Medical Informatics in a United and Healthy Europe
K.-P. Adlassnig et al. (Eds.)
IOS Press, 2009

doi:10.3233/978-1-60750-044-5-700

Centralised versus Decentralised Management of Patients' Medical Records

Catherine QUANTIN [a,b,1], Gouenou COATRIEUX [c], Maniane FASSA [b], Vincent BRETON [d], David-Olivier JAQUET-CHIFFELLE [e], Paul de VLIEGER [d,f], Norbert LYPSZYC [g], Jean-Yves BOIRE [f], Christian ROUX [c], François-André ALLAERT [b,h]
[a] *Inserm, U866, Universite de Bourgogne, Dijon, France*
[b] *Department of Biostatistics and Medical Informatics, CHU Dijon, France*
[c] *Institut TELECOM; TELECOM Bretagne; Unité Inserm 650 LaTIM, Brest, France*
[d] *Laboratory Corpuscular Physics, Physics of Particles and Nuclei, University Blaise Pascal, Clermont Ferrand, France*
[e] *Bern University of Applied Sciences et Université de Lausanne, Switzerland*
[f] *Laboratory Medical Image Processing, Faculty of Medicine, Clermont Ferrand, France*
[g] *Smart-IS, Neuilly-sur-Seine, France*
[h] *Ceren Esc Dijon & Département de Biostatistique, Ecole de Santé Publique Liège, Belgium*

Abstract. For more than 20 years, many countries have been trying to set up a standardised medical record at the regional or at the national level. Most of them have not reached this goal, essentially due to two main difficulties related to patient identification and medical records standardisation. Moreover, the issues raised by the centralisation of all gathered medical data have to be tackled particularly in terms of security and privacy. We discuss here the interest of a non-centralised management of medical records which would require a specific procedure that gives to the patient access to his/her distributed medical data, wherever he/she is located.

Keywords. medical record, patient identifier, direct access, data security, privacy, e-health

1. Introduction

For more than 20 years, many research projects have been conducted on a standardised, centralised, secure and reliable medical record (MR) system but have still not met with success. The French DMP project to implement personal MRs for each patient and accessible to the patient is an illustrative example. The DMP has raised many difficulties regarding ethical and legal aspects, the definition of a common identifier and centralised storage of all records. We are not aware of a country who has successfully implemented a standardised, centralised, secured, privacy-compliant and reliable medical system record at the national level. Thus it is time to develop a new strategy based on a pragmatic, secure non-centralised, unstructured MR system which will be operational in a very short term. The main goal of this article is to promote this non-centralised and non-standardised MR system based on original search and access

[1] Corresponding Author: Prof. Catherine QUANTIN, Service de Biostatistique et d'Informatique Médicale, CHU Dijon, BP 77908, DIJON CEDEX; E-mail: catherine.quantin@chu-dijon.fr.

to distributed medical data like the one that exists in Israel (Clalit HMO and government hospitals), Pittsburg (Pennsylvania – UPMC) [1] and is being implemented in Brussels (IRIS hospitals) [2] and Franche Comte, France (EMOSYST) [3]. In these examples, all focusing on the sharing of medical data, MRs are not standardised but can be structured or unstructured. However, sharing of medical data is standardised and structured.

2. Planned Standardised MR System: The Reasons of the Failure and the Dangers of Centralisation

The main reasons for the failure are related first to insufficient human and financial resources, second to the lack of or failure to properly deploy a unique patient identifier (UPI), third to the lack of standardisation or structuration of the MRs.

Many solutions concerning these aspects are developed to provide (for example an Enterprise Master Patient Index) and standards have been proposed [4]. In practice harmonisation of patient identification is very difficult to achieve in many countries, and re-indexing of previously stored old medical data has to be managed. Facing these national difficulties, the current strategy at the European level, is more to let each country define its own identification policy and to encourage national information systems interoperability. As a consequence, a pragmatic solution, relying on existing data and not requiring a UPI, seems to be more appropriate at the European level. The approach of the new DMP project in France, using a UPI to be implemented immediately, is a progress in this regard.

Regarding standardisation and structuration of the MR system, a lot of time has been wasted to define a unique format for all doctors and all pathologies. The only domain where real harmonisation has been obtained is "coding", as with the Systematised Nomenclature of Medicine clinical terms (SNOMED), terminology widely accepted but at the beginning of its implementation or with the International Classification of Diseases (ICD) used for assessing hospital activities. Even, if ICD codes are now included within MRs to record health-care establishment's activities, they are not being used for the daily management of patients' MRs in all European countries. The same remark can be made regarding the patients' drug treatments, which is key information, and for which there is the recognised International Common Denomination (ICoD) used by the pharmaceutical industry.

