Controlled Dissemination of Electronic Medical Records

Guido van 't Noordende
University of Amsterdam, The Netherlands

Abstract

Building upon a security analysis of the Dutch electronic patient record system, this paper describes an approach to construct a fully decentralized patient record system, using controlled disclosure of *references* to medical records. This paper identifies several paths that can be used to disclose references. Contrary to many existing national-scale system designs, our approach avoids centralization and ensures that patients (and/or their family doctors) remain implicitly or explicitly in control over the disclosure of their information, keeping the network of healthcare professionals who can access a patient's information to a minimum.

1. Introduction

Healthcare is becoming more and more complex, with an increasing elderly population and increasingly complex diseases and treatments, and with a corresponding increase of specialization of clinics and physicians. As a result, patients are becoming increasingly mobile, and there is an increasing need for mechanisms to exchange medical information between physicans in different organizations in an efficient way. Various attempts were made over the last decade, particularly in Europe, to construct national-scale infrastructures for exchanging electronic medical records between physicians [1, 2, 3, 4]. Security and privacy remain a challenge in all these systems. Most of the risks identified are due to the very large scale and the centralized architecture of these (pull-based) systems.

A centralized architecture may be understandable from the point of view of efficiency and control, from the point of view of managing access in a relatively simple way, and with ease of use from the clinical perspective in mind. However, a centralized infrastructure comes with various inherent security and privacy risks. This paper presents an alternative method to organize pull-based access to medical records using a decentralized approach, where patients or their physicians can control the disclosure of medical data. Access to information "follows the patient". The core idea is to *bootstrap* the network of access using a controllable mechanism, such as push-based messaging or explicit transport of information by patients. This approach minimizes risks by avoiding centralization, yet it allows access to records from any place, if the patient agrees.

We start from the Dutch EPD system to distill the fundamental concepts needed to build a system for controlled disclosure of electronic medical records.

2. The Dutch EPD System

The Dutch EPD was proposed as the mandatory infrastructure to exchange professional medical records in the Netherlands. Professional records are maintained and managed by health professionals, i.e., physicians, about their patients. Most countries mandate that physicians maintain a professional record, sometimes in electronic form. Recently, a proposed law to mandate the EPD was rejected by the Dutch senate, among other things due to privacy concerns [1]; the system may remain in use as a privatized system.

Although the Dutch system is flawed due to its largely centralized design, it is still an interesting starting point for discussion. A characterizing feature of the Dutch EPD system is its partially *decentralized* nature. Records remain under control of physicians in their own systems. Read-only access to patient records is provided through a central *switching point*, which contains a **reference index** per patient, where each reference points to a decentrally stored record of the patient. We call this a source-based approach. The system implements role-based access control. Physicans or their employees can sign requests using a personal smartcard backed by a government PKI. Certificates indicate the profession/specialization and the name of the invoking healthcare professional, and this information is used by the switching point to make central access control decisions.

As a starting point, we summarize some shortcomings of the Dutch EPD system from earlier findings [1]:

- A security breach of the central switching point can lead to retrieval of any patient record in the system, since signatures over requests are not forwarded to the endpoints where the records are requested from. The 'trust model' of the system, as most national

systems, thus depends crucially on reliability and operational security of the central switching point.

- The indices and log files in the central infrastructure contain information about all treatment relationships of a patient. From this data, much can be derived about a patient's medical history, even when the information itself cannot be retrieved. The mere fact that a patient has a record at an oncological center or that a doctor at a rehab clinic looked at a record (as visible in the logs), leaks information about a patient. Information should not be accessible for longer than necessary.
- The system relies on *self-authorization* of physicians; it cannot verify whether a physician is authorized by the patient whose record is retrieved. This makes the system vulnerable to attacks using stolen smartcards (with PIN code) and dependent on the (operational) security of thousands of systems connected to the central switching point.
- The impact of a possible intrusion can be very large due to the scale of the system, containing information about almost any person in a country. Role-based access control (RBAC) will not help much to limit damage, as basic information will usually be accessible from any role. In particular, medication information is probably visible to most or all doctors. Some legal safeguards are proposed, but these will not deter all misuse at the scale of the EPD.

Keeping information confidential in a national system may be difficult. An (implicit) goal of these systems is often that they can provide a complete overview of (summaries of) a patient's medical history. The assumption of completeness may hurt medical privacy and healthcare in unforeseen ways. To name one example, a family doctor may be required to sign a *health declaration* for a patient as part of a protocol for obtaining life insurance – and for this may be implicitly required to scan the patient's national record. When patients become aware of such practice, even if this is only *potential* practice, they may opt-out of the system completely, or become hesitant to share information with their physicians. This defeats the purpose of the system. As another example, think of the potential of 'mining' DNA data for research purposes – a central switching point is ideally situated to implement this –, and then think of the possible implications.

