De la « confiance » dans les systèmes d'information de santé

Conférence du 15 novembre 2011, animée par Gilles Trouessin

Rapporté par Véronique Pelletier, membre du Comité d'ADELI

Gilles Trouessin a animé la conférence du 15 novembre 2011, autour « De la confiance dans les Systèmes d'Information de Santé » afin de débattre de la confiance que l'on est et/ou serait en droit de placer, dans les S.I. de Santé en général et les S.I. Hospitaliers en particulier sous différents angles :

- *Sectoriel – les enjeux de confiance ?*
  - *Santé, soins, soins de santé, social, pharmaceutique, épidémiologique, etc. : quels sont les enjeux de la confiance dans ces S.I., selon les types et catégories d'acteurs concernés et les risques encourus s'appliquant sur ces systèmes particuliers que sont les SIS/SIH ?*
- *Factuel – les constats de méfiance ?*
  - *Attaques/menaces/vulnérabilités, us-et-coutumes, pratiques plus ou moins bonnes, etc. : quelles sont les constatations et, surtout, quels sont les retours d'expériences qui devraient nous permettre de matérialiser une méfiance raisonnée dans l'utilisation de ces systèmes ?*
- *Personnel – les sujets de défiance ?*
  - *Données de santé/informations médicales, données de remboursements de soins de santé, données à caractère personnel, données d'épidémiologie et/ou de pharmaco-vigilance, etc. : quels seraient les points de défiance que tout individu ou citoyen serait en droit d'exhiber aux multiples autorités socio-sanitaires en charge de la définition et de l'exploitation de tels systèmes ?*
- *Professionnel – le motif d'« inconfiance » ?*
  - *Management de la qualité et/ou de la sécurité, organisation et pilotage des systèmes et des solutions de protection, mise en œuvre de techniques d'anonymisation, mise en place de systèmes de pseudonymisation / hétéronymisation / etc., quelles peuvent être les mesures légales et réglementaires, managériales et organisationnelles, technologiques et techniques qui permettront de lutter contre cette « inconfiance » ambiante, tant envers la sécurité-security (sécurité-immunité) que la sécurité-safety (sécurité-innocuité) auxquelles ils sont astreints ?*

Le conférencier

Gilles Trouessin est consultant senior dans l'équipe de SCASSI Conseil, société d'expertise, de conseil et d'audit en sécurité et sûreté des systèmes d'information, et notamment pour la sphère santé/social (www.scassi.com). Il est responsable du département « Sécurité des Systèmes d'Information de Santé (SIS) / Hospitaliers (SIH) » et est très impliqué dans la protection des données sensibles (données de santé et/ou à caractère personnel).

Il est membre de l'APSSIS – Association pour la Promotion de la Sûreté des Systèmes d'Information de Santé.
Il est également membre actif de l'AFCDP – Association Française des Correspondants à la protection des Données à caractère Personnel, où il contribue au groupe de travail Sectoriel « Données de santé » et anime le groupe de travail régional – sud-ouest pyrénéen.

Il est adhérent d'ADELI depuis le début des années quatre-vingt-dix.
Gilles Trouessin a soutenu sa thèse en 1991, au LAAS-CNRS – Laboratoire d'Analyse et d'Architecture des Systèmes, sur « le traitement fiable des données confidentielles par fragmentation-redondance-dissémination ».
Il a ensuite effectué un post-doc en 1992 au CERT-ONERA – Centre d'Études et de Recherches de Toulouse – sur les évaluations des propriétés de sécurité (confidentialité & intégrité) par les théories de l'incertain (théories des possibilités, des plausibilités, de l'évidence).

Ensuite et jusqu'en 2001, il a travaillé comme ingénieur d'études sécurité au CESSI – Centre d'Études des Sécurités du Système d'Information – de la CNAMTS – Caisse Nationale de l'Assurance-maladie des Travailleurs Salariés – dans l'équipe qui a conçu, développé et mis en œuvre la méthode d'anonymisation de l'Assurance-maladie, fondée sur la fonction FOIN – Fonction d'Occultation d'Identifiants Nominatifs.

Durant cette période, il a été membre et animateur de groupes d'experts en « sécurité des SIS » pour la normalisation en « informatique de santé » (« health informatics »), à l'AFNOR, au CEN et à l'ISO.

