Giving patients secure ” google-like ” access to their medical record

Catherine Quantin, Maniane Fassa, Gouenou Coatrieux, Vincent Breton, Jean-Yves Boire, François-André Allaert

Giving patients secure « google-like » access to their medical record.

Catherine QUANTIN [a], Maniane FASSA[a], Gouenou COATRIEUX[b], Vincent BRETON [c], Jean Yves BOIRE[d], François André ALLAERT[e]

a. Dpt. of Biostatistics & Medical Informatics, Inserm U866, CHU de Dijon
b. Inserm U650, LaTIM; GET ENST Bretagne, Dpt. ITI
c. LPC, UMR CNRS-IN2P3 Université Blaise Pascal, Clermont Ferrand
d. ERIM-ERI 14 INSERM, Faculté de Médecine, Clermont Ferrand
e. Ceren Esc Dijon & Department of Public Health, McGill University, Montreal, Canada

Abstract: The main problem for the patient who wants to have access to all of the information about his health is that this information is very often spread over many medical records. Therefore, it would be convenient for the patient, after being identified and authenticated, to use a kind of specific medical search engine as one part of the solution to this main problem. The principal objective is for the patient to have access to his or her medical information at anytime and wherever it has been stored. This proposal for secure "Google Like" access requires the addition of different conditions: very strict identity checks using cryptographic techniques such as those planned for the electronic signature, which will not only ensure authentication of the patient and integrity of the file, but also protection of the confidentiality and access follow-up. The electronic medical record must also be electronically signed by the practitioner in order to provide evidence that he has given his agreement and accepted responsibility for the content. This electronic signature also prevents any kind of post-transmission falsification. New advances in technology make it possible to envisage access to medical records anywhere and anytime, thanks to Grid and watermarking methodologies.

Keywords: data security, electronic signature, direct access, medical record, patient identifier, watermarking, grid

Introduction

Throughout Europe, patients are entitled to have direct access to their medical records and this has been true, even in France where previously only indirect access via a physician was allowed, since 4 March 2002. At present, the simplest solution is to give patients a copy of their paper medical record or, if it has been computerised, to give them a printed record or even a copy on a machine readable storage medium. This arrangement of the communication process can be carried out “without constraint at reasonable intervals and without excessive delay or expense” as required by article 12 of the Directive “On the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data” [1]. The time taken to grant access provides the opportunity to ensure that the identity of the individual making the request can be properly authenticated and that any additional conditions on access, such as those provided for in article 13 section 1(g) “for the protection of the Data Subject or

the rights and freedoms of others" have been correctly observed. This current approach does not involve any particular risk to the information system, but there are already pressing demands from patients with their increasingly powerful computing facilities to speed up these processes, and to have direct access to medical record systems. These pressures will be difficult to resist in the present, fast moving, electronic environment and it is difficult to imagine that the traditional, delayed, process will be accepted for much longer. Soon, patients will be expecting to have direct access to their medical files via the internet or its equivalent. Instead of trying to resist this inescapable evolution, it is preferable to seek solutions that provide safety for both patients and medical record systems while allowing this valuable development in the area of personal freedom and human rights.
The French project to implement personal medical records called DMP for each patient and accessible to the patient has raised many difficulties such as defining a common identifier for all health care purposes and structures and centralizing storage of all records. The French health authorities are today redefining the scope of their project taking into account the results of the first experimentation in day-to-day practice. The proposed solution of "google-like" management (providing patients with permanent access to their medical information wherever it has been stored) is an alternative to centralised storage but needs a very high level of security. This paper sets out to define steps in the process of creating a system, similar to a search engine, that will provide patients with secure access to their medical records.

1. Proposal for Secure « Google Like » Access

Today, the main problem for the patient who wants to have full access to his or her health information is that this information is very often spread over many medical records kept by different health structures or professionals that even the patient doesn't remember anymore. Therefore, it would be convenient for the patient, and for his medical practitioner, after being identified and authenticated, to use a kind of specific medical search engine to gain access to the medical information of the patient wherever it has been stored. To provide this access, there are many possibilities. Our proposal relies on two procedures. In the first, the patient authorizes his/her medical practitioner to have access to his/her medical information. As happened in France for the Personal Medical Record (DMP) project, the issue of access to sensitive information (such as HIV, psychiatric diseases, sexual abuses) may be raised. In the second, the patient has direct access to his/her medical data and selects the information that he wants to communicate to his medical practitioner, so that there is no need for the patient to ask for sensitive information to be masked.
In a utopian world, access could be linked to a procedure ideally using a digital signature provided by a patient's medical smart card. More basically, it could be sufficient to incorporate in this secure "google-like" access, the same process of security that has been incorporated in our credit card and that we use daily when we want to have access to our bank account or withdraw money. The main difference with the banking system will be the need for card and access management in order to make it impossible for healthcare information networks to be organised in such a way that the patient is obliged to stay in the network if he wants to keep his "on line" access to his medical record. This risk does not exist in countries where medicine is managed

