DÉCRET CONFIDENTIALITÉ

La sécurité avant tout

POUR ÊTRE COURONNÉ DE SUCCÈS, LE DMP DEVRA IMPÉRATIVEMENT RÉUSSIR À PRÉSERVER LE SECRET MÉDICAL LORS DES ÉCHANGES DE DONNÉES. EN ATTENDANT, LES MESSAGERIES SÉCURISÉES SE DÉVELOPPENT ET DES ÉTABLISSEMENTS DE SANTÉ METTENT L'ACCENT SUR LA CONFIDENTIALITÉ DES DONNÉES.

Siemens

« Admis à l'intérieur des maisons, mes yeux ne verront pas ce qui s'y passe, ma langue taira les secrets qui me seront confiés. » Le serment d'Hippocrate, prononcé par tous les médecins, prônait déjà le secret médical, officialisé en 1910 par le code pénal. Le décret du 15 mai 2007, dit « décret confidentialité », détermine les exigences de confidentialité et de sécurité à respecter par les professionnels et les établissements de santé qui conservent sur support informatique et échangent par voie électronique des données de santé à caractère personnel. Des exigences qui s'appliqueront au DMP. L'un des points fondamentaux de ce décret est la nécessité, pour tout professionnel de santé, d'avoir recours à la carte CPS pour accéder ou transmettre par mail de telles informations. Et pourtant, aujourd'hui, un médecin sur trois qui possède une adresse mail non sécurisée l'utilise sans aucune précaution !

1 337 certificats CPS

Dès 2002, le GIP CPS a donc établi un référentiel d'homologation afin de favoriser le développement d'une offre de messagerie sécurisée adaptée. « Dans ces outils, l'identité des partenaires de l'échange est garantie par l'usage de la carte CPS ; l'interopérabilité des différents produits repose sur le respect de standards internationaux. Les adresses mail des correspondants ainsi que leurs certificats de confidentialité doivent être accessibles dans l'annuaire du GIP CPS. Huit produits sont homologués, une dizaine de dossiers est en cours d'examen », indique Marthe Wehrung, directrice du GIP CPS. Pour le Conseil national de l'Ordre des médecins, la généralisation des messageries CPS est un impératif. Il envisage même de lancer sa propre messagerie et a déjà mandaté l'opérateur Orange afin de réaliser les études de faisabilité.

« Un système efficace est à la fois simple et interopérable. Les médecins pensent parfois qu'utiliser une messagerie sécurisée est complexe, alors qu'il suffit d'installer un logiciel et de se laisser guider. Le coût de notre solution n'est que de 70 €, le frein n'est donc pas financier, ce sont les mentalités qui doivent rapidement évoluer », affirme Michel Nogatechewsky, directeur de la société Medsys, éditeur informatique, dont la messagerie DocteurNetCPS est homologuée. Cegedim logiciels médicaux, autre éditeur, a choisi d'intégrer Secure Medical Mail à l'ensemble de ses logiciels métiers. « Les professionnels n'auront plus qu'à activer leur certificat CPS. Nous espérons ainsi convaincre nos 50 000 clients, notamment les établissements de santé avec CrossWay Hopital », assure Pierre Bruneau, son directeur médical. Fin août, 1 337 professionnels se sont vus délivrer un certificat CPS ; ils n'étaient que 811 au 31 décembre.

Chantier confidentialité

Dans les hôpitaux et les cliniques, la sécurisation des données dépasse le cadre des messageries sécurisées. 24 établissements de santé participent à un chantier « confidentialité » sous l'égide du GMSIH [1]. « Pendant deux ans, ils testent concrètement des organisations, des équipements, des modes de cryptage. Autant d'expériences qui seront mises en commun », assure Hugues Dufey, directeur du GMSIH. « Les industriels présentent des produits performants, mais l'établissement doit savoir ce qu'il souhaite, d'où l'intérêt d'établir un cahier des charges précis. » Le CHU de Nancy participe à cette expérimentation. « Nous avons retenu trois industriels afin de prendre en compte l'ergonomie des équipements, la signature unique à partir d'un annuaire sécurisé et l'utilisation des certificats CPS. Le projet touche à sa fin, il a suscité une bonne adhésion du personnel et permis d'optimiser l'exploitation du système d'information », analyse Jean-Marc Virion, directeur informatique.

Conformément à la loi, tous les établissements de santé devront avoir souscrit aux obligations du décret confidentialité avant le 15 mai 2010. ■

Solène Penhoat

INFORMATISATION DES URGENCES

Accéder à l'information, vite !

Le DMP est particulièrement attendu dans les SAU (services d'accueil d'urgence). L'accès aux données de santé des patients est en effet essentiel pour poser un diagnostic fiable. Déjà, en quelques années seulement, l'informatisation a gagné du terrain.

Août 2003. La France enregistre des températures record. Des personnes âgées déshydratées affluent par centaines, par milliers, dans les SAU. Mais, faute d'informatisation centralisée, l'alerte parvient trop tardivement aux pouvoirs publics. À la suite de ce drame, une campagne d'informatisation ambitieuse est lancée par la DHOS. En 2005, le plan Urgences de Xavier Bertrand fixe comme objectif une informatisation de 80 % des passages d'ici 2 ans. Un pari presque gagné aujourd'hui ! À l'époque, les solutions existantes étaient assez disparates et ne communiquaient pas entre elles. Le GMSIH a donc établi un cahier des charges qui décrit les fonctionnalités utiles, voire indispensables, comme le *tracking* des patients et la veille sanitaire, ainsi que les principes d'intégration. Un outil qui a permis aux industriels d'améliorer sensiblement leurs solutions. « Le SAMU [1] et la SFMU [2] travaillent actuellement à la création d'un moteur de recherche ultra performant basé sur la sémantique ; le logiciel ne recherchera plus un mot, mais une signification. Ainsi, en cas d'urgence, le médecin aura accès directement aux informations les plus pertinentes, ce qui sera révolutionnaire. Ce dossier n'est encore qu'au stade de la recherche, mais sa réussite pourrait modifier l'architecture du futur DMP », explique Yves Lannehoa, membre du conseil d'administration de la SFMU. Un appel à projets sera lancé en 2009 vers les industriels et les unités de recherche. ■