Puis, de 2001 à 2005, il a rejoint le cabinet d'audit ERNST & YOUNG comme auditeur / consultant en sécurité des Systèmes d'information de Santé (SIS) et des Systèmes d'Information Hospitaliers (SIH), période durant laquelle il a conduit le projet de recherche : Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication pour la sphère Santé/Social (MPSSICSS – MP6).

De 2005 à 2010 et avant de rejoindre la société SCASSI Conseil, il avait travaillé pour OPPIDA sud, comme consultant expert en sécurité des systèmes d'information de santé.
Il s'est toujours intéressé à l'anonymisation et à la cohabitation entre les exigences de sécurité classiques, incluant la confidentialité (ou confidentialité-discrétion©) et les obligations de sécurité spécifiques incluant le respect de la vie privée (ou confidentialité-séclusion©).

Attentes des participants

Gilles Trouessin commence son intervention par une question aux auditeurs : « Pouvez-vous, par trois ou quatre mots-clés seulement, définir ce que vous entendez par la « confiance » dans les S.I. de santé ».

Les participants citent successivement :
- confidentialité ;
- fiabilité ;
- périmètre de propriété ;
- risque juridique ;
- risque médical ;
- éthique professionnelle ;
- utilisation au bon moment ;
- dossier médical personnel ;
- vue transversale ;
- complétude ;
- sécurité.

Le mot « confiance » est lié à confidence, à la confidentialité, et aussi à la fiabilité ; selon Jean-Claude Laprie – le pape de la sûreté de fonctionnement selon Gilles – ce mot a pour origine, en vieux français, « fiableté ». La Sûreté de fonctionnement, c'est en fait la perception de la confiance justifiée sous différentes facettes possibles.

Gilles insiste sur l'idée de bâtir les S.I. de santé, médicaux ou hospitaliers, sans construire une nouvelle informatique qui deviendrait « nosocomiale ». C'est-à-dire une informatique qui rendrait les patients plus malades en sortant qu'en entrant. Par exemple, on arrive mal-en-forme à l'hôpital et on en repart encore plus mal-en-point à cause de Systèmes d'Information non suffisamment sûrs de fonctionnement. C'est l'exemple connu des sur-irradiés d'Épinal ou de Toulouse.

Intentionnellement ou pas, la sécurité (security) peut avoir une incidence sur l'innocuité (safety) des personnes. Il faut pouvoir faire la différence entre la sécurité « Security » et la sécurité « Safety » ; même si, en français, il n'y a qu'un mot « sécurité », alors qu'en anglais on en a deux :
- « security », que l'on peut traduire par « sécurité-protection du système d'information » ;
- « safety », que l'on traduira par « sécurité-sûreté des personnes et des environnements critiques ».

On est à la veille d'avoir des attaques en sécurité-security qui pourront avoir des conséquences sur la sécurité-safety, si l'on n'y prend pas garde.

Protection des données à caractère personnel

Partant du constat que la protection des données à caractère personnel est un sujet particulièrement sensible — comme cela apparaît dans les résultats de plusieurs sondages publiés aux États-Unis et dans l'Union européenne[1], — il est jugé important voire très important par les personnes interrogées, de respecter une politique de protection des données personnelles (ou « privacy policy ») dans des proportions assez contraignantes, en particulier dans le secteur de la santé.
En matière d'importance de la « privacy », ce secteur santé / social arrive en deuxième position, après le secteur financier ; en troisième position on trouve la pharmacie, et, loin derrière, les secteurs de la distribution, des télécoms, des transports.

Dans ce sondage, les thématiques sectorielles du « soin » et de la « pharmacie » avait alors été jugées très sensibles, bien avant toutes les autres préoccupations.

[1] *Voir par exemple un rapport de l'Union européenne de janvier 2008 : « Data Protection in the European Union Citizens' perceptions Analytical Report » http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf*

Les données de santé, médicales, de soin ou de remboursement de soins, touchent à l'intimité de la personne.
Ce sont des données plus intimes que le solde de leur compte en banque, leurs habitudes de consommation, leurs achats en grande surface, sur e-bay ou sur Internet. Savoir de quelle pathologie est atteinte une personne est une donnée très intime et donc extrêmement sensible.

On peut décider de ne garder qu'« un » euro seulement sur son compte en banque et d'en retirer tout son argent régulièrement, de ne jamais acheter sur Internet, de n'avoir de carte de fidélité dans aucune enseigne ou grande surface ; mais on ne peut pas décider de ne pas avoir un cancer, de l'asthme et toute affection chronique. Un employeur indélicat pourrait être tenté de décider de ne pas employer une personne dont il saurait qu'elle est gravement malade.