exclusively by public organisations, but information management may be an important issue when different private healthcare providers compete.

2. Conditions of implementation

2.1 Authentication of patients and health professionals before access to medical records on line

Direct access to medical files via electronic media gives rise to many difficulties, and hence very strict access control and authentication measures are essential. The principal difficulty in this field is to ensure that only the holder of the access rights will be able to gain access to the Personal Data. Access control for patients is considerably more complex than for health professionals. For example, in hospitals, the management can encourage administrative and medical staff to participate in relevant training courses. In contrast, patients would have to be provided with intuitive, foolproof access facilities, without requiring them to participate in any training courses. The difference between facilities designed for "doctor or nurse" access and facilities designed for "patient or general public" access is substantial even though the number of applications and functions available to the patient would, of course, be far smaller than that available to and required by members of staff.

A brief consideration of the risks associated with unlawful access to Medical Record systems for patients and the healthcare organization makes it clear that a very reliable authentication system will be required before allowing any public access to such systems. The traditional approach for the authentication of individuals has two components: assertion of identity, followed by proof of the identity [1]. Generally, this proof can be in terms of something that the individual knows or something that the individual has or something that the individual is. Technical solutions are available to cover any degree of proof in authenticating individuals, but many of them would require the establishment of a substantial organization before they could become effective.

Biometric technologies are sometimes proposed as a way to associate a patient with his or her medical data, as they do not require the patient to bring any documents or remember any information. Though this technology represents real progress both in the identification and in the authentication of the patient, there are still many questions [2] regarding the accuracy and reliability of each biometric technology and the associated costs. But the main problem lies in the acceptability of such systems by organizations concerned with ethical considerations such as patients' associations, national ethics committees, human rights associations, and national committees for data protection. For example, in France, the use of biometric solutions for identification in the field of health has not been approved by the National Ethics Committee.

Even today, after extensive computerization of Medical Record systems, the simplest and most common authentication mechanism is still that of an "Identifier" together with a "Password". This approach combines simplicity of use and management, but it is the weakest and the most unsatisfactory mechanism [3]. The most satisfactory approach would lie in the creation of an individual chip card, including the electronic signature cryptographic algorithms [4], both for patients and health professionals. But this will take some time and will engender considerable expenditure before becoming the accepted standard. Moreover, due to the legal recognition of the electronic

signature, this partial solution would provide access follow-up, with legal value of proof in front of the courts. However, as this more satisfactory electronic solution cannot be implemented now and everywhere, only inferior less safe solutions can be considered. For example, the electronic signature has just been retained in France for the access of health care professionals, but due to technical aspects the implementation of this electronic signature has been scheduled for a period of 3 years (French decree on confidentiality dated May, 15th, 2007).
Meanwhile, a possible solution is a smart card [5-7], associated with the attribution of a secret PIN code with 8 characters, like that used in France for the DMP project. This solution would require hospitals to be equipped with powerful firewall-type data-processing devices to filter access. In such a system, the patient commonly declares the list of medical practitioners who are authorized to have permanent access to his medical data. The access rights given to the medical practitioners can be erased at any time by the patient. For other medical practitioners consulted by the patient, the patient authorizes temporary access.

In the case of an emergency, when the patient is unable to express his will, the easiest solution is to provide access through a specific procedure involving the responsibility of the medical practitioner in charge of the patient, with immediate notification to an official security supervisor. People may argue against this solution as even though the medical practitioner can be prosecuted in case of illegal access, security has been breached. This partial solution represents a compromise between security rules and the patient's health care and arises from the fact that collected data is made available. It is a general principle of penal law to consider that citizens generally act in accordance with social rules and that penalties are imposed as a deterrent and to punish those who break the law.

