressee(s). To that end, the file may be password-protected.

In the transmission, it is necessary to avoid unauthorised acquisition of data during any caching, by adopting suitable techniques.

The recipient of the communication should be identified with certainty. In case of an individual recipient, suitable authentication systems based either on standard credentials or, preferably, on strong authentication procedures, have been recommended. Another application of the principle of sure identification of the person concerned has been made with respect to sending the online examination record via email to the patient (in this case it is necessary for the email addresses to be validated by means of an ad-hoc online checking procedure).

It is appropriate to point out that in each case processing operations, even when lawful, should not be carried out unless they are essential.

Transfer of health data within the EU and the countries of the 'European Economic Area' (EEA) (Norway, Liechtenstein and Iceland) does not require compliance with additional conditions. In case of different destination countries, you need to verify that the

level of protection of personal data is equal to that existing in the EU. Currently this is particularly true for a very limited number of countries (eg Switzerland).

4.6 Governance of data processing

The correct identification of the 'responsible' subjects of the treatment is a crucial task.

The data controller is responsible for organising all aspects of processing: for this reason they appear to be the main recipient of responsibility and the penalties prescribed by law on the processing of personal data. The person who fills the role of data controller must be the one who faces choices about the material treatment of data and the type of data to be collected and recorded, the amount of data to be acquired, the time of conservation of the same in relation to the purpose, the sources from which to draw, updates, etc. Article 2, lett. d, Directive 95/46/EC provides the definition:

> '[data] controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law'.

Thus, the main characteristic is represented by the autonomous

power of decision making in relation to the purposes of treatment, the operating choices, tools to use, etc.

We have the particular case of co-data controllers on the same treatment, when the choices on purpose, method, tools and security measures for the treatment are related to multiple subjects. This issue may represent a crucial point in building up digital infrastructure fit to manage health data. The concept of co-data controllership should be considered in parallel with the concept of 'data processor'. Directive 95/46/EC defines the 'data processor' at art. 2 letter e: '[data] 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.'

4.7 Legal validity and reliability of data entered into the system

An e-health platform has to assure the technological and legal certainty of both the data and the metadata entered and gathered. The importance of such a requirement is evident if we consider the profiles of liability.

This issue runs around the legal nature ascribed to electronic documents and electronic signatures at a national level. From a legal point of view, there is often a lack of an articulated clarifying intervention of the legislature that can elucidate the critical issues involved in this new context. As explained above, advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device satisfy the

legal requirements of a signature in relation to data in electronic form, just as a handwritten signature satisfies those requirements in relation to paper-based data, and are admissible as evidence in legal proceedings (see art. 5 Directive 1999/93/EC). The implementation of advanced electronic signatures, however, raises huge issues relating to the management of signed documents, signature keys and certificates that are often barely addressed. On the other hand, the adoption of a strong authentication system seems to help assign to the simple electronic signature (eg data entered by an user) a legal value, which could be considered relevant by a judge, obviously in relation to the context and the praxis (local healthcare organisations) in which the telemedicine pilot is carried out.

The Trento Lawtech Research Paper Series is published since Fall 2010

1. **Giovanni Pascuzzi**, L'insegnamento del diritto comparato nelle università italiane (aggiornamento dati: dicembre 2009) - The Teaching of Comparative Law in Italian Universities (data updated: December 2009), Trento Law and Technology Research Group Research Papers, October 2010.

2. **Roberto Caso**, Alle origini del copyright e del diritto d'autore: spunti in chiave di diritto e tecnologia - The Origins of Copyright and Droit d'Auteur: Some Insights in the Law and Technology Perspective, Trento Law and Technology Research Group Research Papers; November 2010.

3. **Umberto Izzo**, **Paolo Guarda**, Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato - E-health, Data Protection and Generational Digital Divide: Empowering the Interested Party with the Faculty of Nominating a Trusted Person Acting as a Proxy when Processing Personal Health Data within an Electronic PHR, Trento Law and Technology Research Group Research Papers; November 2010.

4. **Rossana Ducato**, "Lost in Legislation": il diritto multilivello delle biobanche di ricerca nel sistema delle fonti del diritto (convenzioni internazionali, leggi europee, nazionali e regionali, softlaw) - "Lost in legislation": The Multilevel Governance of Research Biobanks and the Sources of Law (International Conventions, European, National and Regional legislations, Softlaw), Trento Law and Technology Research Group Research Papers; December 2010.

