

EHR and Data Protection Issues in Italy

Maria Gabriella VIRONE^{a,1}

^a*C.I.R.S.F.I.D. – Alma Mater Studiorum University of Bologna, Italy*

Abstract. Technological progresses and the changed way to collect, access and use data are at the bottom of the European Commission proposal for a “General Data Protection Regulation” (25 January 2012). Implications of safeguarding privacy and harmonization of existing rules are extremely important also for national Health Systems. Mobility of patients and health professionals as well as cross-border healthcare connected with the increasing use of Information and Communication Technologies in Healthcare Services are modifying traditional medical approaches and applications. New tools, as Electronic Health Records, provide significant benefits as empowering health consumers and minimizing health costs. Anyway, EHRs have limits: for example, they should cause risks for individuals, professionals and institutions in terms of personal injuries and liabilities. In this scenario, it’s evident that technical aspects (as health standards and interoperability) are as important as legal and regulatory privacy issues. Presently, mandatory acts on the protection of individuals with regard to the processing of health e-Data still missing at all levels. Italy is adopting binding and non-binding legal documents to tackle the problem. Are they enough?

Keywords. E-Health, Electronic Health Record, Data Protection, Patients rights.

Introduction

Information and Communication Technologies (ICTs) in Healthcare Services are being developed to improve the efficiency and effectiveness of public health: ICTs allow integrating heterogeneous systems (for example, epSOS project aim to interoperability between EHR systems in Europe) and developing medical standards (such as DICOM, HL7, MLMs, GLIF) for sharing e-Medical Data; the use of ICTs is also encouraging the growth of specific business models for e-Health and the quality of patient care is getting better (one of the main results of patient safety is the reduction of clinical risks). In the era of globalization and international mobility, Electronic Health Records are a functional tool to achieve a good level of information and participation among all actors involved in health processes (hospitals, public health administrations, medical doctors, nurses and citizens/patients).

If new developments in ICTs offer benefits, they cause risks for individuals, professionals and institutions in terms of personal injuries or liabilities. Therefore, if it’s decisive implementing health standards and encouraging studies and researches on interoperability, at the same time it’s extremely urgent to focus on privacy protection issues. In fact, legal instruments are essential to guarantee protection of patients rights in cross-border healthcare but also protection of personal health e-Data.

¹ Correspondence to: Maria Gabriella Virone, C.I.R.S.F.I.D., Faculty of Law, Alma Mater Studiorum University of Bologna, via Galliera 3, 40121 Bologna, Italy, e-mail: mariagabriella.virone@gmail.com.

European policy and legislation are improving and promoting well-defined actions and legal documents in advancing specific use of health-related ICTs in health care delivery. Particular attention is also given to develop standards for security and privacy protection. The same is happening at the national and international levels. Directive 95/46/EC is the EU's main legislative act in the field of data protection: even if its general principles remain valid, new digital challenges require more efficient rules to ensure the right to personal data protection.

According to this evidence, in 2009 the European Commission launched a public consultation on a review of the legal framework for the fundamental right to the protection of personal data. As result, on 25th January 2012 the European Commission proposed a comprehensive reform of the Directive, especially to harmonize national rules. In fact, in a connected world, where the way to collect, access and use data is changed, safeguarding privacy is essential. Particularly interesting is the focus of the "proposal for a General Data Protection Regulation" on the controller and processor of data: new elements regard their obligations; in particular, article 23 sets out "the obligations of the controller arising from the principles of data protection by design and by default", principle that was yet recalled by the Commission [COM (2007) 228, COM (2010) 245 and COM (2010) 609] to give more effectiveness to personal data protection; a chapter illustrates rights of the data subject, as "the obligation on controllers to provide transparent and easily accessible and understandable information, including information on the storage period, the right to lodge a complaint, in relation to international transfers and to the source from which the data are originating" and "the right to be forgotten and to erasure".

