View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repositório Científico do Instituto Politécnico do Porto

SECURITY AND PRIVACY IN EUROPEAN EHRS
Should Portugal Follow Denmark and Sweden's Examples?

Catarina Travassos[1,2], Inês C. Moreira[1,2,3], Patrícia Ferreira[1,2] and Gustavo Bacelar-Silva[1,2,3,4]
[1]*Faculdade de Medicina da Universidade do Porto, Al. Prof. Hernâni Monteiro, Porto, Portugal*
[2]*Faculdade de Ciências da Universidade do Porto, Rua do Campo Alegre, Porto, Portugal*
[3]*Escola Superior de Tecnologia da Saúde do Porto, Rua Valente Perfeito, Vila Nova de Gaia, Portugal*
[4]*CINTESIS, Al. Prof. Hernâni Monteiro, Porto, Portugal*

Keywords: Electronic health record, Health data privacy, Health data security, Portugal, Denmark, Sweden.

Abstract: EHR implementation is an important yet challenging technology that provides better patient care by allowing and providing more accurate and available patient information. An efficient digital health service should ensure not only the quality of data processing, but also the confidentiality and safety of patient data. Portugal is now designing a national EHR and discussing its main characteristics and contents. Our study analyses the experiences of two countries where EHRs were implemented: Denmark and Sweden. The aim was to compare them when it comes to measures taken regarding privacy and security of data and also to what Portugal has planned to achieve as described in available documentation.

1 INTRODUCTION

Privacy and security are considered as being major concerns in EHRs (Thakkar and Davis, 2006). As privacy is defined as the control of collection of information, security can be defined as the restriction of data to authorized parts (Bhagat et al., 2010). Also, a key aspect of data security is assuring that confidentiality, integrity and availability (security components) are preserved. As confidentiality ensures that data or information can only be read by the intended or authorized recipient integrity assures the recipient (and the originator) that the data has not been altered in transit. Also, the availability component guarantees that the systems are accessible when needed and by who needs them (Edwards, 2003).

Considering that Denmark has a history e-health strategies ranging back to 1996, and that Sweden, although being a more recent example (EHR implementation in 2009) is also, in our opinion, a good example of a successful EHR implementation, it is our belief that the gathering of both examples could provide valuable options to the Portuguese future EHR.

2 METHODS

The information about the EHR projects, their information models and the implementation has been collected. Literature search was undertaken by consulting electronic databases as well as hand searching reference lists in published papers. In addition, Danish and Swedish legislation and established requirements on security standards were also searched in government as well as national authorities' websites and official documentation. Regarding Portuguese EHR planning projects, the available documentation on the information models creating the basis for the EHR applications has been studied. In this paper, we identify 6 security issues and 4 privacy topics in the analysed projects and will discuss them in more detail.

3 EHR IN DENMARK

Denmark national strategy is based on 3 specific action plans: 1) A staff tool for supporting healthcare quality and productivity; 2) Improving services and involving citizens and patients and 3) Common infrastructure. The latter action plan involves security and privacy, which help to ensure

Travassos C., C. Moreira I., Ferreira P. and Bacelar-Silva G..
SECURITY AND PRIVACY IN EUROPEAN EHRS - Should Portugal Follow Denmark and Sweden's Examples?.
DOI: 10.5220/0003735003540357
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2012), pages 354-357
ISBN: 978-989-8425-88-1
Copyright © 2012 SCITEPRESS (Science and Technology Publications, Lda.)

interaction between the individual solutions (National Strategy for Digitalisation of the Danish Healthcare Service, 2007). Security is at the very core of the Danish Health Data Network. In fact, Denmark implemented the DS 484 security standard as the basis for security activities (National Strategy for Digitalisation of the Danish Healthcare Service, 2008-2012). DS 484, is the national equivalent to the ISO 27002 Code of practice for information security management, modified to suit Danish conditions (ISO 27000, 2008).

As patients expect their data to be confidential and protected from unauthorized access, it is also important to assure than enough information is provided to clinicians so that they can perform a well-supported clinical decision. In Denmark, although patients do not own their data, they are offered two different privacy regimes. They can opt-in or opt-in with restrictions. Opt-in means that they allow use of personal information, but require consent before data can be disclosed to third parties. Most patients choose opt-in, over opt-in with restrictions that are not specified (Deutsch & Turisco, 2009). The "break the glass" system is allowed in emergency situations.

