A Contactless E-health Information System with Privacy

Aude Plateaux, Patrick Lacharme, Christophe Rosenberger, Kumar Murty

A Contactless E-health Information System with Privacy

Aude Plateaux
BULL SAS, F-78340 LCL, France
ENSICAEN, GREYC, F-14032 Caen, France
aude.plateaux@ensicaen.fr

Patrick Lacharme, Christophe Rosenberger
ENSICAEN, GREYC, F-14032 Caen, France
patrick.lacharme@ensicaen.fr
christophe.rosenberger@ensicaen.fr

Kumar Murty
University of Toronto, Canada
murty@math.toronto.edu

***Abstract*—E-health information systems give rise to many security and privacy concerns. Security of these systems involves a large amount of sensitive data shared by several actors, such as doctors or nurses in various institutions. However, the privacy preserving issue, including data minimization and data sovereignty, is not necessary treated. This paper presents an e-health infrastructure intended to minimize personal data disclosure, with an access to right system based on a secret sharing. We analyze the security of the proposed infrastructure in accordance with medical constraints through contactless transactions.**

***Keywords*-privacy; e-health; secret sharing**

I. Introduction

The development of new technologies such as internet, contactless technologies and databases with sensitive information, have particularly exposed personal data. In this context, many regulations attempt to ensure the security of information systems and the data protection. For instance, the resolution 45/95, adopted by the United Nations General Assembly [Uni90] presents different principles concerning the security of computerized personal data files. More recently, several regulations concerning the protection of personal data and privacy of the user has been created, as the directives of European Union [Eur95], [Eur02], [Eur10]. Privacy requirements are generally related to the three following principles:

1) Data minimization principle: Personal data disclosure should be limited to adequate, relevant and non-excessive data.
2) Data sensitivity principle: sensitive personal data require a major attention and a de-centralized structure for the storage.
3) Data sovereignty principle: Personal data belong to an individual, with an user consent and control on these data.

The case of medical records is particularly concerned by the issue of data protection. These information systems are composed of sensitive data and many actors (doctors, nurses and patients) and several institutions (standard clinics, psychiatric hospital) generate many security and privacy threats. Medical data should be easily available in emergency cases and only to authorized people. Nevertheless, most of publications are centered on the security of e-health information systems and are generally limited to single hospitals without any interaction between them. Minimum disclosure of medical data is partially treated, whereas unlinkability and data sovereignty are marginally developped. Finally, medical files should be encrypted in order to avoid a major disclosure of personal sensitive data. However, this encryption system should take into account an accurate access to control and be developed in accordance with medical constraints.

Our contribution: This article proposes a decentralized architecture for an e-health information system, using contactless communications (for instance, wireless and NFC). This solution provides an efficient privacy-preserving management of medical records, with a new system for the encryption of medical files. The proposed approach is intended to be simple and only uses well known cryptographic tools. More precisely, the Shamir's secret sharing is used and adapted to manage the access rights to patient's records.

Organisation: This paper is organized as follows: in Section II, specific privacy requirements and e-health data protection are presented. Section III explains the e-health information system in a contactless environment. Then, the proposed solution for encryption of medical files is presented in III. The security and privacy analysis of our solution is given in Section V.

II. Privacy and e-health information system

Privacy requirements are numerous in a generic information system. For instance, privacy requirements of Common Criteria are composed of anonymity, pseudonymity, unlinkability and unobservability [ISO09], whereas data minimization is suggested in [PH08]. Generally, the difference between anonymity and pseudonymity is related to a possible revocability of the identity. In exceptional cases, the identity of an user must be recovered by authorized persons. In this case, the use of pseudonyms is better than a total anonymity. For example, an encryption function could be used, reversible by and only by trusted persons knowing the secret key. Thus, a symmetric encryption scheme as the AES algorithm is adapted for the creation of pseudonyms. Moreover, unlinkability notion ensures that personal data (and pseudonyms) are protected against aggregation.

