# Minimisation des données de e-santé

Aude Plateaux, Patrick Lacharme, Kumar Murty, Christophe Rosenberger

# Minimisation des données de e-santé

Aude Plateaux, Patrick Lacharme, Kumar Murty
et Christophe Rosenberger
prenom.nom@ensicaen.fr, murty@math.toronto.edu

**Résumé**

Les données médicales sont des données personnelles très sensibles qui forment un gigantesque système d'information où de nombreux acteurs sont impliqués. La protection de la vie privée doit se trouver au centre de toutes les politiques de sécurité mises en place dans ce contexte. Cet article présente cette problématique et propose un système assurant la minimisation des données de e-santé à l'aide d'un schéma de partage de clés.

## 1 Introduction

La numérisation des données de santé a commencé depuis de nombreuses années, mais est loin d'être terminée comme l'atteste le lent déploiement du dossier médical personnel (DMP) en France. Si son objectif est avant tout de faciliter l'accès aux informations médicales pour les professionnels de santé traitant l'information, la sécurité et la protection de ces données personnelles est clairement un problème majeur de ce système. Les menaces en termes de sécurité et de vie privée dans les systèmes d'information de e-santé ont par exemple été présentées par R. Anderson dès le milieu des années 90 [And96, And02, And06, And08], et développées régulièrement dans des cadres variés.

Les bases de données médicales centralisées sont particulièrement dangereuses. Même avec un contrôle d'accès adéquat, il est difficile de garantir la sécurité de ces données car les menaces sont variées (attaques informatique, pannes physiques ou erreurs humaines) et leur divulgation aurait un impact extrêmement important pour les utilisateurs. Les données médicales appartiennent au patient et sont sous le contrôle et la protection du médecin traitant (qui les a crée ou non). Le contrôle sur les données médicales et le consentement du patient doivent être prioritaire devant le besoin de connaissance des personnels médicals, excepté dans certains cas d'urgence. Cet article donne un aperçu de la problématique de la protection de la vie privée dans les systèmes d'informations médicales et propose un système de chiffrement compatible avec le principe de minimisation des données et les contraintes du milieu hospitalier, [PL12, PLMR13].

## 2 La protection de la vie privée dans les systèmes de e-santé

La recommandation [Cou97] du conseil de l'Europe de 1997 définit deux expressions importantes dans le domaine de la vie privée au sein d'un système de santé. Ainsi, les *données personnelles* couvrent les informations relatives à une personne identifiable, alors que les *données médicales* se réfèrent à toutes les données personnelles relatives à la santé d'un individu. Par conséquent, ces données appartiennent au patient qui dispose d'un droit d'accès et de rectification sur ces informations. La loi 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé accorde au patient le droit d'accés à toutes les données médicales le concernant [Mis02].

Certaines informations médicales sont extrèmement sensibles et doivent faire l'objet d'un contrôle d'accès particulièrement restrictif, accompagné d'un système de chiffrement. La CNIL préconise notamment l'adoption de mesures de sécurité physique et logique pour le contrôle d'accés aux données médicales, ainsi que leur chiffrement, que ce soit sur un disque dur ou un support mobile [CNI11]. Plusieurs architectures de e-santé s'appuient sur la cryptographie comme les accréditations anonymes ou les signatures de groupe [AM02, DLVV08, DJP12] pour gérer le contrôle d'accès mais ne concernent pas le chiffrement des données. D'autres solutions, faisant appel au chiffrement basé sur l'identité (HIBE) [BCHL09] ou sur les attributs (ABE) [IAP09, LHBC12], demandent des structures complexes. Par ailleurs, l'intégrité et la disponibilité des données de santé est aussi très importante pour des raisons de continuité des soins.

La traditionelle relation de confiance entre un médecin et son patient est différente quand il s'agit de documents numériques. Cette relation donne implicitement au docteur l'accord du malade pour accéder à son dossier médical, mais elle ne donne pas le droit à n'importe quel docteur d'accéder à tous les dossiers. Une première mesure consiste à enregistrer l'accés (lecture ou écriture) à n'importe quelle donnée médicale.

L'utilisation secondaire des données médicales est un autre problème pour la protection de la vie privée [And12]. Ainsi, dans le milieu des années 1990, environ 50% des 500 plus grandes entreprises américaines ont reconnu utiliser les dossiers médicaux lors de l'embauche de leur employés [b95]. Les possibles utilisations secondaires des données médicales (par exemple pour la recherche dans le domaine de la santé) réclament des techniques d'anonymisation bien définies [Kal03, KDTC04]. La CNIL demande ainsi aux professionnels de santé de prendre des mesures pour empêcher que les données médicales ne soient divulguées ou utilisées à des fins détournées. C'est essentiellement pour le domaine de la santé que la CNIL a été amenée à examiner les procédés d'anonymisation des données [CNI].

