Beyond informed consent: practical approaches for managing consent and fine-grained authorization in large-scale electronic medical record systems.

Guido van ’t Noordende, University of Amsterdam, The Netherlands

Paper/talk abstract Computers, Privacy and Data Protection (CPDP), Brussels, 2011.

Drawing on our work on analyzing the security architecture of the Dutch electronic patient record (presented at CPDP 2010 [1]), this paper gives recommendations on how to better protect patient privacy using simple, practical mechanisms that are easily integrateable in clinical practice. The recommended methods improve transparancy and control over sharing of medical information in large-scale electronic medical record systems. They are applicable not just to very large-scale medical record systems, but also to smaller-scale systems.

First of all, the claim that large-scale systems can protect patient information sufficiently over a very large period of time is fundamentally flawed. Especially for longitudinal medical record systems and very large-scale systems, there exists a significant risk that the system will be broken into in one way or another. Design flaws amplify the risk that such intrusions will be exploited with increasing scale of deployment [1]. Furthermore, any system or record may contain errors, the effect of which in the long run -especially when the system’s size and usage grows- are unclear. Earlier work has shown such flaws in, for example, the Dutch EPD system, the german gesundheitskarte [2], and the U.K. NPfIT [3,4] electronic medical record systems. Many reports have shown that medical data leakages occur and that there is an interest to pay for such information. Celebrity records are a real-world example.

It is unreasonable to require that patients trust a large-scale medical record system to protect their information sufficiently if it contains insufficient methods to control which information is shared with whom, or if these methods are invisible to patienst or physicians. An (often well-founded) lack of trust may have significant implications for patient care, since a lack of trust may impact whether patients feel confident to share critical medical information -which they consider confidential and sensitive- with their physicians.

Patients may be hesitant to trust a very large, diverse, and unknown collection of systems and people over which a system is distributed, even if this system is designed by government or deployed strictly within healthcare. Central components of the infrastructure (such as the central ’switching point’ in the Dutch EPD) may be abused by (future) governments or law enforcement officials to obtain health information without having to request this information through a patient’s physician. Alternatively, there exists a risk that insurers or other (commercial) parties can abuse functionality such as the patient portal to *coerce* patients in providing confidential medical information [3]. Finally, the risk of a succesful attack increases as the size of the system -and the time that data remains stored in it- increases. In short, there are valid reasons for patients to want to avoid that sensitive information is shared through -or even referred to by- an electronic medical record system; yet it is becoming harder and harder to prevent that medical data is shared in practice. More and more systems are being developed which facilitate efficient sharing of information between physicians *across* institutions. Often, these systems operate opaquely, out of sight of patients, and even physicians are often not aware of the scale of such systems, or how they work precisely.

While some of the abovementioned risks can be limited by appropriate technical measures, some problems are fundamental, and certain risks are inevitable. Especially, I pose that *invisible* sharing of information by mechanisms ’under the hood’ may give rise to an increased unease of patients and a significant risk of distrust by patients in the ability of their healthcare professionals to keep medical information confidential. This in turn can result in a ligitimate decrease of confidence in healthcare confidentiality. This can have a large societal impact as it may decrease the overall willingness of patients to convey crucial (but embarassing or sensitive) information regarding their health to their physicians.

Mechanisms are required to increase the confidence that there is sufficient control over data dissemination. This confidence is not only required by patients, but also for the healthcare professionals who may be required to use the system. Such mechanisms are important for any system whose distribution goes beyond what patients *expect* as the ’natural’ boundary of data distribution. Natural boundaries for limiting the sharing of medical information are the perimiter of the primary healthcare institution, or the treatment team of the physician(s) with which patients have an agreement (and who they trust), depending on context. If data is shared beyond such natural boundaries, it should be made clear to patients in advance that information is being shared, and what information this is and with whom sharing may take place. And this should be made clear in advance whenever possible. It is imperative that patients as well as physicians stay well-aware of what information is distributed and accessible where - especially if this goes beyond what patients reasonably and intuitively expect to be the natural and necessary use of their data over the course of patient treatment, i.e., beyond the boundary of the health organization and care professionals with whom they have a treatment relationship.

Transparancy and control mechanisms need to be in place whereever any a ’natural’ boundary of data dissemination or usage is crossed.

