SECURISER LES ECHANGES ELECTRONIQUES DE DONNEES MEDICALES

Définition

L'échange d'informations médicales entre professionnels de la Santé est critique pour établir un diagnostic et pratiquer les soins adaptés au patient. Cependant, bien que la dématérialisation et l'échange électronique de données médicales soient devenus incontournables, les gains de productivité engendrés par l'adoption de ces méthodes ne doivent pas masquer les menaces qu'elles peuvent impliquer.

Les informations médicales sont, pour la plupart, nominatives ou identifiables et doivent faire l'objet d'une sécurisation importante. Le respect du secret médical implique que, lors d'échanges électroniques, ces données soient protégées et sécurisées afin d'éviter qu'elles ne soient interceptées et consultées par des personnes non autorisées, voire modifiées ou altérées.

En résumé, pour ce type d'informations sensibles, la mise en œuvre d'échanges électroniques doit s'accompagner d'un processus de réflexion sur les méthodes utilisées visant à d'une part respecter le secret professionnel et d'autre part à recueillir le consentement éclairé des patients.

Exemples

De nombreux exemples peuvent être cités. Ils concernent notamment tous les documents échangés entre les professionnels de santé, patients…

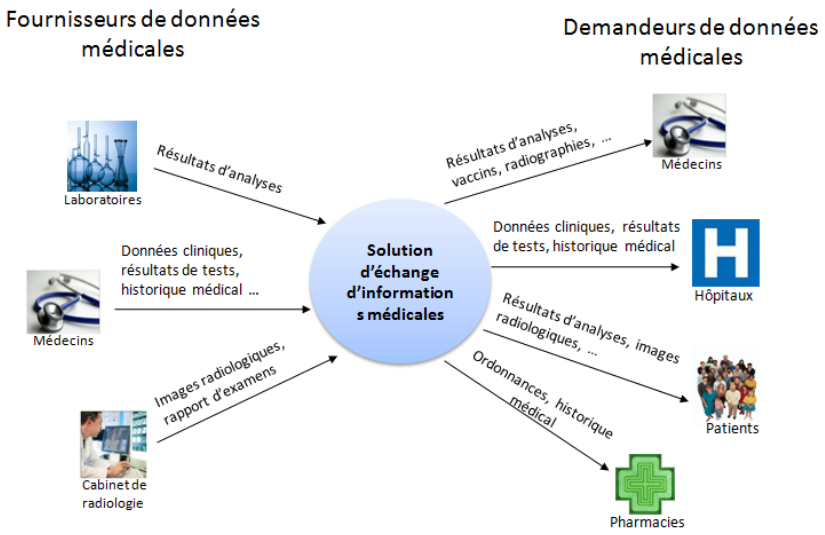
Ainsi, le groupement hospitalier **MiPiH** (Midi Picardie Informatique Hospitalier) a mis en place une solution d'échange, **Medim@il**, pour sécuriser et tracer les échanges confidentiels entre professionnels de santé. Aussi simple qu'un mail, l'enveloppe numérique **Medim@il** permet l'insertion de pièces jointes diverses et confidentielles telles que des radiographies, des comptes-rendus ou tous documents médicaux (nativement électroniques ou numérisés). Les enveloppes **Medim@il** sont certifiées, sécurisées et tracées de façon unique. Pour accéder à l'interface et générer des enveloppes, il faut être abonné au service. Les destinataires s'enregistrent en ligne, et valident ensuite leur inscription avec leur carte CPS (Carte Professionnel de Santé - carte d'identité électronique des professionnels de Santé). Conforme à la législation française, sa fiabilité en fait un instrument hospitalier moderne et universel pour les échanges entre professionnels. Il facilite ainsi les échanges entre hôpitaux et médecins libéraux.

Nous pouvons aussi prendre le cas d'échanges électroniques avec un laboratoire médical. Le laboratoire Biomnis, un des leaders français de la biologie médicale, est en en relation quotidienne avec près de 4000 correspondants (laboratoires d'analyse médicale, centre hospitaliers, cliniques, médecins prescripteurs, maisons de retraites, etc.). Ce laboratoire publie chaque jour environ 100 000 analyses, 25 000 comptes rendu de résultats et 16 000 échanges de fichiers sécurisés. Il a ainsi mis en place une solution d'échange électronique permettant de transférer en toute sécurité et automatiquement (deux

fois par jour) les données d'analyses médicales issues de son laboratoire. Ces échanges sont aussi parfaitement tracés, ce qui leur confère une valeur probatoire.

Cibles

L'obligation de secret médical s'impose à toute personne amenée à suivre l'état de santé d'un malade : médecins, radiologues, pharmacies, etc… Le schéma ci-dessous décrit les prinpaux acteurs concernés, ainsi que les données sensibles qui peuvent-être échangées :



Cadre réglementaire

Le cadre réglementaire concernant les échanges électroniques est basé sur :

- **Les articles 1316-1 et 1316-4 du Code Civil** : ils définissent les conditions impératives que doit revêtir un échange électronique pour acquérir une force probatoire
- **La réglementation CFR 21 Part 11** : elle définit les critères selon lesquels les dossiers et signatures électroniques seront considérés comme équivalents à des dossiers sur support papier et des signatures manuscrites. La réglementation s'applique aux dossiers sous forme électronique, qui sont créés, modifiés, maintenus, archivés, récupérés ou **transmis** dans le cadre des exigences liées à tout dossier décrit dans la réglementation de la FDA (Food & Drug Administration). Malgré son caractère américain, elle est couramment requise dans le milieu de la santé.