## 3 Minimisation des données médicales

Un simple chiffrement des données médicales pose un problème en termes de gestion des clés. En effet, plusieurs personnes doivent avoir accès au dossier d'un patient mais pas forcément dans sa totalité. De plus, si chaque dossier doit être chiffré avec une clé différente, cela implique qu'un docteur suivant plusieurs patients doit posséder autant de clés que de dossiers, ce qui n'est pas souhaitable pour des applications pratiques. On considère ici que chaque acteur possède une unique clé de chiffrement stockée, par exemple, sur sa carte professionnelle de santé (CPS).

De manière simplifiée, on considère quatres types d'acteurs : les patients, les docteurs, les infirmières et le personnel administratif. Un médecin peut accéder pleinement aux informations médicales de ses patients alors qu'une infirmière a uniquement accès aux ordonnances. Dans les deux cas, ils n'ont pas besoin de connaître les informations administratives du patient, à l'exception de certaines données comme son âge. La méthode de chiffrement proposée se généralise facilement à d'autre types d'acteurs ou d'autres contraintes si besoin. L'hôpital possède en outre un serveur qui stocke un certain nombre de clés (un par patient et par type de données). De plus, dans une institution médicale, il est nécessaire de pouvoir ajouter facilement des acteurs aux systèmes.

Le système proposé s'appuie sur le principe de partage de secret. Ce partage, proposé par Shamir en 1979, permet de retrouver la clé partagée par interpolation polynomiale [Sha79]. Ce système fait partie de la cryptographie à seuil, dont le but est de diviser le secret en plusieurs parties distribuées à chacun des participants. L'idée est qu'il suffit de $n$ points pour définir un polynôme de degré $n-1$. Ainsi, à partir d'un secret $S$ que l'on code sous forme d'un polynôme $P$ de degré $n-1$, chaque participant $i$ reçoit un point $P(i)$. Le secret est retrouvé si au moins $n$ participants partagent leur information. Ce partage des clés remplit l'ensemble des exigences souhaitées pour notre architecture de gestion de clés.

Le patient, le docteur et l'infirmière doivent donc utiliser leur clé (ici sous forme de point), ainsi que celle(s) du serveur, pour obtenir la clé de déchiffrement des données. En effet, le point d'un des acteurs associé au(x) point(s) du serveur permettent de retrouver l'équation du polynôme. La clé de déchiffrement est alors l'ordonnée à l'origine de celui-ci.

La Figure 1 donne un aperçu de la solution proposée. Ainsi, les prescriptions doivent être accessibles par le patient, l'infirmière et le docteur. Si ces points n'existent pas, on les choisit de façon à ce qu'ils appartiennent à la même droite. Par conséquent, la clé de déchiffrement est cachée dans une équation de degré 1. On choisit alors un point de cette droite qui constituera la clé du serveur. De cette façon, si l'un des 3 acteurs souhaite accéder aux prescriptions, son point ajouté à celui du serveur permettent de retrouver l'équation de degré 1 puis l'ordonnée à l'origine, c'est-à-dire la clé de déchif-

frement des prescriptions. De la même façon, les données administratives doivent être accessibles par la secrétaire et le patient. On dissimule alors la clé de déchiffrement de ces données dans un polynôme de degré 1. Une clé de serveur est également choisit sur la droite correspondante.

Enfin, la clé de déchiffrement des diagnostiques doit pouvoir être retrouvée par le docteur et le patient. Or, la droite relative aux prescriptions passe déjà par ces deux points, ainsi que par le point de l'infirmière qui n'a pas accès aux diagnostiques. Il n'est donc pas possible d'utiliser cette équation pour dissimuler la clé des diagnostiques. Par conséquent, cette dernière doit être cachée dans une équation de degré 2 qui passera uniquement par les points du patient et du docteur. De plus, afin de retrouver cette équation, il est nécessaire de regrouper 3 points. Dans ce cas, le serveur possède 2 autres points relatifs à cette parabole.

