HealthManagement
Promoting Management and Leadership

Volume 14 - Issue 4, 2014 - Management Matrix

Integrity and the Personal Health Record

Luís Bastião Silva, CTO of BMD Software
******@***bmd-software.com

Carlos Costa

Assistant Professor

José Luis Oliveira

Associate Professor

University of Aveiro, DETI /

IEETA, Aveiro, Portugal

BMD Software Lda

Key Points

• Citizens are becoming increasingly concerned about their personal health information.

• Personal health records (PHR) put the control of these data in their own hands.

• However, the utilisation of existing patient data (EHR, PHR) is a crucial step towards new

How to store , access and explore integrated health records and ensure their privacy

What is a Personal Health Record?

Personal health data is being generated in many distinct points of care and in many different formats. Medical tests such as blood pressure, medical imaging, electrocardiogram and others, are being gathered regularly, contributing to the patient's medical history and providing a valuable insight for future diagnostics. There are several definitions of personal health record (PHR), most of them share the idea of an electronic application through which individuals can access, manage and share information in a secure and confidential environment (AHIMA e-HIM Personal Health Record Work Group 2005). The PHR is a self-contained registry controlled by the subject of care, which allows accessing and consolidating health information, making it available to the ones with the right access credentials. There are several types of PHR instances, such as portable data devices, web entities, or integrated electronic health records.

The PHR is intended to be an electronic individual record maintained by the consumer and can be obtained by several Electronic Health Records (EHR) from different medical healthcare providers. However, considering this dual way of information feeding, the information supplied by the PHR can be factual or subjective. For instance, daily monitoring results (e.g. glucose), periodic weight monitoring, and measurements generated by home monitoring devices, is information that the healthcare professionals can rely on. Subjective information is not fully trustable, is related to its own assessment and could include details such as illness symptoms or fitness information.

Privacy and Confidentiality Concerns

With the explosion of health information technologies, citizens are becoming increasingly concerned about their personal information, as it is increasingly accessible and exposed to disclosure. These concerns about privacy and confidentiality can only be addressed if they control the process related to their medical records, including the control of access to registries, control of transfers and processing, and control of

information deletion. However, citizens cannot be confident and secure about this process, if they do not have access to the information themselves.

The public's concern has been raised by disclosures and violations of confidential medical information. Patients with chronic diseases and other severe medical conditions are a perfect example of a patient group, whose sensitive health information may be vulnerable to misuse. That could affect not only their job status, but also their quality of life in the case of certain insurance denials. Moreover, with the advances in gene research, even young and healthy adults may be concerned about the disclosure of genetic information.

An Approach to Dealing with Security and Privacy Issues

While technology advances have created new equipment and devices to help medical doctors to diagnose specific pathologies, they have also generated more patient data as a natural consequence. The storage of these records has been supported through new technologies such as cloud computing services. Moving personal health data to the cloud is already a reality in several medical institutes around the world, including for instance medical imaging, clinical reports, vital signals, laboratorial tests and many other data sources. Figure 1 depicts key components and data flows. Currently, a significant part of companies in the EHR/PHR industry are claiming their products to be supported over the cloud, and are developing Software-as-a-Service, such as PHR, over the web. Clearly, these approaches bring benefits to healthcare institutions, since they no longer need to scale their own IT infrastructure. Nevertheless, a major issue is to guarantee the privacy of the patient and medical staff. In order to solve the privacy and confidentiality concerns, HIPAA (The Health Insurance Portability and Accountability Act) has defined privacy rules that should be covered by the PHR providers.

The first, and one of the most important issues to address when outsourcing health data storage to third party solutions, is the SLA (Service Level Agreements) with cloud providers. The SLA should clearly define the access level by the infrastructure maintainers, and specify if they are or not HIPPA compliant. While the cloud providers should respect the data ownership, there are no guarantees that special monitors are looking to the data for any special purposes. In order to minimise the problem, the developed solutions should rely on a system authentication, authorisation and accountability. Moreover, researchers are studying strategies to grant privacy and confidentiality of the data and to avoid data tamper (Ribeiro et al.; Silva et al. 2012).

Trends in Personal Health Data

There are successful initiatives such as MyHealtheVet or Microsoft HealthVault, which are offering PHR for patients to update their own health and fitness information. Nonetheless, in recent years, other platforms such as PatientLikeMe have also been gaining momentum. These kind of platforms have the main goal of sharing some of the patient health conditions in order to find similar patients and thus, figure out an adequate treatment or ways to compare treatment outcomes with other subjects. While this can help the patients, they need to be aware that exposing their health problems publically can be risky (see Figure 1).