The dangers of centralising the standardised MRs can be summarised mainly on drawbacks and management of access difficulties. For many years, the public authorities have understood the danger of a centralised system, notably the considerable risk of losing all of the data if the centralised organisation is destroyed. After realising the weaknesses of a centralised system, the USA ministry of defence created in 1969 the ARPANET, a network system that would continue to function in the case of a catastrophe. The USA has accepted the idea that a network has the advantage of being able to preserve functioning structures, even after major destruction, and that new systems could be built on the remains of damaged ones. Concerning health data, it would also be safer to store it in different places to ensure protection of both privacy and information. Furthermore, hackers may see a centralised system as a challenge and try to gain access to the central patient MR system and modify patients' medical information. It could also be a target for terrorists who wish to destabilise a country by pirating its health system and divulging health information on citizens.

Secure management of access for a centralised system will be very difficult to obtain. In addition, it raises problems related to access rights, rights to read, to write or modify data related to the patient. In a decentralised system, a doctor who has made the effort to reconstitute and synthesise his patient's medical history will not need to connect to a centralised system for every consultation but only to update the patient's records, if desired.

3. The Alternative: Decentralised Management of MRs

3.1. Proposal for a Secure « Google Like » Access

Today, the main problem for health professionals or patients who want to have full access to medical information, is that this information is very often spread over many medical records kept by different health structures or professionals. Therefore, it would be convenient for the patient, after identification and authentication, to be able to use a medical search engine to gain access to the medical information that has been selected by the medical practitioner (i.e., suitable for viewing by the patient) wherever it has been stored. The patient can also authorize other medical practitioners (for example if they meet for the first time) to consult his/her information.

First, generally speaking, in industrialised countries each health-care structure whatever the type (public or private) has an information system that gathers structured or unstructured computerised medical records. Secondly, information contained in the routine daily MR is sufficient for the needs of health professionals. Thus, the additional work a doctor needs to do to reconstitute a patient's medical history (MH) is limited even if some patients frequently consult in different places. Doctors therefore have this extra workload only occasionally. Given the two previous points, and the dangers and complexity of a centralised system, it seems reasonable to us to set up a system that allows each doctor, once the consent of the patient has been obtained, to collect information on that patient from the different health structures. The doctor will then have to synthesise the patient's MH for his personal use, save it in his personal information system site, and update it regularly. This effort to synthesise MRs will be reduced because one doctor can pass on information about his patients to other doctors in case the patient moves. For example, the General Practitioner could summarize the patient's MH which could be accessed by his/her colleagues when necessary, and with the patient's consent.

The main organisational advantage is that it could be operational rapidly because problems of harmonisation will be reduced and information will be more secure. The decentralised management principle supposes that the saved MR will remain in its unmodified form in terms of content and structure in hospitals and clinics, and will remain identifiable by certain elements that exist in all patients' MRs such as first names, last names and dates of birth, and require no complementary indexation. When patients or doctors want to gain access to medical data that are distributed among the servers of various hospitals or clinics, they have to be connected to an electronic server on which they identify themselves. In the case of access by a doctor, at the first connection, the patient must be present so as to give his/her consent. This first connection will be made using the doctor's professional card with a password. In the future, authentication could be ensured by using a professional identity or national identity card based on cryptographic methods. The system would transform the

patient's identity using a cryptographic algorithm [5, 6]. This transformation is only done temporarily, in order to link patient information stored in the different health structures. There is no creation of a Unique Patient Identifier. The aim of this algorithm is to obtain a strictly anonymous code, but always the same one for a given individual in order to link all the information concerning the same patient. It would not be possible for the management system to read directly in the memories of the local information system. All of the information would be gathered at the level of the decentralised management system which transfers it to the doctor. The interest of this approach is that it protects the confidentiality of the patient's identity, particularly during transfer in the network. Only encrypted medical information would be moved. However, to go further about data security, questions must be answered on how to verify that information is reliable and on how to trace data after several copies have been made or when the data come from outside the system. Data reliability relies on proof of information integrity, of its origins and that it belongs to one patient. Though most standards provide for such proof for one transmission, continuity of protection through several transactions is not guaranteed. Hackers who disrupt the confidentiality chain have to be identified and prosecuted.

3.2. Grid Technology for Distributed Medical Data Management

Providing patients with "Google-like" secure access to their medical records requires the information to be available for querying and retrieval. Google is able to query and search for any data published on the Internet. However, it will be absolutely necessary to ensure the security of this Internet environment before storing any medical data on it. An alternative is provided by grid technology which allows distributed data to be queried securely according to personal access rights. Grids are defined as fully distributed, dynamically reconfigurable, scalable and autonomous infrastructures to provide location independent, pervasive, reliable, secure and efficient access to a coordinated set of services encapsulating and virtualising resource. Their relevance for managing medical information has been investigated within the framework of the HealthGrid initiative. Some platforms in medical data management [7], management of paediatric data [8] or medical radiography data [9] already benefit from grid technologies to manage medical data securely thanks to dedicated grid middleware services such as MDM [10] or Globus Medicus [7]. The use of grids overcomes the difficulties inherent in a centralized storage system, especially high cost and complexity. Grids also make it possible to store data where or very close to where they are produced. Through grid authentication, authorization and accounting, only duly authorized persons can gain access to data which are encrypted and made anonymous when they are transmitted [11].