Lors d'un travail de groupe au sein de l'AFNOR, un participant a témoigné que sa banque l'avait convoqué à propos de la révision de son prêt d'accession à la propriété, car elle avait constaté sur son compte des montants de remboursement d'actes de soins symptomatiques d'une pathologie lourde connue ; n'étant pas encore pris en ALD — Affection Longue Durée, il avait donc été obligé d'avancer ces frais. Le passage en statut ALD aurait permis de masquer les sommes perçues.
La banque a fini par s'excuser car cette personne, très au fait des lois sur « l'Informatique, les Fichiers et les Libertés », l'a mise devant ses contradictions. Cet exemple montre bien que l'on peut connaître beaucoup de la vie des gens rien qu'en observant leurs comptes en banque…

Tant que l'on n'a pas de problème, la transparence sur les données de santé n'a pas d'incidence ; mais dès qu'un problème survient, cela peut devenir très vite très pénalisant. Gilles aime a prétendre que : « ce n'est pas parce que je n'ai rien à cacher que… je n'ai rien à cacher ».

Loi informatique et libertés

Les articles IX et X de la loi sur « l'Informatique, les Fichiers et les Libertés » sont entièrement consacrés au cas particulier des données de santé, au numéro de sécurité sociale (le NIR ou n° INSEE pour être exact). Ce NIR, Numéro d'Inscription au Registre national d'identification des personnes physiques (RNIPP), a été prêté de longue date par l'INSEE à la sous-sphère assurance-maladie, de la sphère santé-social : il est très sensible.
Toute organisation, publique comme privée, doit respecter la loi dite « Informatique et Libertés » du 06 janvier 1978, ou loi modifiée du 06 août 2004.

Il y a obligation absolue d'informer les personnes lors de la collecte d'informations nominatives à caractère personnel. Les droits « fondamentaux » de la loi Informatique et Libertés sont :
- le droit d'accès aux données personnelles manipulées dans les S.I. ;
- le droit de rectification des données personnelles erronées ou périmées ;
- le droit de suppression de données personnelles abusives, sur motif légitime.

L'intervention introduit ensuite des droits plus « futuristes » pour la loi Informatique et Libertés tels que :
- le droit à l'oubli « implicite » : avec une durée de conservation maximale de données « périmées » ;
- le droit à l'oubli « explicite » : en lien avec l'ex-projet de petite loi « Destraignes-Escoffier », prônant le droit à l'oubli électronique sur les réseaux (et donc le respect de la vie privée, notamment sur Internet).

Sûreté de fonctionnement

La sûreté de fonctionnement d'un système informatique est cette « ***propriété générique qui permet aux utilisateurs de placer une confiance justifiée dans le service qui leur est délivré par ce système*** ».

Ses caractéristiques, ou attributs perceptifs tels que définis par Jean-Claude Laprie, sont :
- la fiabilité, vis-à-vis de la capacité à offrir une « continuité de service », dans les contraintes définies ;
- la disponibilité, vis-à-vis de l'aptitude à « être prêt à l'usage » dans les conditions prévues ;
- l'intégrité, vis-à-vis de la non-occurrence « de modification inadéquate », selon les politiques prévues ;
- la confidentialité, vis-à-vis de l'absence « de divulgation inappropriée », selon les politiques prévues ;
- la maintenabilité, vis-à-vis de la capacité « à être réparé et évoluer », en fonction des environnements ;
- la sécurité-safety, vis-à-vis « des défaillances catastrophiques » pour l'environnement ou la personne ;
- la sécurité-security, vis-à-vis de la « protection des informations traitées » par le système concerné ; c'est-à-dire la combinaison des propriétés de disponibilité, d'intégrité et de confidentialité.

Sécurité du Système d'Information

La sécurité du S.I. ou sécurité-immunité ou encore sécurité-security est la combinaison des propriétés de base garantissant que les informations sont manipulées de façon autorisée.