Personal Health Data Exploration: How to Maintain Patient Privacy and Utilise Data to Answer Research Questions

The confidentiality of patients' records is a social and medico-legal issue. Personal health data is considered valuable information for many entities including hospitals, doctors, researchers and insurances companies. However, to biomedical research communities they are key in the discovery of new and better treatments and drugs. To achieve outstanding results, access to many already existing EHR and PHR is a major necessity. However, access to clinical data depends on patient authorisation, countries' laws, ethical and legal issues, bureaucracy, and several other social, commercial and scientific issues.

While the privacy of patient data is a requirement, it also creates new barriers to research. Recently, new approaches have been used to create distributed environments, which allow research questions to be performed over a set of databases without exposing patientlevel data. The Electronic Health Records for Clinical Research (EHR4CR) and EMIF (EMIF 2014) are two such examples. European Medical Information Framework (EMIF) aims to construct a socio-technological platform to promote the efficient reuse of existing patient data. The patient privacy needs to be kept in safeguard, and in most cases the information cannot flow outside the institution. Moreover, several strategies are being investigated to allow summarising information and extracting aggregated data to answer specific research questions. The analysis of large populations' healthcare data is performed inside the health centre, within their own control, and data never flows outside their safeguard.

While there still exist many issues and controversies about scaling these processes, which are mostly executed in a manual way by the researchers, the ethical and legal aspects will continue to be the major constraint in this path.

Conclusion and Future Perspectives

New technologies have created new opportunities for the integration and centralisation of patient health data. In many cases, moving data is a major requirement in order for the patient or medical staff to access these data everywhere, if they are authorised to do so. Thus, many concerns related to the mobility and data privacy have been raised. Technological solutions already exist to tackle these challenges, allowing to have the data over third party providers, and to access it without losing privacy while ensuring further data exploration. In the coming years, several efforts will be made to create an integrated view of patient records, i.e. to explore patient level data without exposing their privacy. There are still several gaps in the integration of data because, besides the security problems, clinical databases rely on proprietary solutions, distinct languages and terminologies, raising semantic interoperability issues. So, it is fundamental that both ICT and biomedical researchers work together to create new and advanced techniques that help improving patient treatments and general healthcare.

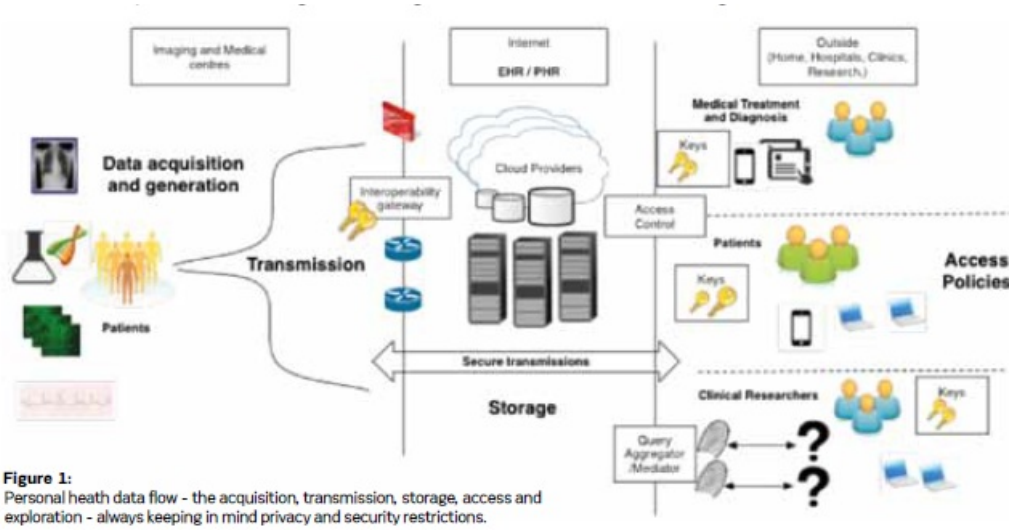

Figure 1:
Personal heath data flow - the acquisition, transmission, storage, access and exploration - always keeping in mind privacy and security restrictions.

Published on : Sat, 8 Nov 2014