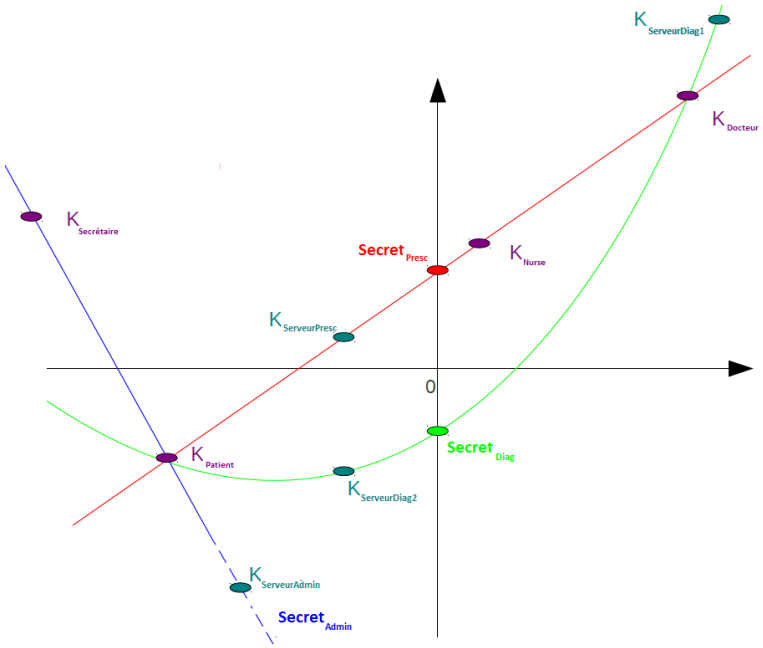


FIGURE 1 – Gestion des clés dans un hôpital par un partage de secret

Ce système permet en outre à un médecin de suivre plusieurs patients différents sans avoir à posséder de clés différentes. Par exemple, une nouvelle droite peut être crée pour chaque nouveau patient, passant par le même docteur, et l'intersection avec l'axe des ordonnées donne la clé de déchiffrement des prescriptions. Dans le cas où un médecin et une infirmière suivent plusieurs patients, on construit alors des paraboles différentes pour chaque patient, avec deux clés de serveur pour chaque parabole.

# 4 Conclusion

Les données de santé sont présentes sur des supports variés où de multiples acteurs entrent en jeu. Ce sont des données extrèmement sensibles au niveau de la vie privée des personnes concernées. Cet article est focalisé sur le stockage des données médicale au sein d'un hôpital et prend en compte le principe de minimisation des données ainsi que les contraintes médicales concernant les données. Celles-ci sont trop sensibles pour être protégées par un simple contrôle d'accés et doivent être chiffrées. La CNIL préconise l'utilisation d'un algorithme de chiffrement robuste comme ceux contenus dans le référentiel général de sécurité de l'ANSSI, mais ne donne pas d'indication sur la gestion des clés.

Le système proposé, basé sur le partage de clé de Shamir, permet de gérer efficacement le chiffrement de telles données. Grâce à ce système, seules les personnes autorisées peuvent obtenir les clés de déchiffrement des données. De plus, cette architecture nécessite le stockage d'une seule clé cryptographique par acteurs, ce qui peut être réalisé facilement à l'aide de la carte professionnelle de santé.

# Références


[AM02] G. Ateniese and B. De Medeiros. Anonymous e-prescriptions. In *ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 19–31, 2002.

[And96] R. Anderson. A security model for clinical information system, 1996.

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

[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.

[And12] R. Anderson. The privacy of our medical records is being sold off, 2012.

[b95] Is your health history anyone's business ?, mccall's magazine, avril 1995, p.54, rapporté par M. Bruce sur usenet newsgroup `comp.society.privacy`.

[BCHL09] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter. Patient controlled encryption : ensuring privacy of electronic medical records. In *ACM workshop on Cloud computing security, (CCSW'09)*, pages 103–114, 2009.

[CNI] CNIL. L'état des lieux en matière de procédés d'anonymisation.

[CNI11] CNIL. Guide professionnels de santé, 2011.

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

[DJP12] N. Dong, H. Jonker, and J. Pang. Formal analysis of privacy in an ehealth protocol. In *ESORICS'12*, volume 7459 of *LNCS*, pages 325–342, 2012.

[DLVV08] B. De Decker, M. Layouni, H. Vangheluwe, and K. Verslype. A privacy-preserving ehealth protocol compliant with the belgian healthcare system. In *EuroPKI'08*, volume 5057 of *LNCS*, pages 118–133, 2008.

[IAP09] L. Ibraimi, M. Asim, and M. Petkovic. Secure management of personal health records by applying attribute-based encryption. In *International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth'09)*, pages 71–74, 2009.

[Kal03] A. A. El Kalam. *Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales*. PhD thesis, Institut National Polytechnique de Toulouse, 2003.

[KDTC04] A. A. El Kalam, Y. Deswarte, G. Trouessin, and E. Cordonnier. Une démarche méthodologique pour l'anonymisation de données personnelles sensibles. In *SSTIC04*, 2004.

[LHBC12] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal. Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *IEEE International Conference on Computer Communications and Networks (ICCCN)*, 2012.

[Mis02] P Mistretta. La loi n 2002-303 du 4 mars 2002, relative aux droits des malades et à la qualité du système de santé. réflexions critiques sur un droit en pleine mutation. *Juris classeur périodique*, pages 1075–1083, 2002.

[PL12] A. Plateaux and P. Lacharme. Organisation d'une architecture de santé respectueuse de la vie privée. In *SARSSI*, 2012.

[PLMR13] A. Plateaux, P. Lacharme, K. Murty, and C. Rosenberger. A contactless e-health information system with privacy. In *IWCMC*, 2013.

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