Les données médicales, quant à elles bénéficient d'une protection particulière :

- **Décret n° 2007-960 du 15 mai 2007 :** relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique.
- **L'article L1110-4 du Code de la Santé Publique** (CSP) sur le respect du secret médical
- **L'article L161-36-1 A du Code de la Sécurité Sociale**
- **L'article 226-13 du Code Pénal,** relatif aux sanctions en cas de révélation du secret médical.
- Directive Européenne du 24 octobre 1995 relative à la protection des personnes physiques à

l'égard du traitement des données à caractères personnel
- **Loi du 6 janvier 1978** modifiée relative à l'informatique, aux fichiers et aux libertés
- **La loi « Hôpital, patients, santé et territoires »**

Principaux standards d'échange

- **H.P.R.I.M** (Harmonie et Promotion de l'Informatique Médicale) est une norme de transmission des examens de Biologie. Initialement développée par les laboratoires d'analyse pour communiquer entre eux, cette norme a été ensuite utilisée pour transmettre les résultats aux médecins prescripteurs.
- **HL7** (Health Level 7) : ensemble de spécifications techniques pour les échanges informatisés de données cliniques, financières et administratives entre systèmes d'informations hospitaliers (SIH).
- **DICOM** (Digital Imaging and Communication in Medicine) est un standard d'échange d'imagerie médicale
- **IHE** (Integrating the Healthcare Enterprise) est une initiative des professionnelles de la santé destinée à améliorer la façon avec laquelle les logiciels du domaine échangent leurs informations. IHE propose l'utilisation coordonnée de standards établis, comme DICOM et HL7, afin d'apporter des solutions aux problèmes récurrents d'intégration de différents logiciels de santé.

Evaluation des risques

En cas d'échanges non sécurisés de données médicales, une violation du secret médical (interception des données par exemple), voire l'altération des données elles-mêmes, peut donner lieu à des sanctions de diverses natures.

- Des sanctions pénales : l'article 226-13 du Code pénal établit que « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie* ***d'un an d'emprisonnement*** *et de* ***15000 euros*** *d'amende.* »

- Des sanctions professionnelles : concernant les médecins notamment, les sanctions du Conseil de L'Ordre peuvent aller de la suspension provisoire à une radiation définitive.

Outre la violation du secret médical, la fraude à l'Assurance Maladie est un autre problème à prendre en compte. En 2010, le montant des fraudes totales détectées à l'Assurance Maladie représentait 156 milliards d'euros. Les moyens de protection décrits plus bas, tels que le chiffrement des données et la signature électronique via les cartes vitales et CPS permettent d'y remédier.

Moyens de protection

Il est important d'établir une politique de confidentialité rigoureuse, et instaurer la Confiance dans les échanges électroniques devient l'enjeu primordial pour éviter les risques évoqués précédemment. Schématiquement, la Confiance consiste à transmettre les données entre un émetteur et un destinataire en garantissant la sécurité et la traçabilité de celles-ci. Les éléments de Confiance de l'échange incluent :

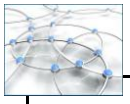
- **L'identification et l'authentification (si possible forte)** de l'émetteur et du destinataire : La CNIL a rappelé dans ses avis que le recours à la CPS (Carte Professionnelle de Santé) était prioritaire par rapport à un dispositif login/password beaucoup moins efficace pour garantir la sécurisation des échanges.

- **La confidentialité :** le chiffrement des données médicales permet aux seules personnes autorisées de lire et traiter le contenu.

- **L'intégrité** des données envoyées : La solution d'échange d'informations calcule une empreinte numérique (fonction cryptographique) avant l'envoi des données médicales. Si l'empreinte reçue par le destinataire est la même que celle envoyée par l'expéditeur, alors les données médicales n'ont pas été altérées depuis l'envoi.

- **La traçabilité des échanges** et des traitements sur les données tout au long de leur cycle de vie permet de conserver de manière complète, fiable et inaltérable l'ensemble des opérations réalisées, qui les a réalisées, les contrôles effectués, les résultats obtenus, … Appelé aussi « journalisation formelle », il s'agit d'un élément fondamental dans le processus de preuve, et donc de valeur probatoire du système lui-même

- **La signature électronique sécurisée :** des données envoyées avec contre-signature du destinataire permet d'identifier avec certitude l'émetteur et le destinataire d'un message, de garantir son intégrité, et d'établir de manière fiable la date et l'heure des signatures.



Liens utiles

- **ASIPSanté (Agence des Systèmes d'informations Partagés de Santé).** Elle a pour rôle de favoriser le développement des systèmes d'informations partagés dans le domaine de la santé et le secteur médico-social, afin d'améliorer la coordination et la qualité des soins, la prévention, la veille, et l'alerte sanitaire http://esante.gouv.fr/

- **CISS (Collectif Iner-Associatif sur la Santé).** Il regroupe plus de 30 associations intervenant dans le domaine de la santé http://www.leciss.org/

- **MiPiH (Midi Picardie Informatique Hospitalière)** a mis en œuvre un service en ligne permettant de génerer des échanges sécurisés, tracés, et confidentiels entre professionnels de santé. Ce service, baptisé Medim@il est aujourd'hui utilisé pour les échanges entre le milieu hospitalier et les médecins libéraux. http://www.mipih.fr/