On parle souvent de DIC + ? ou de DICA Disponibilité + Intégrité + Confidentialité + Auditabilité :

- la Disponibilité — pas de « rétention/blocage » non autorisée de l'information ;
- l'Intégrité — pas de « modification/altération » non autorisée de l'information ;
- la Confidentialité — pas de « divulgation/ propagation » non autorisée de l'information ;
- l'Auditabilité© — « capacité du système à auditer » l (es) élément (s) mis en œuvre et « capacité du système à auditer » la (les) sécurité (s) mis (es) en place, c'est-à-dire la « capacité à fournir les éléments de preuves de la confiance ».

Confidentialité

La confidentialité est une propriété permettant de garantir que les informations sont divulguées de façon autorisée :

- confidentialité — accès à l'information en justifiant du « besoin d'en connaître » ;
- secret médical — accès légitime mais dans le respect du « colloque singulier » ;
- secret professionnel — accès autorisé à l'information mais obligation de réserve ;
- discrétion professionnelle — accès inévitable avec obligation de respect de l'individu.

Mais incluant aussi :

- anonymat strict — suppression (irréversible) des identités (directes ou indirectes) ;
- pseudo-anonymat — remplacement (inversible) des identités (directes ou indirectes) ;
- vrai-faux anonymat — modification provisoire (réversible) des informations « ré-identifiantes ».

Confidentialité-discrétion©

La « confidentialité-discrétion© » est une propriété garantissant que les informations sont transmises en toute discrétion grâce à :

- la cryptographie — technique consistant à protéger l'information électroniquement ;
- au chiffrement à clé secrète ou à clé publique/privée — chiffrements symétrique et asymétrique ;
- des techniques éprouvées — les techniques actuelles pouvant être testées mondialement ;
- des techniques réversibles — par exemple, la protection des données durant leur transport.

Et aussi :

- en respectant la loi, longtemps restreinte au militaire, la cryptographie s'est assouplie depuis 1999 ;
- avec l'accord de l'individu, en prenant en compte les exigences et avis émis par la CNIL ;
- dans le respect de l'état de l'art, car ces techniques sont pointues et ne s'improvisent pas.

Confidentialité-séclusion©

La « confidentialité-séclusion© » est la volonté intime garantissant que les informations sont divulguées de manière entièrement anonymisée :

- irréversibles — aucun retour n'est possible depuis les anonymats vers les noms et/ou identités ;
- inversibles – le seul retour possible aux noms et/ou identités serait la voix légale et réglementaire ;
- chaînable – c'est la possibilité de relier ensemble tous les épisodes de soins et/ou de remboursements ;
- robuste – face aux attaques qui sont menées par inférence (déductive, inductive, abductive, adductive).

Et aussi :

- anonymisation vraie – l'irréversibilité est totale et prouvée (juridique, organisationnelle, technologique) ;
- par fonction à sens unique – la fonction cryptographique est plus sûre que du chiffrement irréversible ;
- avec des dimensions juridiques/éthiques – organisation indispensable pour garantir un anonymat vrai.

Les acteurs de la sphère « Santé-social »

Quatre grands métiers existent dans la sphère santé-social :

- gestion administrative et financière : par exemple les trois grands régimes CNAMTS, CCMSA, RSI ;
- prévention individuelle et production de soins : la médecine prévention/curative, ambulatoire ou non ;
- recherche clinique : qu'elle soit publique ou privé, pharmaceutique ou autre, la R & D est fondamentale ;

- santé publique : avec toutes les actions et réglementations autour des x-vigilance et x-évaluations.

Le passage d'une sphère à l'autre, d'un domaine à l'autre, voire d'un métier à l'autre, peut poser le problème de la confiance « justifiée » dans les S.I. des autres sphères, et donc la problématique de la sécurité d'un système vis-à-vis d'un autre. Dès qu'un transfert de données a lieu, se pose la question de la confiance autour de ce transfert. Par exemple, les fonctions d'anonymisation des identités des individus sont un besoin flagrant par endroits, mais il faut être outillé pour vraiment anonymiser.

Passer une frontière, que ce soit entre des sphères de compétences, des domaines d'activités, des métiers, ou entre des États ou sortir de la frontière européenne, pose également le problème de la confiance. Un flux transfrontière doit être déclaré (voire autorisé), et surveillé (voire supervisé), afin d'identifier les données à caractère personnel concernées et les garanties de sécurité à y apporter.

Il est possible de raffiner ou non les données ou informations médicales, les données de santé, les données à caractère personnel ; on arrive très vite à des schémas de données très complexes ; mais, comme dans toute analyse de risques SSI digne de ce nom, on peut faire un arbre plus ou moins repliable sur lui-même, pour modéliser fidèlement ces schémas d'informations et, par conséquent, les protections à y associer.