2.2 Verification of the data source

2.2.1 Regarding the patient

Recently, watermarking has been proposed for the protection of medical information. Basically, watermarking is defined as the invisible embedding or insertion of a message in a host document, for example an image. Watermarking provides an original way to share a document with some ancillary data like protection data or meta-data. For example, with regard to images, watermarked data remains attached at the signal level independently of the image file format. It means that embedded data can be recovered after file format conversion.
Most of the work on watermarking for medical images has concerned the need to verify image integrity (embedding a digital signature of the image) or improve confidentiality [8], as it is often considered that embedding information makes it more difficult for unauthorized persons to gain access to this information. Watermarking appears to be complementary to other security mechanisms. It gives access to a kind of communication channel that is transparent to non-compliant systems, as it is not an extra header information addition, while compliant systems will be able to read embedded data.
In the considered framework, access to or sharing of an isolated medical document requires that the document can be identified. A watermarked authentication code may

allow identification of the health professional who consulted the patient data for the purpose of traceability, or the identification of the patient him or herself. To go further, if the embedded identity is rendered anonymous [9], then it is possible to gain access to and link information concerning the same patient without knowing his or her identity so as to guarantee both privacy and interoperability. These patient privacy issues may appear during the verification process, which is necessary to reduce the risk of errors when identifying documents in everyday practice or when sending a patient's Electronic Health Record. For example, the verifier may be able gain access to patient data without authorization. This method may also provide a solution to the problem of the identification of lost medical documents. Further research and development is necessary to extend watermarking methodology to text.

2.2.2 Regarding the health practitioner

The medical record transmitted to the patients must be electronically signed by the practitioner to be sure that he has given his agreement and that no unauthorized modifications have been made. Here also, the recognition of the legal value of the electronic signature permits controlled electronic transmission of the medical record to the patient. This electronic signature also makes it possible to ensure that any modifications of the medical record, for example, adding new medical information, are made by the medical practitioner.

2.3 Data accessibility

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 all data published on the Internet. But, it will be absolutely necessary to ensure the security of this Internet environment before storing any medical data. An alternative is provided by grid technology which allows distributed data to be stored securely. This data can be consulted and queried according to personal access rights. Grids are defined as a fully distributed, dynamically reconfigurable, scalable and autonomous infrastructure 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 [10], [11],[12],[13],[14]. 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 [15].

2.4 Technology against ethics and law: the limits of liability.

Even if grid methodology allows us to solve the most important part of the problem concerning secure access of the patient to his or her medical record by embedding a strong identification marker in the document through watermarking, two main dangers still exist. The first lies in the fact that this process of "automatic" access is not accompanied by any medical explanation and even more importantly, there will be no medical warning about the contents that the patient will read. It is by no means certain

that providing patients with routine direct access to their medical records automatically extracted from the database is a very satisfactory solution from a medical point of view. If the medical records contain information which may cause serious psychological distress (possibly leading to suicide), the hospital or the medical practitioner could be held responsible from a legal point of view or at least from an ethical or deontological point of view. Moreover, the contents of the medical record also need to be conscientiously reviewed (updated or validated) before being delivered to patients. In other cases, information contained in a medical record may refer to third persons, and divulging such information may be considered a breach of confidentiality. Once again, the hospital or the practitioner may be held legally responsible. Therefore, even though providing patients with automatic access to their medical records appears to be satisfactory from a technical and data-security point of view, it may not fulfil the quality requirements for the security of healthcare information. No transmission should be allowed without the consent of the medical practitioner who takes care of the patient, or his representative. As the practitioner is legally responsible, his formal agreement to the transmission is required, and the transmitted document should be electronically signed by him.

The second point lies in the use of the medical record by the patient. As patients are deemed to be responsible adults, we will not consider the eventual unexpected effects of the communication of their medical records to their insurance company or bank, which may have required it officially or unofficially. From a medical point of view, the main problem could come from modifications of the medical record by the patient himself to erase information that prevents him from obtaining certain advantages. If such modifications were possible, imagine what could happen if a patient erased the fact that he was epileptic in order to be allowed to drive a machine of some kind. Thus, it does not seem desirable to give direct access to the system that manages the files to everybody, even authenticated users. The original medical record, which is the means to bring evidence in case of litigation, should be protected from any kind of attempt to modify the information by unauthorised persons. It will then be preferable to envisage a request procedure for access, including the search for the file and the extraction of the communicable documents authorized by the law. This approach, in which a special access file is created, could happen much faster than the time delay allowed in some European countries (in the UK the authorities have 40 days to comply with a Subject's Access request, whereas in France, the delay is 8 days).

