Protection des données médicales numérisées : questions à Jean-François Parguet et à Philippe Pucheral, propos recueillis par Dominique Chouchan

Jean-François Parguet, Philippe Pucheral

Protection des données

QUESTIONS À JEAN-FRANÇOIS PARGUET

D.R.

Jean-François Parguet est directeur du pôle Référentiels, architecture et sécurité au sein de l'ASIP Santé, dont il est également le responsable de la sécurité des systèmes d'information (RSSI). Depuis une vingtaine d'années, il a exercé diverses responsabilités dans la mise en place de grands systèmes d'information et de leur sécurité, dans le privé ou le public (Steria, Telesystemes, ON-X Consulting, ministère des Finances…).

La maîtrise d'ouvrage du dossier médical personnel (DMP) a été confiée à l'Agence nationale des systèmes d'information partagés de santé (ASIP Santé)*. Quelques enjeux de la dématérialisation des données de santé en bref.

La fin de cette année verra la concrétisation du projet de DMP. De quoi s'agit-il ?

Jean-François Parguet : Les informations de santé font partie des dernières à être dématérialisées, c'est-à-dire accessibles sous forme numérique. Ce n'est pas un hasard : il s'agit d'un domaine sensible où la question de la protection des données est particulièrement délicate. Le projet de dossier médical personnel a démarré en 2006 et a été relancé dans ses orientations actuelles au début de l'année 2009. Fin 2010, nous aurons sélectionné un hébergeur capable d'accueillir les premiers dossiers, avec une montée en charge en 2011-2012. Il s'agit avant tout d'un outil de coordination thérapeutique mais, à terme, ces dossiers pourront apporter une aide au diagnostic compte tenu de la richesse des données médicales qu'il contiendra. Au cours de la vie d'un individu, les sources médicales sont en effet nombreuses : médecins généralistes, spécialistes, analyses biologiques et radiologiques, séjours hospitaliers… Le DMP permettra d'accéder rapidement à une image documentée de l'histoire médicale de chacun. Bien entendu, l'un des bénéfices attendus est aussi d'améliorer la gestion économique des soins (éviter les examens redondants, etc.).

La mise en place de ce dossier nécessite d'identifier chaque individu. Pourquoi ne pas avoir choisi le numéro de sécurité sociale ?

J.-F. P. : Il fallait en effet disposer d'un identifiant unique et sûr pour chaque titulaire de dossier médical personnel. La Commission nationale de l'informatique et des libertés (CNIL) puis la loi se sont opposées, dans ce cas précis, à l'usage du numéro d'inscription au répertoire des personnes physiques (NIR), autrement dit du numéro de sécurité sociale. Elles ont en effet exigé un identifiant spécifique à la fois moins marqué historiquement* et non signifiant : il était par exemple hors de question que l'on puisse remonter à l'origine géographique (notamment nationale) des individus, comme avec le NIR. Après une période transitoire, l'identifiant national de santé adopté dès 2011 sera généré de manière totalement aléatoire (d'où le sigle INS-A). La Caisse nationale d'assurance vieillesse (CNAV) nous accompagne dans la mise en œuvre de ce programme INS avec l'aide, pour la phase transitoire, de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI).

La création de ce dossier est toutefois soumise au consentement du patient…

J.-F. P : C'est un aspect majeur. Il faudra en effet le « consentement éclairé » du patient pour le créer, mais aussi pour que tel ou tel professionnel de santé ait l'autorisation d'accès à son contenu. Nous pilotons donc également une réflexion sur le mode de mise en œuvre de ce consentement.

Mais comment se prémunir contre les « indiscrétions » ?

J.-F. P. : Cette question rejoint directement celle de la spécificité des données de santé. Typiquement, la sensibilité d'un individu à telle ou telle information varie selon un grand nombre de paramètres : son statut social, son âge, sa situation (vie normale ou à la veille d'une intervention chirurgicale…), la nature de sa pathologie et son impact social (qu'il s'agisse de maladies cardiovasculaires, d'alcoolisme…), etc. Comme le patient aura la maîtrise de son dossier, c'est à lui qu'il reviendra d'arbitrer, au cours de sa vie et de son parcours médical, entre consentement et « perte de chance ». Par perte de chance, il faut entendre tout ce qui peut réduire les chances d'amélioration de son état voire de sa survie : libre à lui par exemple de courir le risque de dissimuler certaines allergies, cela ne dépendra que de lui. Notre stratégie consiste ainsi à faire de la sécurité à deux niveaux : *a priori* et *a posteriori*. Chaque titulaire de DMP définira *a priori* les personnels ou institutions qu'il habilite à consulter son dossier. *A posteriori*, il pourra suivre à la trace la liste de ceux qui ont accédé à son dossier et les données que chacun a consultées : c'est ce qu'on appelle la traçabilité. La question de la gestion du modèle de consentement est absolument décisive. C'est l'une des réflexions majeures que nous menons et qui aboutira notamment à la mise en place d'un « séquestre » des régimes d'habilitation choisis par les patients.

Propos recueillis par Dominique Chouchan

* Le Groupement d'intérêt public (GIP) ASIP Santé regroupe les missions auparavant dévolues aux GIP DMP et Carte professionnelle de santé ainsi que la mission interopérabilité du Groupement pour la modernisation du système d'information hospitalier (www.asipsante.fr).