Well-identified areas of relevance of the grid paradigm are epidemiology and computer-intensive analysis of geographically distributed medical images. Epidemiology focused on population-level research requires access to distributed, critically sensitive and heterogeneous data, resulting in overall costly computing processes. Users ought to be able to take it for granted that the security mechanisms are sufficient to protect their data; that the results of their research will be private and available to third parties only if designated; that the system will meet the concerns of the ethical and legal committees of their research institutions; that the services are reliable, efficient and permanent; that they do not have to change significantly their current procedures; protocols or workflow, and finally that the data is somehow

automatically organised and gathered, and thus available for further exploitation. Early attempts at epidemiological applications of grids [12] have demonstrated their relevance for patient customized research, such as cancer surveillance.

Another attractive field of application for grid technology is computer-intensive analysis of distributed medical images. The impact of grid technology comes from the secure management of distributed images together with the capacity to gain access to large computing resources on demand to analyze them. In the field of oncology, the use of Computer-Aided Detection (CAD) for the analysis of mammograms was addressed by the MammoGrid project as early as 2005 [9]. Other efforts focus on using grid computing resources to plan radiotherapy treatment [13].

4. Conclusion

The main reasons for the failure of an MRs-centralised management are related not only to insufficient human and financial resources but also to the lack of the MRs standardisation. In this paper, we have discussed the interest of a pragmatic solution relying on existing data. The collection of information should then be possible by setting up a decentralised MR and a search system for distributed patient data. We also have illustrated the potential of grid technology for medical data record sharing the deployment of such technology needs to be coupled with relevant security measures and mechanisms.

References

[1] Martich, G.D., Worrall, T. (2008) Interoperability platforms: Bringing intelligence to healthcare data. *Hospital Information & Technology Europe* Autumn 1(3):65.
[2] eHealth Europe (2008) Belgium Hospitals Use dbMotion for Interoperability eHealth Europe, 7 juillet 2008, http://www.ehealtheurope.net/News/3921/belgium_hospitals_use_dbmotion_for_interoperability.
[3] Leavy, P. (2008) Israeli vendor sees telecom contract as foothold in French market. *Healthcare IT News.eu*, Thursday, 5 June, http://healthcareitnews.eu/content/view/1050/40/.
[4] Global IHE Standards-Based Profiles Adopted by Several National and Regional Projects, www.ihe.net.
[5] Faldum, A., Pommerening, K. (2005) An optimal code for patient identifiers. *Computer Methods and Programs in Biomedicine* 79:81–88.
[6] Quantin, C., Coatrieux, G., Fassa, M., Allaert, F.A. (2009) A cryptographic research engine for the management of distributed medical records. IMIA/WG4 SiHIS CoMHI 2009, Hiroshima, (submitted).
[7] Erberich, S.G., Silverstein, J.C., Chervenak, A., Schuler, R., Nelson, M.D., Kesselman, C. (2007) Globus MEDICUS – Federation of DICOM medical imaging devices into healthcare grids. *Studies in Health Technology and Informatics* 126:269–278.
[8] Freund, J., Comaniciu, D., Ioannis, Y. et al. (2007) Health-e-child: An integrated biomedical platform for grid-based paediatrics. In *Proceedings the 4th HealthGrid International Conference (HG'06)*, Valencia, Spain, *Studies in Health Technology and Informatics* 120:259–270.
[9] Warren, R., Solomonides, T., del Frate, C., Warsi, I., Ding, J., Odeh, M. et al. (2007) Mammogrid – A prototype distributed mammographic database for Europe. *Clinical Radiology* 62(11):1044–1051.
[10] Montagnat, J., Jouvenot, D., Pera, C. et al. (2006) Bridging clinical information systems and grid middleware: A Medical Data Manager. *Studies in Health Technology and Informatics* 120:14–24.
[11] Mohammed, Y., Sax, U., Viezens, F., Rienhoff, O. (2007) Shortcomings of current grid middlewares regarding privacy in HealthGrids. *Studies in Health Technology and Informatics* 126:322–329.
[12] Blanquer, I., Hernández, V. (2005) The grid as a healthcare provision tool. *Methods of Information in Medicine* 44:144–148.
[13] Benkner, S., Berti, G., Engelbrecht, G., Fingberg, J., Kohring, G., Middleton, S.E., Schmidt, R. (2004) GEMSS: Grid-infrastructure for medical service provision. *HealthGRID 2004*, Clermont-Ferrand, France, http://eprints.ecs.soton.ac.uk/8934/1/healthgrid2004inf.pdf.