Conclusion

Thanks to advances in technology it is now possible to envisage access to medical records via the Internet anywhere and anytime, thanks to Grid and watermarking methodologies. Electronic access will require very strict identity checks using cryptographic techniques such as those planned for the electronic signature, which will ensure the protection of confidentiality, the integrity of the files, the authentication of the applicant's identity and access follow-up. The electronic medical record must also be electronically signed by the practitioner in order to provide evidence that he has given his agreement and has accepted responsibility, and to prevent any kind of post-transmission falsification of the record. Currently, the idea that every citizen will have an electronic signature allowing him to have direct access to his medical records anywhere appears to be Utopian, but this is the implication of much of the work that is

going on world-wide in e-Government, e-Health and e-Shopping. With regard to search engines, who could have imagined ten years ago that a system would be able to retrieve everything you have ever published and list all of the people who have made a reference to it in a matter of seconds!

Acknowledgements

This research was supported by The French National Agency for Research (ANR).

References

[1] Allaert FA, Le Teuff G, Quantin C. Law and standards faced to market rules in health information security. Stud Health Technol Inform, 2003; 95:125-9.
[2] Vaclav M, Zdenek R. Biometric authentication systems. A technical report. Retrieved April 15, 2006 from ecom-monitor.com web site: http://www.ecom-monitor.com/papers/biometricsTR2000.pdf
[3] Chao HM, Twu SH, Hsu CM. A patient-identity security mechanism for electronic medical records during transit and a rest. Medical Informatics and the Internet in Medicine. September 2005;30(3):227-240.
[4] Allaert FA, Le Teuff G, Quantin C, Barber B. The legal acknowledgement of the electronic signature : a key for a secure direct access of patients to heir computerised medical record. International Journal of Medical Informatics 2004;73:239-42.
[5] Roger France FH, De Clercq E, Bangels SM. Purposes of health identification cards in Belgium – EFMI, European Federation for Medical Informatics, IOS Press, 2005, Connecting Medical Informatics and Bio-Informatics.
[6] Pharow P, Blobel B. eHealth Competence Center, Regensburg, Germany. peter.pharow@ehealth-cc.de Benefits and weaknesses of health cards used in health information systems. Stud Health Technol Inform. 2006;124:320-5.
[7] Pharow P, Blobel B. Fraunhofer Institute for Integrated Circuits IIS, Erlangen, Germany. Security infrastructure requirements for electronic health cards communication. Stud Health Technol Inform. 2005;116:403-8.
[8] Coatrieux G., Lecornu L., Sankur B., Roux C. A Review of Image Watermarking Applications in Healthcare, IEEE-EMBC06, Sept. 2006, New York, USA.
[9] Quantin C, Cohen O, Riandey B, Allaert FA. Unique patient concept : a key choice for European epidemiology. International Journal of Medical Informatics, 2007;76:419-426.
[10] V. Breton, K. Dean and T. Solomonides, editors on behalf of the Healthgrid White Paper collaboration,"The Healthgrid White Paper", Proceedings of Healthgrid conference, Studies in Health Technology and Informatics, IOS Press, Vol 112, 2005.
[11] Vincent Breton, Kevin Dean, Tony Solomonides The Healthgrid White Paper, Studies in Health Technology and Informatics, Vol 112 (2005) 249-321
[12] Olive M, Rahmouni H, Solomonides T, Breton V, Legré Y, Blanquer I, Hernandez V. SHARE, from vision to road map: technical steps. Medinfo. 2007;12(Pt 2):1149-53.

[13] Bridging clinical information systems and grid middleware: a Medical Data Manager Montagnat J, Jouvenot D, Pera C, Frohner A, Kunszt P, Koblitz B, Santos N, Loomis C. Stud Health Technol Inform. 2006;120:14-24.
[14] Erberich SG, Silverstein JC, Chervenak A, Schuler R, Nelson MD, Kesselman C. Globus MEDICUS - federation of DICOM medical imaging devices into healthcare Grids. Stud Health Technol Inform. 2007;126:269-78.
[15] Mohammed Y, Sax U, Viezens F, Rienhoff O. Shortcomings of current grid middlewares regarding privacy in HealthGrids. Stud Health Technol Inform. 2007;126:322-9.