A. Privacy protection in the e-health context

Security and privacy of data medical records is investigated since the mid 90s by Anderson [And02], where several principles on e-health data management were proposed. Specific regulations to the e-health context have been developped, such as the HIPAA for United States (2006, [US 06]), or the recommendation for European Union (1997, [Cou97]). This last recommendation has allowed to define the personal data. These data cover any information related to an identifiable individual. Moreover, the medical data refer to all personal data concerning the health of an individual. Consequently, medical data belong to the patient, who can require his/her own sovereignty on them.

Quantin et al. in [QCF+09] suggest the de-centralized approach for e-health information systems. This solution, combined with the unlinkability principle, gives rise to an identity management based on a local identifier for each patient in each hospital. The aggregation of personal health information is thus prevented. A first solution is the management of these local identifiers by a central trusted authority, with a global table of local identifiers. This authority transfers the required identity from a service to another. However, as the centralized approach, this approach presents problems. Indeed, the identifier table is vulnerable to data removal or disclosure.

These vulnerabilities can be avoided. The identity management shall not store the relationship between different used local identifiers on the database. This solution is proposed by Deng et al. in the context of e-health providers [DDCP09], [DSDC+09]. Nevertheless, access rights are not really taken into account according to the role of the medical employee and no authentication between different hospitals is realized. Moreover, the unlinkability principle involves another problem. Indeed, in their scheme, a doctor requests the local identifier to the identity provider with a patient description. Consequently, these data are linked in a table. The patient description could be an alternative to a global identifier and provides a possibility of aggregation.

Ateniese and Medeiros [ADM02] propose others alternatives in the context of privacy in healthcare in suggesting a group signature scheme. Similarly, De Decker et al [DDLVK08] use privacy preserving credentials. Nevertheless, both schemes require major changes in existing e-health infrastructures.

B. Privacy requirements in e-health information systems

The privacy in medical records is realized according several criteria. Firstly, the use and the collection of data are safeguarded. Then, the anonymity and the unlinkability principle must be ensured. Moreover, the patient has control over their data. Finally, the patient's registers must be de-centralized.

Security requirements: Each medical record requires an access control, with the name of the people or the group of people who may read or modify data. All access must be marked on the record with the name, the date and the time. The access control ensures data confidentiality and data integrity, verifying that only authorized people could access medical records. Moreover, a direct application of the security principle of computarized data files requires encrypted databases. Availability of medical data must be ensured by hospitals and only to authorized medical personal, even if medical data are shared between several healthcare providers.

Medical data minimization: This principle equally provides the anonymity of medical data, including a possible reversibility in emergency cases. Unlinkability property involves effective measures preventing the aggregation of personal health information, inside the hospital and between different e-health providers. Moreover, an accurate access to right policy is used for data minimization. For instance, a doctor can fully access medical information of his/her patients, contrary to a nurse who will have a limited access. In both cases, they do not need to know patient's administrative information, according to the data minimization principle.

Sovereignty of medical records: The doctor creating the medical data or the hospital storing them are not the owners of this information. Indeed, all medical information belongs to the patient. Consequently, patients have control over their data and the access to this information. Moreover, the transfer between two institutions must be realized with his/her consent. Obviously, the emergency scenario, where the life of the patient depends on external information, must take into account. A typical characteristic of an e-health context is the trusted relationship between a doctor and his/her patient. Implicitly, this latter gives the doctor his/her consent to access his/her medical record. Nevertheless, this consent does not concern all the medical records of all institutions. This issue is confirmed by the numerous illegal information flows which have been discovered in the British NHS. Besides, Anderson [And06], [And08] recalls this conflict between the consent of patient and the *need to know* of doctors.

De-centralized system: In many countries, as for the British NHS system, a national database of medical records has been considered in order to improve the availability of medical records. However, strong criticisms of practitioners combined with negative reactions of public opinion have emerged for several reasons. For example, in case of system problem, a complete failure of medical information could be caused by the centralized data. Moreover, a major disclosure of these data would also have a strong national consequence for the privacy of citizens [And06], [And08]. Thus, a direct consequence of the data sensitivity principle is the use of de-centralized systems.

