MODELLING A PORTABLE PERSONAL HEALTH RECORD

J. Santos[1,2], T. Pedrosa[1,3], C. Costa[1] and J. Oliveira[1]
[1]*DETI/IEETA, Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, Portugal*
[2]*DEE, Instituto Superior de Engenharia de Coimbra (ISEC), Rua Pedro Nunes, Coimbra, Portugal*
[3] *Instituto Politécnico de Bragança, Bragança, Portugal*

Keywords: Personal health record, Electronic health record, Patient empowerment, Portable personal health record, Personal health in formation.

Abstract: Active and responsible involvement of patients in their own health is accepted as an important contribution towards an increased quality of health services in general. Management of Personal Health Information by the patient can play an important role in the improvement in quality of the information available to health care professionals and as a means of patient involvement. Electronic Health Records are a means of storing this kind of information but their management usually falls under the responsibility of an institution and not on the patient himself. A Personal Health Record under the direct control and management of the patient is the natural solution for the problem. When implemented in a storage hardware portable device, a PHR, allows for total mobility. Personal Health Information is very sensitive in nature so any implementation has to address security and privacy issues. With this in mind we propose a structure for a secure Patient Health Record stored in a USB pen device under the patient's direct management and responsibility.

1 INTRODUCTION

Personal Health Information (PHI) is generated dispersedly (Tang, et al, 2006) and stored under different formats. Modern diagnose and treatment techniques generate great amounts of PHI and population ageing can only increase it. This poses the problem of efficient usability and management. Many PHI management strategies have been proposed (Costa, 2004) namely Electronic Health Record (EHR) systems (Classen, et al., 1991, 1992; Evans, et al., 1992; Schoenbaum, et al., 1992; Tierney, at al. 1993) that have some limitations. Interoperability between different systems is limited (Mandl, et al., 2001; Schonberg, et al., 2000), most contain only institution-generated data and sometimes only at a departmental level (Hasselbring, 1997). Some information supplied by the patient is incorporated in the EHR by healthcare professionals, but making patients responsible and active in their own health, is not a concern of such systems since an EHR is usually managed by an institution. That goal can only be achieved through the use of a Personal Health Record (PHR). This is stressed by the generally accepted definitions of EHR and PHR provided by the Markle Foundation (2004).

People are increasingly mobile. A PHR on a portable device that can also be a repository of emergency data, integrated with an EHR system is the best architecture (Detmer, et al., 2008), since it is standalone, closely integrated with external data sources and allowing for mobility (Román, et al., 2006). In this paper we propose the structure for a portable PHR (pPHR) with main objectives:

- Allow the patient full management capabilities;
- Populated by the patient from various sources;
- Availability to third parties in different contexts.

Such an implementation relies on:

- Strong user authentication;
- Secure data encryption;
- Separate data storage depending on data type;
- Electronic signatures for integrity.

2 BACKGROUND

Current PHR implementations include network-PHRs with decision making tools such as the ones offered by Microsoft and Google, both promising the creation of systems and standards for automated

Santos J., Pedrosa T., Costa C. and Oliveira J. (2010).
MODELLING A PORTABLE PERSONAL HEALTH RECORD.
In *Proceedings of the Third International Conference on Health Informatics*, pages 465-468
DOI: 10.5220/0002746504650468

data collection and updating, allowing for patient mobility since data is accessible from any place with Internet access. But they have some limitations since concerns may be raised as to the security and privacy of data contained in a system over which the patient has no control. The patient controls which information is on the system but not the security and privacy issues pertaining to the system's internal design or the information disclosure policies enforced by the owning companies.

A pPHR overcomes all the mentioned limitations providing full mobility to its users through regular backups, strict access control policies, cryptography, and detailed audits of each activity.

Among the various candidates to a portable PHR device (Costa, et al., 2003), flash USB pens present the most advantages since they can be carried around, their use has been proposed for developing countries (Srinivasan, et al., 2007) and they can also be used in developed countries. Security issues have been raised concerning PHR implementations in these devices (Wright, et al., 2007a, b) but they can be overcome with careful design.

3 PROPOSED STRUCTURE

The basic paradigm of the pPHR is total patient empowerment. Our model also allows patient mobility and provides an emergency data repository.

The pPHR is a complete and fully functional PHI management platform where a repository of the lifelong patient's history is kept based on close interoperability with all the participating institutions where an individual's health data is generated. The pPHR is the most complete repository of an individual's PHI. In the limit, any external EHR system can have as much information, but none is meant to have more. Any access to the pPHR and its data depends exclusively on patient's authorization. In order to allow the patient to both manage the PHI contained in the pPHR and to make it available to other healthcare actors in a scalable manner, various operating modes are available upon patient's option. Population of the pPHR is done by the patient in two different situations, in person and remotely via an Internet connection.