Deux médecins qui se parlent, avec les nouvelles technologies, sont évidemment soumis au secret médical. En fait, on parle de secret professionnel depuis plus de dix ans, bien que le secret médical soit vraiment particulier. La Carte de Professionnel de Santé – CPS - est utilisée par la médecine ambulatoire. Les professionnels hospitaliers ne l'ont pas encore suffisamment déployée, car le coût est encore souvent trop élevé. Le chiffrement est généralement utilisé ; mais nombre de professionnels de santé échangent par courriels.

Il existe des organismes de normalisation et des groupes de normalisation dédiés à l'informatique de santé et même à la sécurité des données de santé, et donc de nombreux référentiels en la matière.
Le GMSIH qui, avec la MEAH et la MAINH, a intégré l'ANAP ; tout comme le GIP-CPS et le GIP-DMP ont donné naissance à l'ASIP-Santé, sont à l'origine de nombre de ces référentiels. L'ASIP-Santé est l'agence nationale qui s'occupe des Systèmes d'Information Partagés de Santé et est désormais en charge du DMP, entre autres grands chantiers.

La sécurité de l'information est donc une préoccupation de très longue date des acteurs de la santé, mais il y a encore assez peu d'endroits où on a raisonnablement et rationnellement pu atteindre un niveau de maturité acceptable vu la sensibilité des informations traitées.

Dans le monde hospitalier, il faut convaincre les grands patrons que la sécurité est importante pour l'image de marque de l'hôpital, mais aussi pour la confiance que le patient va accorder à l'hôpital. Si on fait un audit en sécurité-security (protection des données et non protection des personnes), le premier critère traité par les politiques de sécurité à l'hôpital, c'est la confidentialité et on se rend compte que c'est le plus mal traité. Les exigences sur les systèmes portent de plus en plus sur la disponibilité, la réactivité, la qualité de service. On dépend de plus en plus de l'informatique, des systèmes d'information. On se rend compte que les ressources humaines et financières se focalisent sur une des quatre propriétés de base de la sécurité qu'est la disponibilité et non pas exclusivement sur la confidentialité.

Propriété DICA de la Sécurité-security ou Sécurité-immunité

Les quatre grandes propriétés de la Sécurité informatique (datant des années 1980), de la Sécurité de l'information sont :

- la Disponibilité — pas de rétention ou de blocage de l'information non autorisée par la politique de sécurité ;
- l'Intégrité – c'est aussi l'exactitude, l'intégralité, la justesse au sens de « correctness », la complétude, l'exhaustivité ; c'est, par exemple, ne pas se tromper de posologie, ou d'extrait de patient lors d'une analyse médicale ; ne pas faire de modification, ne pas altérer les données non autorisées ; c'est ne pas se tromper sur l'identité du patient. Il y a déjà eu des collisions sur le numéro INSEE, mais c'est très rare. On définit un cadre, un permis d'exercer ;
- la Confidentialité – c'est la plus importante côté citoyen ; dans le monde militaire on parle du « besoin d'en connaître » ; dans le monde médical, il est question de « colloque singulier » c'est-à-dire un dialogue particulier entre le patient et son médecin qui impose que ne soit pas divulgué par le médecin tout ce qui lui est confié par le patient sous le sceau du secret médical. Le secret médical est d'ordre public et protège l'individu contre lui-même, contre ses faiblesses.

Ce n'est pas le même type de secret que le secret bancaire, le secret industriel ou le secret défense ; même si la prise en compte de ces exigences sera traduite par des technologies désormais classiques dans le monde de la sécurité ;

- l'Auditabilité, appelée parfois non-répudiation ou traçabilité de façon un peu réductrice ; car les sécurités mises en place doivent pouvoir elles aussi être auditées. L'auditabilité revient à garantir les propriétés de disponibilité, d'intégrité et/ou de confidentialité sur des méta-données telles que celles qui sont nécessaires pour former une signature électronique, par exemple :
  - l'auditabilité couvre d'abord des aspects purement techniques, à travers :
    - la traçabilité ou capacité à garder la trace des événements dits « de sécurité »,
    - l'imputabilité ou propriété qui permet d'imputer un auteur à chaque événement,
  - l'auditabilité couvre ensuite des aspects purement juridiques, à travers :
    - l'opposabilité, qui consiste à rendre admissibles les éléments de preuve juridique,
    - l'irréfutabilité (irréfragabilité) qui revient à faire prononcer l'authenticité par jugement.