III. Global approach of the e-health architecture

A. Identity management

In the proposed scheme, a Public Key Infrastructure is used. The PKI is a hierarchical infrastructure with one certification authority, depending on the current country. This authority allows the generation and the storage of public/private keys pair. The private key allows to sign the certificates of different hospitals, clinics and other e-health providers H_1,..., H_n. Thus, a trusted communication is created between them. Then, these institutions generates and stores a pair of public/private keys. These latters are used to sign the certificate of each medical employee M_i. Moreover, each medical personnel has a numerical identity (login/password) provided by his e-health provider[1].

In this architecture, the identity derivation service IDS is considered as the trust part, by creating and managing local pseudonyms for the patient from his/her global identifier Gid. This number identifies the patient in all health structure and is used during a transfer of medical records. Gid is a very sensitive data. Consequently, the storage of a table of all patients' global identifiers in a given institution would be very dangerous for the patients' privacy. Thus, instead of store the global identifier, the identity derivation service IDS computes two local identifiers from the patient's global identifier. Two identity controllers are then used to check identities and access rights for data inside the e-health provider and in other institutions. The access controller specific medical information is called MAC (Medical Access Controller), the corresponding administrative data is the AAC (Administrative ccess Controller).

Consequently, in our scheme (see Fig.1), two databases are considered: one for administrative records (first name, last name, civil status, address, phone number,...) and another for medical records. These bases correspond to two local identifiers Lid_1 and Lid_2. At admission to the hospital, the patient may be given a wristband (or contactless smartcard) equipped with a RFID tag. This wristband contains his/her name, first name, his/her Lid_2, used as a pseudonym for the patient in his/her medical records and also one secret point explained in the Section IV.

During the registration phase of a patient P, described in the frame III-A.1, the identity derivation service IDS uses two secret keys K_1 and K_2. Then, it applies the encryption scheme AES to the patient global identifier Gid. The AES is used with K_1 and K_2 in order to respectively compute Lid_1 and Lid_2. The global identifier is deleted to avoid accidental disclosure of this very sensitive information. Moreover,

[1]A secure smart card for medical personnel would increase the security of this authentication. The card could contain the digital certificate of the holder, with the signature of the certification authority.

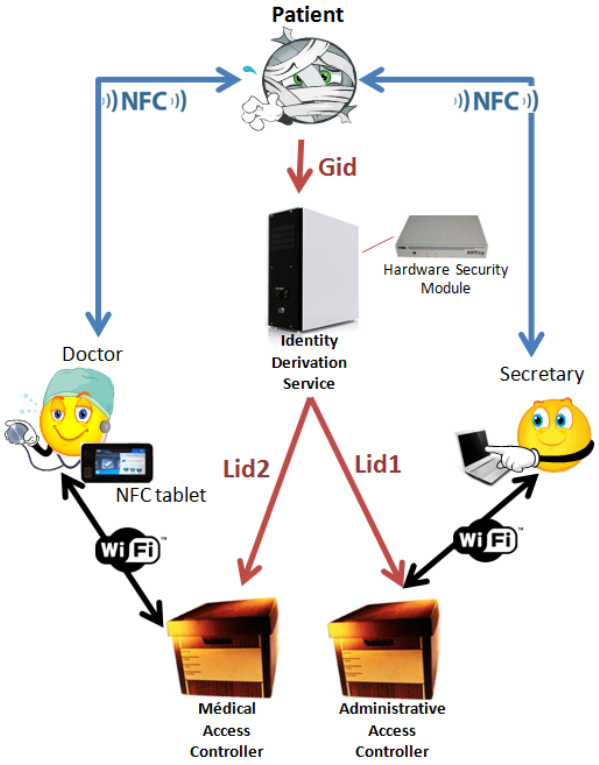

Figure 1. Organization inside an hospital

these keys are managed by the institution, independently of patient global identifiers. Their management must be realized in a secure way and in a secure element, as a Hardware Security Module (HSM). The identity derivation service IDS is the only one able to retrieve the global identifier of the patient with the knowledge of the secret keys K_1 and K_2. Moreover, IDS only computes the local identifiers and has not access data. In addition, in order to avoid the link between medical database and administrative database, the access to data are controlled by AAC or MAC which do respectively not know local identifiers Lid_2 and Lid_1.