Patient authentication for account provisioning is required for pPHR issuance, authentication method depending on the prior relationship of the issuing institution with the patient. The device is supplied with a built in master-password that will be used for the initial setup of pPHR native applications, upon which the user is prompted to create his working-password. The system only allows three tries of logging. Upon failure of the three attempts, the PHR and all its functionalities are blocked and will only be unblocked via the master-password. Whenever the patient accesses the PHR, he will be prompted to supply the password and to select an operating mode. An inactivity timer blocks the system after a time interval of inactivity that is preset but configurable by the patient. This inactivity lock can be unlocked via the password. One of the key concepts of our model is the existence of different conceptual data types. There are five different data types:

- Confidential pPHR Data: information considered to be extremely sensitive and to be kept secret.
- Normal pPHR Data: information to be disclosed to users in general.
- Transfer pPHR Data, recently downloaded into the PHR waiting for patient's management.
- Prescription pPHR Data, typically generated by physicians to be read by other users.
- Emergency pPHR Data, publicly available in case of emergency.

Figure 1 shows the data types in usage context and Table 1 expresses the different information access privileges by all the actors involved. Through the implementation of this working scenario we achieve free and easy access to emergency information. Prescription PHR Data is still freely available but not displayed because it might be relevant in an emergency situation. Access to prescription information and the possibility of writing Tranfer pPHR Data are given. All actions taking place in the pPHR are recorded and become part of an audit report that keeps track of all information transactions and the respective dates in which those actions took place. The data management functionality is implemented as document classification or document drag and drop strategies.

All data items are electronically signed by their author for information integrity but, in case they aren't, the pPHR provides a functionality that allows the patient to act as a delegated signer. For efficient storage space management, the individual files placed inside each container are compressed with a choice of "deflate" or "bzip2" algorithms. A compression level can be chosen for each file, no compression being also a possibility.

Table 1: Information Type Access Privileges of the various pPHR users.

Information Type / Actor	Confidential	Normal	Transfer	Prescription	Emergency
Patient	Read/write	Read/write	Read/write	Read/write	Read/write
Physician	-	Read	Read/write	Read/write	Read
Social Institution	-	Read	Read/write	Read	Read
Researcher	-	Read	Read/write	Read	Read
Laboratory	-	-	Write	Read	Read
Pharmacy	-	-	Write	Read	Read
Non-qualified	-	-	Write	Read	Read

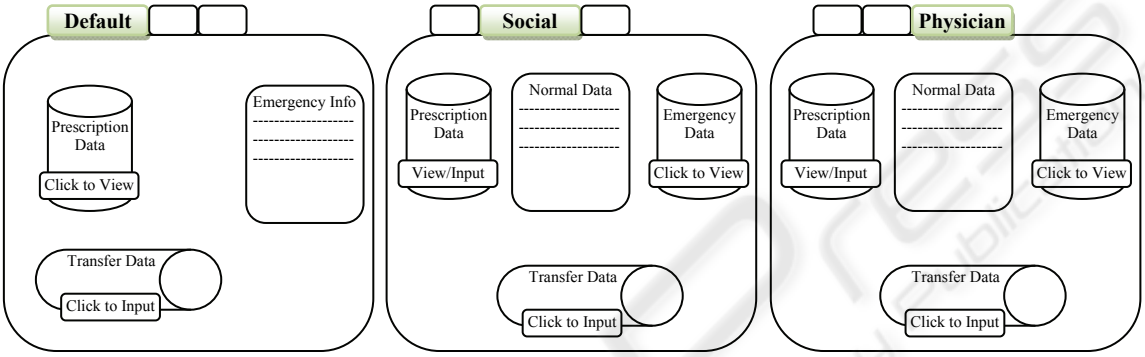

Figure 1: Data types contained in the pPHR.

The pPHR is completely pen-resident and consists of a stand-alone application with various functionalities, one of which allows access to a virtual container where a database and the various data items are stored. The virtual container is implemented in a zip-like manner (ZipArchive) with compression and file encryption via a soft-coded encryption key. AES encryption algorithm and the fact that, upon access by the application, the files are decompressed to computer memory only are important features contributing for enhanced security. The database is built upon SQLite and contains entries that are pointers to individual data items.

Automatic Zip64 extensions allow upgrade of maximum size, maximum size of individual files in an archive, and the number of files in an archive. Each file inside an archive is encrypted by the Advanced Encryption Standard (AES) algorithm with a 256-bit key encryption key. The access to any individual file stored inside a virtual container is subject to authentication and the decompression of the files is made to computer's memory only for improved security.