First, it is imperative to provide **up-front transparency** regarding *what* information is shared with *whom,* at what scale, and for what purpose. The most important of the above keywords is *what,* since the whom and the purpose of data sharing are often clear from context or can be made clear through other means, such as by means of folders or other ways of providing information to patients. Up-front transparency regards *specific* information which is to be shared about a specific patient; a simple way to achieve up-front transparancy is to require physicians to place a second monitor on their desk which shows a ’professional summary’ before this is shared through a distributed medical record system. When shown to patients (and physicians), it becomes clear what information is to be shared. This provides a possibility to correct the information before it is shared, and more importantly, no uncertainty can occur on whether data is shared or not. If applicable, the information or parts thereof can be marked as particularly sensitive if the patient wants this, or patients may indicate that specific information should not be shared at all for privacy reasons. In such cases, the physician may disagree and discuss the need to share the information with the patient, or the information is not registered or additional measures may be taken to protect the information (see below and [5]). In cases where no immediate agreement or consent can take place, technical solutions may be conceived to ensure that the patient is involved in consenting at some point in time [6]. In short, up-front transparancy provides a means to support *explicit* consent for sharing medical information.

Second, it is imperative to **differentiate policies** for authorization in large-scale electronic medical record systems. A one-size-fits all approach to consent and authorization cannot sufficiently protect privacy for more sensitive types of information, since ’general’ mechanisms and policies intended for exchanging information between physicians are not optimized for ’hard’ cases [1]. For some data, such as psychiatric information, more strict policies and access control mechanisms are required. However, it is hard to predict in a general way which information requires a strict authorization regime, as this may differ from case to case.

Since it is not generally possible to define a-priori which specific information may be regarded sensitive by a patient, interaction with patients is required at the time of including some data in a large-scale medical record system, to decide which data is sensitive and which is not, and possibly to decide on how to best protect this information. Up-front transparancy -as indicated above- can allow for the possibility to use a more stringent autorization regimes for more sensitive information, based on the requirements of a patient. Up-front transparancy provides an appropriate means to achieve this. At the same time, the proposed mechanisms allow for increasing the *quality* of the information which is shared, since up-front transparancy provides a possibility (for the patient and the physician) to catch and correct information before it is shared.

Note that it is important to make a distinction between consent (which takes place *before)* and authorization (which takes place *after* information has been registered in a system). It is particularly important to distinguish the two concepts in very large-scale systems. The methods proposed in this paper are mostly related to consent before registering or sharing information in an electronic medical record system; mechanisms for fine-grained autorisation will be described elsewhere.

As a final note, it is important to ensure that physicians and patients can decide on alternative communication mechanisms -in particular compared to large-scale, national or longitudinal dossier systems- depending on the context and sensitivity of information. This aspect is related to differentiation of privacy policies, but it has wider implications since it allows for designing and using systems for a specific purpose, to ensure that appropriate security mechanisms can be chosen instead of general-purpose mechanisms which may be ill-suited for a given purpose.

Summarizing, it is imperative to maintain patient and physician control over the disclosure and dissimination of medical information in large-scale systems. This paper proposed *up-front transparancy* as a simple means to achieve this goal, by allowing for control by patients and physicians over sharing of information before this takes place. These solutions are applicable to any electronic medical record system, from very large-scale longitudinal health record systems such as the Dutch National EPD or the U.K. NPfIT system, to any ’regional’, specialized, or smaller-scale patient record system which is used for sharing medical data beyond what patients expect.

References

1. Guido J. van ’t Noordende, “Security in the Dutch Electronic Patient Record System,” *2nd ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS), ACM CCS, Chicago, Illinois, USA, October 8, 2010. pp. 21-31* (2010).
2. Marcel Winandy, “A Note on Security in the Card Management System of the German E-Health Card,” *Accepted for 3rd Int’l ICST Conf. on Electronic Healthcare for the 21st century (eHealth), Casablanca, Marocco* (2010).
3. R. Anderson, I. Brown, T. Dowty, P. Inglesant, W. Heath, A. Sasse, “Database State,” *Report commissioned by the J. Rowntree Reform Trust, U.K. Available online* (2010).
4. T. Greenhalgh, K. Stramer, T. Bratan, E. Byrne, J. Russell, S. Hinder, H. Potts, “The devil’s in the detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes,” *University College London* (2010).
5. M. D. Ploem, M. Zwaanswijk, F. J. Wiesman, R. A. Verheij, R. D. Friele, J. K. M. Gevers, “Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD: een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners,” *Nivel (Amsterdam, Utrecht)* (2011).
6. Guido van ’t Noordende, “Overview security/privacy EPD,” *http://www.science.uva.nl/ noordend/epd/* (2010).