III.A.1. Registration phase

1) The patient gives his/her Gid to IDS.
2) IDS uses K_1 and K_2 and computes the local identifiers $Lid_1 = AES_{K_1}(Gid)$ and $Lid_2 = AES_{K_2}(Gid)$.
3) IDS deletes Gid and returns Lid_2 and Lid_1 to the patient.
4) IDS returns Lid_1 and Lid_2 respectively to AAC and MAC.
5) The patient gives his/her Lid_2 to his/her doctor.
6) The doctor adds Lid_2 in his/her list of patients.

During the consultation, the patient presents his/her wristband to the doctor as a proof of his/her consent for the access and the update of his/her medical record by the doctor. The communication between the RFID tag and the doctor's NFC tablet allows the transfer of Lid_2. As a result, the doctor has to maintain a list of his/her patients along with the list of local identifiers in his/her personal tablet. In each consulted service, the patient presents his/her medical wristband. Thus, after check of access controllers, the service could access his/her medical record. The requestor's identity is recorded by the access controllers together with a date and time stamp.

Thus, the doctor's authentication authenticates the doctor to MAC as a doctor affiliated with the hospital. The knowledge of Lid_2 allows MAC to extract the information of the affected patient. The access procedure to medical record is similar for each employee (see Frame III-A.2). However, as detailled in the Section IV, this knowledge is not enough to be considered as the affected patient's physician, and consequently to have access rights.

III.A.2. Access medical data with the local identifier

1) The doctor provides his/her login/password and Lid_2 of his/her patient to MAC.
2) MAC controls the doctor's identity, personal certificate and access rights.
3) MAC accepts or refuses authorization to medical data and replies to the request using Lid_2. The requester's identity, the date and the time are registered.

In emergency case, if the patient is unconscious, an authorized doctor or service needs to access the patient's medical records, the concerned medical personnel gives the patient's identity instead of Lid_1 or Lid_2 (see Frame III-A.3). If the patient is already registered, AAC can retrieve Lid_1 from the patient's identity. Then, IDS retrieves Gid from K_1 and Lid_1, and then Lid_2 from Gid and K_2. Finally, MAC registers the requester's identity, with the date, the time and the type of requested medical information. After the operation, the patient is informed of this process.

III.A.3. Access medical data without the local identifier

1) The doctor provides his/her login/password and an patient's identity, such as the name, to AAC.
2) AAC controls the doctor's identity, the personal certificate and the access rights.
3) AAC retrieves Lid_1 with the patient identity.
4) AAC gives Lid_1 to IDS.
5) IDS computes the patient's Gid with Lid_1 and K_1.
6) IDS computes Lid_2 with Gid and K_2.
7) IDS deletes Gid and gives Lid_2 to MAC.
8) MAC accepts or refuses authorization to the medical record and replies to the corresponding request with Lid_2. The identity of the requester, the date and the time are registered.

B. Data transfer between hospitals

The collaboration between two hospitals or clinics for cross communications of medical records is sometimes required. This collaboration ensures the continuity of the patient's medical treatment and the availability of medical data. The communication must be realized on a secure channel with the consent of the patient (except, of course, in some exceptional cases such as an emergency).

This architecture easily supports this requirement, through the PKI infrastructure and the patient's local identifier. More precisely, an authorized medical personnel, authenticated by his own medical access controller, can request external information. In this case, the identity derivation service recovers the global identifier (without storage) and transfers it to the second hospital, which can retrieves the requested information.

IV. Encryption of databases

In order to access patient's medical records, the employee provides information on his/her rights and on his/her patient. If an employee is authorized, the access controller MAC transfers the requested medical records. However, employees have not the same rights in a hospital. For instance, we can considered the following simplified scheme, described in the table 2: the doctor and the patient can access and complete medical records, whereas the nurse only need access prescriptions and therefore has no right diagnosis.

Actors	Admin. data	Diagnostics	Prescriptions
Patient	X	X	X
Doctor		X	X
Nurse			X
Secretary	X		

Figure 2. Access rights function of actors

In order to manage the employees' access rights in medical institutions, it is necessary to be able to add actors to the systems. Moreover, for practical reasons, the actors must have one unique private key. The principle of Shamir's secret sharing perfectly applies [Sha79]. The idea is to divide the secret into several parts distributed to participants and is based on the fact that n points are enough to define a $(n-1)$-degree polynomial. Thus, in order to find the secret, a certain number of $(n-1)$ points must unite.