4 CONCLUSIONS

PHI has been dramatically increasing raising the issue of efficient information management. EHR systems have been implemented but they have some limitations that can be overcome by the use of a portable PHR in a USB pen device that complements existing EHR systems.

Our model totally empowers the patient with respect to his PHI. He decides which data becomes part of the record, who, and under what circumstances, has access to it. The pPHR is fully interoperable and populated with information from various external sources as well as self-entered PHI. Data is kept in separate conceptual data containers.

There are five different data types, each of each of which with different security and confidentiality characteristics.

Some concerns have been expressed regarding the trust a physician can place on patient-generated information. By the use of pPHR, the patient is invited to better understand his own health and, by being able to manage it, his increased health awareness can only be beneficial. The pPHR is meant to be used with an EHR, therefore the

traditional interactions the physician is used to establish with his patients can still be enforced but the later being more informed and collaborative.

There is some overlapping of disclosure and write privileges concerning Emergency and Prescription Data Types. From a technical perspective it's arguable that they could be grouped into a single type but from an organizational and usability perspective they are different. They both are possibly disclosed to most actors but Prescription data is to be generated by the physician and not necessarily to be disclosed in an emergency situation (although possible). The patient can write into that area (although he shouldn't) because nobody should have better access privileges to any part of his pPHR and since every data item is to be electronically signed, there is no confusion possible between physician-generated data and eventual patient-generated data.

REFERENCES

Tang, P., et al. 2006. Personal Health Records: Definitions, Benefits and Strategies for Overcoming Barriers to Adoption. Journal of the American Medical Association, 12, pp.121-126.

Costa, C., 2004. Doctoral Thesis: A Security Dynamic Model for Healthcare Information Systems, in Departamento de Electrónica e Telecomunicações, Universidade de Aveiro.

The Markle Foundation, 2004. Connecting Americans to their Healthcare: Final Report.

Classen, D. C. et al., 1992. Computerized Surveillance of Adverse Drug Events in Hospital Patients. Journal of the American Medical Association, 266, pp.2847–2851.

Classen, D. C., et al., 1992. The Timing of Prophylactic Administration of Antibiotics and the Risk of Surgical-wound Infection. New England Journal of Medicine, 326, pp.281–286.

Evans, R. S., et al., 1992. Computerized identification of patients at high risk for hospital-acquired infections. American Journal of Infectious Control, 20, pp.4–10.

Schoenbaum, S. C., Barnett, G. O., 1992. Automated Ambulatory Medical Records Systems: An Orphan Technology. International Journal of Technical Assessment in Health Care, 8, pp.598–609.

Tierney, W. M., et al., 1993. Physician Inpatient Order Writing on Microcomputer Workstations: Effects on Resource Utilization. Journal of the American Medical Association, 269, pp.379–383.

Mandl, K., Szolovits, P., Kohane, I., 2001. Public Standards and Patient's Control: How to Keep Electronic Medical Records Accessible but Private. British Medical Journal, 322, pp.283-287.

Schonberg, R., Safran, C., 2000. Internet Based Repository of Medical Records that Retains Patient Confidentiality. British Medical Journal, 321, pp. 1199-1203.

Hasselbring, W., 1997. Federated Integration of Replicated Information Within Hospitals. International Journal on Digital Libraries, 1(3), pp.192-208.

Román, I., et al, 2006. Demographic Management in a Federated Healthcare Environment. International Journal of Medical Informatics, 75 (9), pp.671-682.

Detmer, D., et al, 2008. Integrated Personal Health Records: Transformative Tools for Consumer-centric Care. BMC Medical Informatics and Decision Making, 8, p.45.

Costa, C., et al, 2003. A New Concept for an Integrated Healthcare Access Model, Proceedings of MIE 2003 (Medical Informatics Europe). The New Navigators: from Professionals to Patients, Studies in Health Technologies and Informatics, 95, pp.101-106, IOS Press Book Series (ISBN: 1-586-03347-6).

Srinivasan, U., Datta, G., 2007. Personal Health Record (PHR) in a Talisman: An Approach to Providing Continuity of Care in Developing Countries Using Existing Social Habits. 9th International Conference on e-Health Networking, Application and Services, pp.277-279.

Wright,A., Sittig, D., 2007. Security Threat Posed by USB-based Personal Health Records. Ann Intern Med, 146, pp.314-5.

Wright,A., Sittig, D., 2007. Encryption Characteristics of 2 USB-based PHR Devices. Journal of the American Medical Association, 14, pp.397-399.