At the light of this ongoing international and European debate (particularly significant are "the Annual European Data Protection and Privacy Conference" and "the Annual Conference on Computers, Privacy and Data Protection"), on the same basis (having more efficient guidelines on data protection in a connected world), two Italian institutions - the Data Protection Authority and the Ministry of Health - enacted non-binding rules governing EHRs: "Linee guida in tema di Fascicolo Sanitario elettronico e di dossier sanitario" (2009) and "Il Fascicolo Sanitario Elettronico. Linee guida nazionali" (2010). One of the main goals of the two mentioned documents is ensuring health protection for citizens but also regulating medical doctors and nursing procedures; moreover, mentioned documents stressed the necessity to introduce on the Italian system detailed binding legislative acts on Health e-Data protection. In fact, currently, the main Italians' act in the field of data protection is the "Italian Privacy Code" (d.lgs. 196/2003) that has the same limits of the Directive 95/46/EC: rules are too flexible and they risk of failing to protect citizens; there are also lots of indications for the controller and processor of information but generally legislative structure ignores new networks (and consequently more complex dynamics on data management and transfer) that have been grow up with the use of ICTs in Healthcare systems.

Similarly to the Proposal, both Italians non-binding documents set out detailed indications on consent, on the data subject's right to be forgotten and to erasure, on the controller and processor of information: a common element among all principles is the special attention to the relationship between data protection issues and EHRs. It means that the Italians institutions shared the idea that implementing digital tools and their related technical aspects (as health standards and interoperability) is as important as legal and regulatory e-privacy issues; it's true especially along this complexity and fragmented juridical framework.

It is expected that future privacy protection issues will be increasingly enacted by legislators at all levels - international, European, and national -. EHR and its evolutions are vital tools in a mobility background, but they need to be regulated, also adopting standards and best practices. The international community and Europe should aim to draw up strategic documents, useful for themselves and especially for Governments. Countries need to enforce pragmatic and appropriate legislation in the field of health e-Data privacy protection.

1. Methods

The overview is focused on exploring existing Italian data protection legislative acts, with special attention on EHRs. A general review has also take into account the EU's main legislative act in the field of data protection (Directive 95/46/EC) and its latest developments.

The following approaches have been used:

- review of the following European documents: Comparative study on different approaches to new privacy challenges, in particular in the light of technological development (2010); Communication "A comprehensive approach on personal data protection in the European Union" (COM (2010) 609 final); Communication "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century" (COM (2012) 9 final); Proposal for a "General Data Protection Regulation" (COM (2012) 11 final);
- review of the following Italian legal documents: the "Privacy Code" (d.lgs. 196/2003); the Italian Privacy Authority guidelines on EHR and health dossier (16 July 2009); the Italian Ministry of Health guidelines on EHR (11 November 2010).

The research is structured around existing binding and non-binding Italian documents related to privacy protection issues with a focus on EHRs. Deeply convinced that the use of ICTs in Healthcare Services is a logical pillar to guarantee the fundamental right to access to health care and to exercise citizens' empowerment, the study considered Italian current legal documents "pioneers" in the field.

The survey also includes the European legal framework on data protection issues, mainly because a deep connection exists between the national and European legislations.

2. Results

The Italian Data Protection Authority guidelines on EHR and health dossier (16 July 2009) and the Italian Ministry of Health guidelines on EHR (11 November 2010) emphasize that it's essential:

- to have national binding laws for realizing a uniform and steady organization in the field of e-Health;
- to set legislative tools fostering multilevel EHR use.

Currently, existing legal documents are regulating only cases in which data are used for healthcare reasons. In the future, access to EHR will also be useful and

necessary for central and local administrations, considering that e-Data helps to manage and simplify the complex bureaucratic state apparatus.

According to this scenario, it's also significant to take into account that different and sometimes antithetic interests have to be regulated by legislators, because many actors are involved in healthcare systems (as patients, providers, government, data-collectors etc.) and they will increase with technological progresses.

In addition, it's important to mention that mandatory acts on the protection of individuals with regard to the processing of health e-Data are still missing at all levels (national, European and international).

The European community should aim to draw up strategic documents, useful for itself and especially for the Member State governments. Countries need goals to enforce a pragmatic and appropriate legislation on the field of EHR and privacy protection issues.

3. Discussion

The Prague Declaration, adopted during the conference "e-Health for Individuals, Society and Economy" (19-20 February 2009) by European Union Health Ministers, exhorted Member States to pay close attention to "legal and ethical issues" including "data protection and privacy issues ... [in pursuit of] a common approach to optimize existing directives on data protection and privacy".