During the patient's registration, a $(n-1)$-degree polynomial is attributed to the patient. Thus, in addition to the local identifiers, his/her wristband with RFID tag contained one secret point of this polynomial. Concerning the employees, during the consultation, the patient presents his/her wristband to the employee. Then, a secret point of polynomial is created by the server for this employee. The server must also store $(n-1)$ points of this polynomial. Indeed, if the patient or the employee wants access these

data, the combination of his/her secret point with the $(n-1)$ points of server allows to retrieve the initial polynomial. Thus, the intercept represents the encryption key of medical patient data. Similarly, the decryption of administrative data appeals to the secretary's secret point and the $(n-1)$ server points. The Fig.3 gives an overview of the solution. The cryptographic calculations can be executed inside an HSM or in implementing crypto-processors as explained by Sklavos in [Skl10].

Consequently, the access right checks by AAC and MAC are realized through this protocol. Thus, if a rogue doctor obtains Lid_2 of a patient who he/she does not follow, he/she will not have a point of polynomial. So, he/she does not access the data. Moreover, when he/she accesses data, the history is updated.

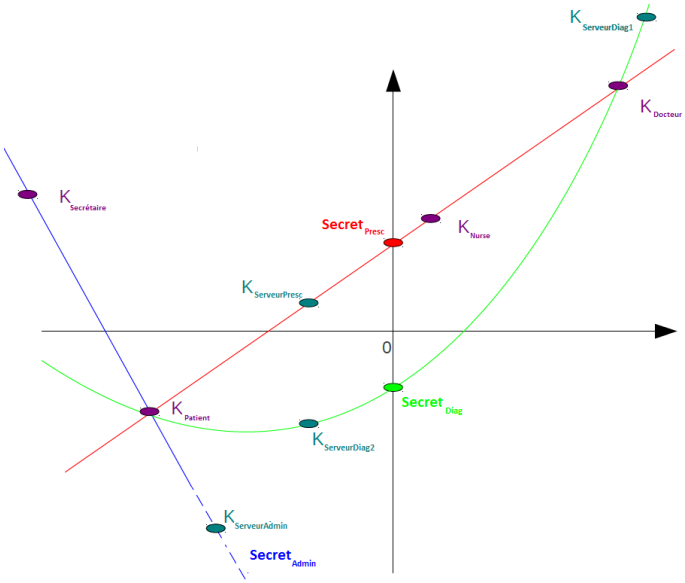

Figure 3. Shamir's secret sharing in a e-health system

As indication, in the administrative file, the name, first name and age must not be encrypted to ensure potential admission to the emergency.

V. Security and Privacy Analysis

A. Security requirements

In order to access patient's data, the medical employee must be authenticate thanks to a classical system of login and password and their certificates. Therefore, only relevant employees can access or update information inside the institution. Moreover, the files of databases, the contactless transactions are encrypted and all exchanges are authenticated. Consequently, the confidentiality and integrity of personal data are ensured by the access controllers. Finally, the medical data can be read in the exceptional emergency case. Thus, the availability of personal data is also respected.

B. Medical data minimization

Firstly, the use of different local identifiers for one patient inside one hospital allows to ensure the anonymity of medical data. Thus, if the contents of the medical records and of the administrative records are stolen, it is not possible to aggregate these information without the knowledge of the secret keys. In the same way, the possession of two medical data files of two different institutions does not allow to bind these information.

Moreover, only the identity derivation service knows the relation between Lid_1, Lid_2 and Gid, and is able to generate them. Reciprocally, the medical access controller accesses to the medical databases, but MAC does not know the link between the local identifiers. Moreover, MAC is not able to access administrative database. The same constraint is observed for administrative access controller. Thus, the distinction between identity manager, controllers and databases allows to ensure the unlinkability principle.