4 EHR IN SWEDEN

The Swedish project, known as NPÖ aims to improve patient security and quality of care by developing the national electronic health record in stages. Sweden implemented the SS-ISO/IEC 27001:2006 security standard (SS-ISO/IEC 27001:2006) as the basis for security activities. A digital communication system, "Sjunet," ensures that physicians use a special electronic ID card to log in, and keeps track of each instance that a health record is accessed. Patients not only have the option of restricting which professionals can access their record, but they can also restrict the period of time after the visit that the health professional can continue to access it. As in Denmark, the system has a "break the glass" option, allowing healthcare professionals to access the record in an emergency.

5 EHR IN PORTUGAL

The documents that plan the future implementation of the Portuguese EHR recommend a security policy based on principles and norms relevant for IT systems as ISO 27799 based on ISO 27002 (RSE-R1, 2009) (RSE-R2A, 2009). The plan of operations for Portugal's 2010, refers several aspects in which is stated the harmonization of legal bases to assure permission, privacy, confidentiality and safety when accessing and treating information. One of the topics is Legal harmonization and it includes activities that aim to obtain a legal consensus that allows EHR implementation, assuring also that all matters of confidentiality, access security, transfer and data use are completed (RSE – PO, 2010). According to the Portuguese legislation, the patient is the owner of his own health data, and the health institutions are the keepers of that information. In Portugal, two types of privacy regimes will be possible: opt-in and opt-out. In the first option, the patient won't have his data included in the EHR by default, being necessary the patient to state his intention of including his data in the EHR. In the latter, the patient will have his health data in the EHR repository by default and may request for selected data not to be included in the EHR. The "break the glass" policy has also been considered as it happens in Denmark and Sweden.

6 COMPARING PORTUGAL TO DENMARK AND SWEDEN

As previously mentioned, these countries present some differences about privacy and security concerns. These differences regarding privacy are presented in more detail in Table 1, 2, 3 and 4.

Table 1: Comparison in terms of data use restriction.

	Restriction of data use
Denmark	Privacy laws do not restrict data use to improve quality and for public reporting.
Sweden	The law aims to allow patients to decide who can access their medical record, while allowing care providers to communicate permitted patient data in the exchange securely.
Portugal	As part of citizen rights over their own data, it has been found necessary for the citizen to control who can view his information, and whose property would exams, diagnosis results and reports be. While medical exams and diagnosis results are property of the patient, whichever reports come from those results are intellectual property of the physician.

Table 2: Comparison in terms of health professional choice.

	Choose the health professionals that can access data
Denmark	Privacy is protected by a requirement that all health professionals get patients' consent to look at their health information, with the exception of medication profiles, which are accessible to all physicians.
Sweden	Access by the prescriber or pharmacist to information in the database must require the patient's consent.
Portugal	Health care providers require authorization of the patient, to access information. Patient authorization should have a well established validity, meaning that it should be expirable and able to be renewed or not.

Table 3: Comparison in terms of health professionals that can access data.

	Choose the health professionals that can access data
Denmark	According to DS484 this is included.
Sweden	According to SS 627799 this is included. The Social Services Act and the Health Records Act contain provisions designed to protect access to patient information.
Portugal	Not mentioned.

Table 4: Comparison in terms of privacy regimes.

	Privacy regimes
Denmark	Opt-in or Opt-in with restrictions.
Sweden	To meet the goal of the legislation, the Swedish system uses an opt-in with restrictions consent model.
Portugal	Opt-in or Opt-out.

Differences regarding security can be consulted in tables 5, 6, 7, 8, 9 and 10.

Table 5: Comparison in terms of availability.

	Availability
Denmark	Available citizen services are: electronic booking of appointments, access to one's own medical records, prescription renewals, health appointment calendars.
Sweden	Not mentioned.
Portugal	User's access needs should be taken into account.

Table 6: Comparison in terms of confidentiality.

	Confidentiality
Denmark	"Information and services must be accessible and protected so that everyone can rest assured that the information is correct and reliable and that due confidentiality is maintained".
Sweden	Predicted in laws governing the use of information, such as the Secrecy Act (sekretesslagen, 1980:100), the Personal Data Act, the Care Registers Act (lagen om vårdregister, 1998:544) and several other acts concerning registries.
Portugal	According to the Ethics code the law, health professionals are obliged to secrecy in order to keep information security.

Table 7: Comparison in terms of integrity.