It has been observed, "the declaration is a clear signal that the technical integration of health systems is insufficient by itself. Systems must also include processes for protecting the security and privacy of individual health information" [Rohstein, Boehl, 2009]. In fact, it often happens that citizens and patients from one side and clinicians and nurses from the other side are skeptical in regards to ordinary use of EHRs. There are lots of causes but most of them are related to the fact that the main people involved in the healthcare process frequently believe that robust privacy protections need to be introduced. In fact, a successful implementation of health information technology is strictly linked to this legislative action, which will also facilitate developing EHRs benefits.

If the previous considerations are true, at the same time it is extremely urgent to solve other relevant privacy and security issues, for example ones related to hacking that cause an alteration of information in transmission.

The current state of the Electronic Health Record is evolving. Many projects and studies are exploring and implementing the realization of these new tools at national, European and international levels; however, privacy issues are not so well focused: a new specific "*corpus iuris*" has to be modeled in Italy as in the other European countries focusing its attention on the emerging e-Health and EHR field.

References

- [1] Angst CM, Agarwal R. Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. J MIS Quarterly archive. 2009; 33(2):339-370
- [2] Appari A., Johnson ME. Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management. 2010; 6(4):279-314
- [3] Article 29 Data Protection Working Party. Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments. 00683/11/EN WP 184

- [4] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. 01197/11/EN WP187
- [5] Article 29 Data Protection Working Party. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 02356/09/EN WP 168
- [6] Bindahman S, Zakaria N. Privacy in Health Information Systems: A Review, Informatics Engineering and Information Science Communications. Computer and Information Science. 2011; 254(6): 285-295
- [7] Callens S. The EU legal framework on e-health. Cambridge University Press; 2010
- [8] Cockcroft SKS. eConsent: provenance, use and future role. International Journal of Internet and Enterprise Management. 2010; 6(4):315-325
- [9] Commission of the European Communities, Communication from the Council, the European parliament, the European Economic and Social Committee of the Regions. e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area. Brussels. COM (2004) 356
- [10] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). Brussels. COM (2007) 228 final
- [11] European Commission, Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health records. Brussels. C (2008) 3282 final
- [12] Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions. A Digital Agenda for Europe. Brussels. COM(2010) 245.
- [13] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. Brussels. COM (2010) 609 final
- [14] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. Brussels. (COM (2012) 9 final)
- [15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- [16] European Commission, DG Justice, Freedom and Security. Comparative study on different approaches to new privacy challenges, in particular in the light of technological development; 2010
- [17] Empirica Communication & Technology Research, TanJent Consultancy, Report on The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond, Final study report; 2009
- [18] Garets D, Davis M. Electronic Patient Records. EMRs and EHRs, Healthcare Informatics. The McGraw-Hill Companies; 2005
- [19] Haasa S, Wohlgemuthb S, Echizenb I, Soneharab N, Müllera G. Aspects of privacy for electronic health records. International Journal of Medical Informatics. 2011; 80(2):e26-e31
- [20] London Economics. Study on the economic benefits of privacy - enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security; 2010
- [21] Kahn S., Sheshadri V. Medical Record Privacy and Security in a Digital Environment. IT Professional, IEEE Computer Society. 2008; 10(2):46-52
- [22] Kelly B. E-health: ethical and data privacy challenges in the EU 2011; 27-28
- [23] Ministry of Health, The Electronic Health Record, National guidelines, Italian Official Gazette n. 50, March 2nd 2011
- [24] Ministry of Health, The National eHealth Information Strategy National context, state of implementation and best practices: Italy; 2011
- [25] Moruzzi M. e-Health e Fascicolo Sanitario Elettronico. Milano: Il Sole 24 ore; 2009
- [26] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012) 11 final)
- [27] RAND Europe, Capgemini Consulting, Business models for e-Health, Final Report. 2010
- [28] Rothstein MA. Is Deidentification Sufficient to Protect Health Privacy in Research? AM. J. BioEthics. 2010; 10:3-11
- [29] The "Privacy Code" (d.lgs. 196/2003)
- [30] The Italian Privacy Authority guidelines on EHR and health dossier (16 July 2009)
- [31] www.cdpconferences.org (April 2012)
- [32] www.dataprotection2011.eu (April 2012)
- [33] www.ec.europa.eu (April 2012)
- [34] www.eur-lex.europa.eu/ (April 2012)
- [35] www.normattiva.it (April 2012)