Another often-discussed issue is emergency access to records using a "break the glass" policy. If a "red button" policy – with auditing after the fact as a security measure – would apply to most medical records, this would open up the system for misuse, similar as self-authorization in the Dutch EPD system does. In general, only a limited amount of information should be accessible under any self-authorizing policy, if at all. Designing a complete medical information exchange system around emergency requirements seems misconstrued and – by definition – insecure. Although we do not treat emergency access further in this paper, the concepts described in this paper *can* be used to construct a system (nation-wide or on a stick) for accessing emergency data, – if patients explicitly consent to making such data accessible. Note that information about, e.g., allergies or blood-thinning medication can also be carried quite effectively on a piece of paper in a patient's wallet.

To generalize the above observations, a source-based system seems a good idea, but using a central index, centralized logging, and a uniform, centralized system to provide access to all (historical) information of patients brings various risks. To mitigate these, patients should be able to control *what* goes into the system (by means of flexible consent options), and what information is shared with *which* physicians. This extended abstract is about the latter aspect: controlling disclosure, using simple, intuitive mechanisms.

3. Key Concepts

The most interesting aspect of the Dutch EPD is that it uses references to disparate patient records. In contrast, in the U.K. NPfIT system, records are uploaded to several central databases, from which many people can access these records [2]. In Germany, information is encrypted before information is uploaded to a central infrastructure. This is much more secure in view of attacks on the central infrastructure: information can only be decrypted using a patient smartcard called the *Gesundheitskarte.* However, key management and key escrow are an issue here, as information should not get lost once a smartcard is lost [3]. In both cases, there is the problem of inconsistencies when information is updated. Similar issues can arise when sending information – e.g., hospital discharge letters – using a secure push mechanism (e.g., [5]). Neither of these problems exist when using references, where information is accessed directly from the physician's system.

The concept of a reference is one of the strong points of the Dutch approach. However, storing all references of a patient in a central component and enforcing access control there, is from a privacy and risk management perspective not such a great idea.

This paper proposes a different approach. We *extract* the references from the central switching point, and abolish the central component completely. Instead, we focus on a set of decentralized solutions to transfer

references *explicitly* from the source to the place (e.g., physician, hospital) where access to a record is needed. By explicitly transfering references to the place where they are needed, we can achieve a naturally evolving, flexible, and controllable network of access organized *around a patient.* This in contrast to centralized 'regional' or national-scale systems, which are organized around inflexible and typically ever-growing organizational boundaries. In addition, explicit dissemination of references – with a patient or a family doctor in charge – allows for fine-grained distribution of *specific* references to records to physicians who require them. For example, relating to specific episodes.

4. References and Reference Passing

The idea of reference passing is conceptually simple. References can be passed on paper, on a USB stick or smartcard, through a Personal Health Record (PHR) such as Microsoft HealthVault, by secure email (push messaging, [5]), or even – if necessary and if the patient or physician chooses to put the references there – through a regional or central infrastructure. Note that references have some resemblance to capabilities[1].

This section presents a tentative overview of possible information in a reference. We assume for this section that physicians have PKI-backed smartcards with which they can set up (mutually) authenticated, encrypted connections to servers, possibly over a protected network. However, the approach is by no means limited to such a setup. Indeed, references (or tokens) can be passed on paper, and access could be allowed over the public Internet. Authorization takes place at the source, where the data resides; auditing (logging) of access also takes place there. It is relevant to define an (open) standard which allows for binding references to various transports and different information types. The system should be usable in various contexts – not only in highly developed and well-organized countries such as Holland or France, but also in third world countries, for example. This makes it important to include measures for protecting access which do not specifically depend on, e.g., (patient) smartcards.

References can contain the following:

- **Basic reference content.** The reference should contain sufficient information for a client to locate (and authenticate) the server where the record is, and for the server to locate the appropriate record. Conceptually, think of a reference as a URL to a https web-service, with a specifically formatted document string pointing to the record.
- **Authorization.** Authorization takes place at the source, i.e., in the server that obtains a request. If physicians have smartcards using which they can sign requests, RBAC may be applied based on the client smartcard's certificate, similar to the Dutch system. It would be preferable if patients could somehow authorize physicians explicitly to prevent unauthorized access.
- If patients have PKI-backed smartcards, as they could have in Holland, then a patient could sign a certificate to assert that a given physician is authorized to access a record, over a given timeperiod. An alternative authorization method may be to register a PIN code with a record (to be securely verified at each time of access), or to use a one-time password (a token) as explained below. Note that these mechanisms are non-exclusive.
- **Bound references.** A random number can be included in a reference at generation time, such that it becomes unique. This allows the source to *bind* each requestor (e.g., authorized physician, mandated employee, or ward) to a reference at the time it is first used. This can help limit what in essence amounts to a 'confinement problem' for references. Reference binding is only useful in scenarios such as sending a reference in a referral letter, since a new reference has to be created for each new physician or organization that requires access to a record. For example, in shared regional directories or in chain-of-care situations, unbound references are easier to use.
- A **timeout** ensures that a reference cannot be used longer than necessary. (Physicians may copy information to complete their historical records). After expiry, references can be locally garbage collected.
- **Tokens.** Including a random number in a reference may be useful for authorization. An idea is to have the source generate a token (or have the patient choose a passphrase), that must be included in the reference before the record can be retrieved. A token can be a large random number, or something that a person can remember, depending on the context. The key idea is to pass or carry the token to the physician who has to retrieve the record *separate from the reference*, as a way to authorize the physician.[2]