5**. Giuseppe Bellantuono**, The Regulatory Anticommons of Green

Infrastructures, Trento Law and Technology Research Group Research Papers; February 2011.

6. **Francesco Planchenstainer**, La regolamentazione dell'acqua destinata ad impiego alimentare: analisi storico comparativa dei differenti approcci sviluppati negli USA e nella UE - The Regulation Of Water For Nutritional Use: A Comparative and Historical Analysis of the Different Approaches Developed in US and EU Law, Trento Law and Technology Research Group Research Papers; April 2011.

7. **Roberto Caso, Giovanni Pascuzzi**, Valutazione dei prodotti scientifici nell'area giuridica e ruolo delle tecnologie digitali – Evaluation of Scientific Products in the Legal Field and the Role of Digital Technologies, Trento Law and Technology Research Group Research Papers; May 2011.

8. **Paolo Guarda,** L'Open Access per la dottrina giuridica e gli Open Archives: verso un futuro migliore? - Open Access to legal scholarship and Open Archives: toward a Better Future?, Trento Law and Technology Research Group Research Papers; November 2011.

9. **Thomas Margoni**, Eccezioni e limitazioni al diritto d'autore in Internet - Exceptions and Limitations to Copyright Law in the Internet, Trento Law and Technology Research Group Research Papers; January 2012.

10. **Roberto Caso**, Plagio, diritto d'autore e rivoluzioni tecnologiche - Plagiarism, copyright and technological revolutions. Trento Law and Technology Research Group Research Papers; February 2012.

11. **Giovanni Pascuzzi**, Diventare avvocati e riuscire ad esserlo:

insegnare l'etica delle professioni forensi attraverso le trame narrative - How to become lawyers and able to do so: teaching the ethics of the legal profession through narrative, Trento Law and Technology Research Group. Research Papers; July 2012.

12 **Umberto Izzo**, IL 'Contratto sulla neve' preso sul serio: due modelli di contratto (per la fruizione delle aree sciabili e per l'insegnamento sciistico) – Taking the 'Contract on the Snow' Seriously: Two Model Contracts (For Accessing and Using the Ski Area, and For the Teaching of Skiing), Trento Law and Technology Research Group Research Paper; 2012.

13. **Francesco Planchestainer**, "They Collected What Was Left of the Scraps": Food Surplus as an Opportunity and Its Legal Incentives, Trento Law and Technology Research Group Research Paper; Febraury 2013.

14. **Roberto Caso**, I libri nella "tempesta perfetta": dal copyright al controllo delle informazioni digitali - Books into the "perfect storm": from copyright to the control of information, Trento Law and Technology Research Group Research Paper; March 2013.

15. **Andrea Rossato**, Beni comuni digitali come fenomeno spontaneo - Digital Commons as a Spontaneous Phenomenon, Trento Law and Technology Research Group Research Paper; May 2013.

16. **Roberto Caso**, Scientific knowledge unchained: verso una policy dell'università italiana sull'Open Access - Scientific knowledge unchained: towards an Open Access policy for Italian universities, Trento Law and Technology Research Group Research Paper; May 2013

17. **Valentina Moscon**, Copyright, contratto e accesso alla

conoscenza: un'analisi comparata - Copyright, contract and access to knowledge: a comparative analysis, Trento Law and Technology Research Group Research Paper; December 2013

18. **Roberto Caso**, La via legislativa all'Open Access: prospettive comparate - The legislative road to Open Access: comparative perspectives, Trento Law and Technology Research Group Research Paper; January 2014

19. **Roberto Caso**, Misure tecnologiche di protezione: cinquanta (e più) sfumature di grigio della Corte di giustizia europea, Trento Law and Technology Research Group Research Paper; March 2014

20. **Federica Giovanella,** Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale, Trento Law and Technology Research Group Research Paper; April 2014

21. **Umberto Izzo, Rossana Ducato,** The Privacy of Minors within Patient-Centered eHealth Systems, Trento Law and Technology Research Group Research Paper; June 2014

22. **Roberto Caso, Rossana Ducato,** Intellectual Property, Open Science and Research Biobanks, Trento Law and Technology Research Group Research Paper; October 2014