* Le numéro national d'identité a été créé sous l'Occupation. Des instructions de 1941 et de 1942 avaient imposé d'adjoindre au premier chiffre (le sexe) une indication relative à la nationalité ou à l'origine, notamment juive, de chaque individu.

médicales numérisées

QUESTIONS À PHILIPPE PUCHERAL

La possibilité d'accéder en ligne au dossier médical d'un patient devrait offrir de multiples avantages en termes de qualité de soins. Mais la plus grande prudence est de rigueur afin que soient respectées les règles en vigueur de protection des données de santé.

Vous vous êtes engagé depuis 2009 dans un projet pluridisciplinaire sur la protection des données de santé. Quels en sont les enjeux ?

Philippe Pucheral : L'objectif principal du projet Demotis* est de confronter les exigences juridiques en matière de protection des données de santé et l'état de l'art en informatique : est-on capable, au plan technique, de mettre en œuvre la législation actuelle ? S'il est très difficile pour des informaticiens d'appréhender les textes juridiques, il l'est tout autant pour des juristes d'évaluer la portée de ces textes du point de vue informatique. Notre rôle d'informaticien est d'identifier les verrous technologiques potentiels. Par exemple : comment permettre au patient d'identifier ceux qui ont interrogé son dossier médical personnel (DMP) et la nature précise des données consultées, comme le prévoit la loi* ? S'il est facile de tracer les connexions à un dossier, il est beaucoup plus difficile de fournir un outil à la fois intuitif et précis (simple d'utilisation pour le patient) permettant de construire une vue intelligible de l'ensemble des accès effectués à partir d'un journal de requêtes. Autres exemples : comment mesurer l'efficacité d'une protection cryptographique des données stockées face à des attaques statistiques ou des attaques internes ? Comment garantir le droit à l'oubli alors que l'effacement irréversible d'une donnée dans une base reste un problème technique ouvert ? Ou encore comment s'assurer de l'irréversibilité d'un processus d'anonymisation de données ? *etc.*

Toutes ces questions, vous les aviez déjà rencontrées dans le cadre de vos travaux sur les données médicales…

P. P. : Nous travaillons en effet depuis plusieurs années sur la protection de la confidentialité des données personnelles, notamment médicales, et sur les verrous technologiques associés. La centralisation des données personnelles sur des serveurs, comme c'est le cas du DMP, offre des avantages indiscutables en termes de disponibilité des données, de tolérance aux pannes, de cohérence des politiques de sécurité, etc. Sans vouloir rentrer dans un débat idéologique, cette centralisation n'est cependant pas neutre du point de vue de la protection de la confidentialité. Nous travaillons donc sur une approche complémentaire, et non opposée à une solution serveur, qui permette à chacun de mieux contrôler la façon dont ses données les plus sensibles sont stockées et échangées. Nous avons ainsi conçu un véritable « serveur personnel de données ». Ce dernier est embarqué dans une nouvelle génération de cartes à puce à très grande capacité de stockage (le SPT*), dont le prototype est fabriqué par la société Gemalto*. La carte est composée d'un microcontrôleur sécurisé (véritable ordinateur miniaturisé) relié à une mémoire persistante de plusieurs Giga-octets de capacité (de type mémoire flash). Le tout tient dans une puce de format carte SIM, que l'on peut insérer dans un châssis de clé USB. Le microcontrôleur embarque une chaîne logicielle similaire à celle d'un serveur classique : serveur web, serveur d'applications, serveur de base de données (intégrant le contrôle d'accès). Pour naviguer sur ce serveur, il suffit de brancher le SPT sur le port USB d'un terminal quelconque puis de s'y connecter *via* un navigateur Web, comme pour n'importe quel serveur. Le patient peut ainsi tirer partie des deux serveurs à sa disposition : le serveur central pour gérer ses données classiques et son serveur personnel pour ses données les plus sensibles, données qu'il ne souhaite pas laisser en ligne et pour lesquelles des modes d'échange personnalisés avec des professionnels de santé sont possibles.

© INRIA / J. WALLACE

Philippe Pucheral, professeur d'informatique à l'université de Versailles Saint-Quentin-en-Yvelines (UVSQ), est responsable de l'équipe-projet SMIS (Secured and Mobile Information Systems), commune à l'Inria, à l'UVSQ et au CNRS.

C'est ce dispositif que vous expérimentez avec le Conseil général des Yvelines ?

P. P. : Nous leur avons effectivement présenté notre solution. Au-delà de la protection de la confidentialité des données, la portabilité du système a été pour eux un argument décisif. Le Conseil général souhaite améliorer la coordination des soins et des prestations sociales auprès des personnes dépendantes. Dans ce contexte, pouvoir disposer du dossier médico-social de la personne à son domicile, sans nécessiter de connexion internet est un avantage déterminant. Notre partenariat a fait l'objet d'une première convention de trois ans (2006-2009) *. Nous venons de commencer une expérimentation sur le terrain qui va se dérouler pendant dix-huit mois.

Propos recueillis par D. C.

* Le projet Demotis (2009-2012), financé par l'Agence nationale de la recherche (ANR), associe trois partenaires : Sopinspace, société spécialisée dans la mise en œuvre d'outils de travail collaboratif, le Centre d'études sur la coopération juridique internationale (Cecoji, unité mixte de rcherche CNRS) et l'Inria.

* Voir l'entretien avec Jean-François Parguet.

* La société Gemalto est le leader mondial de la sécurité numérique.

* Le sigle SPT signifie *Secure Portable Token*, pouvant être traduit par jeton sécurisé.

* Cette action, soutenue par le Conseil général des Yvelines et l'ANR, associe l'INRIA, l'Université de Versailles, les sociétés Gemalto (sécurité numérique) et Santeos (hébergeur de données de santé) ainsi que Cogitey et ALDS (deux coordinations gérontologiques).

INRIA