	Integrity
Denmark	Not mentioned.
Sweden	Not mentioned.
Portugal	Availability of versions for modified and registered data.

Table 8: Comparison in terms of identity.

	Identity
Denmark	Digital signature. Citizens and patients may only access their own data following individual authentication via a personal digital certificate based on the national OCES-standard. Health professionals may also access patient data having obtained the relevant consent and a local authentication.
Sweden	Citizens will need to use smartcards or similar plastic ID cards to verify their identity. Users will also be required to sign up for the service by filling out a number of security-related documents.
Portugal	National identity card (smart card) A National Patient Database (*Registo Nacional de Utentes*) and a Health Professionals Database should be created, and then spread to private institutions; also create a database for entities that provide health care.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 9: Comparison in terms of access control.

	Access control
Denmark	Only physicians can see all patient data Register nurses can see only current encounter data for patients on their ward. Restrictions on selected diseases, for example, HIV lab tests and results are blanked out ("trusted answer"). Patients can restrict access by role, facility, and type of data. Region laws can override national laws in certain instances (structure decentralized). "Break the glass" regime.
Sweden	In order to view any healthcare record, health care professionals must have a "patient relation" with the patient, meaning the patient has given consent for them to look at his or her health record. Patients not only have the option of restricting which professionals can access their record, they can also restrict the period of time after the visit that the professional can continue to access it. Sweden also restricts health care professionals on how much of the record they can see. County councils and municipalities, not patients, designate which professionals can see which parts of the record. "Break the glass" regime; however, access will be logged and professionals will have to explain why they needed to view the information.
Portugal	Different professional categories should have different user profiles and restricted information. Insurance companies and courts may also require health information from health care institutions. "Break the glass" regime.

Table 10: Comparison in terms of auditability.

	Auditability
Denmark	Full audit trail for access and updates.
Sweden	Health care quality audits available.
Portugal	Audit required to control privacy of patient data, reduce medical error, assure responsibility and insert correction measures. Subject to access rules and policies as the data being audited. Certification and periodic auditing to verify that security measures are in fact active.

7 CONCLUSIONS

Based on all documents consulted about the Danish and the Swedish EHRs implementation, it is our belief that they managed to create a system with functional and useful characteristics that is reliable and considers the most important aspects on patient data security as well as privacy. It would therefore be an example to follow in all its extent and detail. We find that detailed rules provide enough clarification about all these issues, which in turn results satisfactory results and in patient satisfaction. The last public consultation on the EHR proposal ended on 15th September 2010. If all goes according to planned, the EHR should be active with basic functionalities in all national health institutions by 2012, and the complete version should be available by 2015. Even though technically and as far as information security is concerned, the Portuguese EHR is set to be implemented in 2012, this will depend on future government decisions.

REFERENCES

Appendix C: Select Examples of Exchange in Other Developed Countries. *Denmark Country Report*, 2010.

Introduction to ISO 27002 (ISO27002), 2005.

National Strategy for Digitalisation of the Danish Healthcare Service 2008-2012, 2007.

National Strategy for eHealth: Sweden, 2009.

RSE - PO, 2010. RSE - Registo de Saúde Electrónico. PO: *Plano de Operacionalização*.

RSE-R1, 2009. RSE - Registo de Saúde Electrónico. R1: *Documento de Estado da Arte*.

RSE-R2A, 2009. RSE - Registo de Saúde Electrónico. R2A: Orientações para Especificação Funcional e Técnica do Sistema de RSE.

SS-ISO/IEC 27001:2006, 2006. Swedish standard SS-ISO/IEC 27001:2006 Information technology - Security techniques (ISO/IEC 27001:2005, IDT), SIS/TK 318.

ISO 27000, 2008. The ISO 27000 Directory: Introduction to ISO 27002 (ISO27002).

Bhagat, S., Fontaine, D. and Gibson, K., 2010. Danish Healthcare Information Technology - An Analytical Study of Consumer Issues.

Deutsch, H. and Turisco, F., 2009. Accomplishing EHR/HIE (eHealth): Lessons from Europe. *CSC*.

Edwards, R., 2003. Cryptography.

Protti, D. and Johansen, I., 2010. Widespread Adoption of Information Technology in Primary Care Physician Offices in Denmark: A Case Study.

Thakkar, M. and Davis, D., 2006. Risks, Barriers, and Benefits of EHR Systems: A Comparative Study Based on Size of Hospital. *Perspectives in Health Information Management*, p.1-14.