---

[1] See for example J. Shapiro, "What's a capability, anyway?". http://www.eros-os.org/essays/capintro.html

[2] A Dutch company, ZorgDomein, uses a referral scheme with numbers printed on paper. A doctor has to obtain the number from the patient (e.g., by calling) to complete the referral. However, ZorgDomein does not embed any notion of references to records. An alternative could be where an (incomplete) reference is printed on paper as part of an (open) referral letter, and the patient learns the token by heart. Thanks to Abraham van Eldijk for suggesting this approach.

Fig. 1 shows a few possible means to pass references. For simplicity, we ignore separate token passing. We believe the approach fits well enough with natural concepts (such as physicians emailing collegues, sending referral letters, or patients who take smartcards with them), that it can be used in daily medical practice.

- The patient is in charge of disseminating references. For example, if a patient has a smartcard (or a USB-stick), references can be placed on it by the doctor. If the patient decides to share the information, she can give the USB stick or selected references to another doctor, who can read, copy, and use them (modulo authorization). The patient is in charge of *who* gets the smartcard and thus over who gets to see any references – at all. On smartcards, RBAC may be an option. Depending on implementation, patients may copy or delete their references off their smartcard or USB stick, either as a back-up or to prevent disclosure of certain references.
- Deleting or losing references does not delete the source, so it only impacts *disclosure* of records. References can be reconstructed. In countries where family doctors exist and where a secure infrastructure exists for sending messages, it is likely good practice to send a copy of each reference to the patient's family doctor, who could keep copies of the data and the references, also as a backup.
- References may also be relayed through a patient's (insecure) mailbox, or through a PHR. The patient is – again – in charge of disclosing the references. Note that it may also be possible for patients to retrieve medical records directly when references refer to online patient-accessible records. However, disclosing medical information to patients should only take place on explicit request by the patient, as it is problematic from several perspectives. Coerced access is one of these [2, 1].
- Physicians may also dissiminate (sets of) relevant references directly between each other in the course of treatment. References should not point to huge (collections of) historic records; references should preferably be typed, dated, and correspond to some kind of medical episode.
- If the patient agrees, some references may be placed in a regional or even in a national directory service, which may be accessible to physicians using a suitable access control method – e.g., using a generic RBAC policy, a "red button" policy, or using explicit authorization. Patients may be able to define policies governing reference registration and authorization aspects. In one extreme case, a system functionally identical to the Dutch EPD system may be constructed. However, since references are independent from their carrier, it should be possible to engineer more flexible systems, such that patients can express preferences such as "put references on my smartcard only", or "use only regional directory services, never the national one".

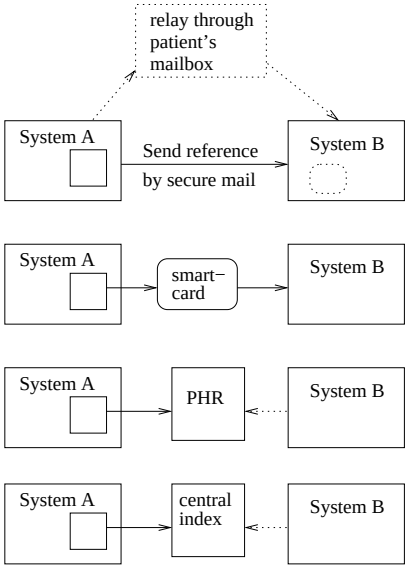

Fig. 1. Different scenarios for passing references.

As an aside, note that in contrast to e.g., the German system, reference usage is completely independent of (patient) key distribution and key escrow mechanisms. Replacement of a (patient's) key thus does not necessarily require replacement of (back-up) references.

References

1. G. van 't Noordende, "Security in the Dutch Electronic Patient Record System," *ACM SPIMACS workshop, Chicago*, (2010).
2. 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).
3. M. Winandy, "A Note on Security in the Card Management System of the German E-Health Card," *3rd ICST Conf. on Electronic Healthcare for the 21st century, Marocco*, (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 Coll. London*, (2010).
5. Direct project, "Secure messaging - project overview," *http://www.directproject.org*, (2011).