Finally, the use of Shamir's secret sharing manages the access rights and ensures that only relevant information are provided to medical employee. Indeed, each employee has one secret point which allows to find the $(n-1)$-degree polynomial associated with $(n-1)$ points of trust server. Moreover, if the server is damaged, its $(n-1)$ points do not allow to find the sensitive $(n-1)$-degree polynomial. Consequently, the minimization principle is also ensured. Moreover, the proposed access control policy takes into account the modifications of employee's access rights. For instance, if a nurse has not access to patient data, his/her point is deleted. In addition, the points of other members with access rights are recomputed.

C. Sovereignty of medical records

The exchange between the patient and the employee through the patient's wristband and the employee's NFC tablet allows to provide the Lid_2 and to generate a secret point for the employee. The consent of the patient for the access to his medical record is thus realized. Moreover, when an employee accesses to the patient's data, the identity of the employee, the date and the time of the request are registered. Consequently, the data sovereignty principle is ensured and strengthened.

VI. Conclusion

The protection of sensitive medical information in an e-health system is a complex challenge for security and privacy protecting technologies. The proposed solution preserves the privacy of the patient, under strong constraints of the medical system. The access system of encrypted data, based on the Shamir's secret sharing, presents an efficient solution, that could be integrated in existing health infrastructure.

ACKNOWLEDGMENT

The authors would like to thank Coline Migonney for her participation during the section *encryption of database*, as well as the BULL company and the ANRT association for their financial support.

REFERENCES

[ADM02] G Ateniese and B De Medeiros. Anonymous e-prescriptions. In *Workshop on Privacy in the Electronic Society (WPES)*, pages 19–31. ACM, 2002.

[And02] R.J. Anderson. A security policy model for clinical information systems. In *Security and Privacy, 1996.*, pages 30–43, Cambridge, 2002. University of Cambridge Computer Laboratory, IEEE.

[And06] R. Anderson. Under threat: patient confidentiality and nhs computing. *Drugs and Alcohol Today*, 6(4):13–17, 2006.

[And08] R. Anderson. Patient confidentiality and central databases. *Br J Gen Pract*, 58(547):75–76, 2008.

[Cou97] Council of Europe. Recommendation R(97)5 on the protection of medical data, February 1997.

[DDCP09] M. Deng, D. De Cock, and B. Preneel. Towards a cross-context identity management framework in e-health. *Online Information Review*, 33(3):422–442, 2009.

[DDLVK08] B. De Decker, M. Layouni, H. Vangheluwe, and Verslype K. A privacy-preserving ehealth protocol compliant with the belgian healthcare system. In *Public Key Infrastructure*, pages 118–133, 2008.

[DSDC+09] M. Deng, R. Scandariato, D. De Cock, B. Preneel, and W. Joosen. Identity in federated electronic healthcare. In *Wireless Days, 2008. WD'08. 1st IFIP*, pages 1–5. IEEE, 2009.

[Eur95] European Commission. Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, 1995.

[Eur02] European Parliament. Directive 202/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector, 2002.

[Eur10] European Commission. A comprehensive approach on personal data protection in the european union, November 2010.

[Ghi08] D. Ghindici. *Information flow analysis for embedded systems: from practical to theoretical aspects*. PhD thesis, INRIA, Sophia-Antipolis et Univ. Laval, Canada, 2008.

[ISO09] ISO 15408. Common criteria for information technology security evaluation, july 2009.

[PH08] A. Pfitzmann and M. Hansen. Anonymity, unlinkability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology. Technical Report, 2008. v0.31.

[QCF+09] C. Quantin, G. Coatrieux, M. Fassa, V. Breton, D-O Jaquet-Chiffelle, P. De Vlieger, N Lypszyc, J-Y Boire, C. Roux, and F-A Allaert. Centralised versus decentralised management of patients' medical records. In IOS Press, editor, *Medical Informatics in a United and Healthy Europe K.-P. Adlassnig et al. (Eds.)*, 2009.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM 22*, pages 612–613, 1979.

[Skl10] Nicolas Sklavos. On the hardware implementation cost of crypto-processors architectures. *Information Security Journal: A Global Perspective*, 19(2):53–60, 2010.

[Uni90] United Nations. Guidelines for the regulation of computerized personal data files, december 1990.

[US 06] US Department of Health & Human service. Health insurance portability and accountability act, 2006.