Pour illustrer cette gradation, l'auteur explique que l'on peut récupérer l'adresse IP de l'auteur présumé d'une tentative d'intrusion (traçabilité), mais qui n'est pas toujours imputable (car il est possible de forger une vraie-fausse adresse IP). Et ainsi de suite, une information traçable et imputable n'est pas toujours opposable ; il faut pour cela qu'elle soit bien formée pour être « admissible en preuve », comme diraient les Anglo-Saxons.

Dans un Système d'Information de Santé qui sert à soigner ou à rembourser, qui permet d'exercer la télémédecine ou le télédiagnostic, il n'est pas rare que les exigences demandées sur chacune des quatre propriétés de base de la sécurité (variant de 0 à 3) soient 3333. C'est-à-dire très élevées.

La sécurité-security est une sorte d'assurance contre les diverses attaques informatiques. Elle permet de diminuer les risques. On parle aussi de sécurité-immunité par similitude avec le langage médical.

Sécurité-safety ou innocuité

Par opposition (bien souvent) à la sécurité-security, la sécurité-safety ou innocuité permet de ne pas nuire à l'intégrité physique des individus (cas des sur-irradiés d'Épinal ou de Toulouse).

La sécurité-safety permet de supprimer les risques aux conséquences catastrophiques pour l'environnement et/ou les individus. D'un côté on a la sécurité informatique et de l'autre la sécurité des biens et des personnes : un seul mot en français pour deux notions bien différentes.

On peut déjà imaginer que certains cas de piratages vont vouloir attaquer des systèmes qui soignent, pour « mal soigner ». Ainsi, une défaillance en sécurité-security (système mal protégé, mauvais contrôle d'accès, mauvais positionnement des architectures sécurité) peut laisser la porte ouverte à un défaut de sécurité-safety.
C'est vrai dans le monde médical, mais aussi dans le monde nucléaire (système de « command-control ») ou ferroviaire (transport automatisé sans chauffeur), où l'on peut imaginer qu'un défaut de sécurité informatique peut entraîner une défaillance de la sûreté nucléaire, de la sûreté ferroviaire ; toutes ces notions sont englobées par cette notion générique qu'est la sûreté de fonctionnement.

PSSI – Politique de Sécurité du Système d'Information

La démarche sécurité a tendance à dire ce que l'on a le droit de faire et ce que l'on n'a pas le droit de faire.
Il y a quatre domaines principaux de santé.
Chaque secteur peut avoir sa propre politique de sécurité. Elles ne se parlent pas forcément intelligemment, mais elles doivent être cohérentes les unes avec les autres.
Il faut tenir compte de la globalité.
Il faudrait prendre en compte les propriétés de la sûreté de fonctionnement pour traiter les systèmes dans leur globalité.

Politique d'anonymisation

Les trois formes de la politique d'anonymisation, pour les Systèmes d'Information de Santé, définies dès 1998 dans un document normatif élaboré pour l'AFNOR (le FD S 97-560), sont :

- irréversibles (la vraie anonymisation) ;
- inversibles (autorisation, par la loi, de lever l'anonymat pour retrouver des patients contaminés) ;
- réversibles (cas du chiffrement/déchiffrement ; mais est-ce vraiment de l'anonymisation).

La sphère santé s'est intéressée de très près à l'anonymisation depuis le milieu des années 1990, à la suite du plan Juppé, lorsque les politiques ont souhaité une MMDES — Maîtrise Médicalisée (et non comptable) de l'Évolution des Dépenses de Santé.

Ce type de système consiste à chaîner entre eux tous les épisodes de soins relatifs à une même personne dans le cadre du déploiement d'une version anonymisée du PMSI — Programme de Médicalisation du Système d'Information ; cela permet de rendre plus fiable les statistiques individualisées (mais anonymisées) de consommations de soins. On a ainsi pu anonymiser tous les épisodes de soins, toujours et partout de la même façon pour une même personne concernée : on parle alors de pseudonyme.

La loi informatique et libertés impose le respect de l'intimité de la personne, même après son décès ; et ce type de système d'anonymisation, irréversible par construction, permet de respecter les exigences de la loi. La sphère santé/social a été un précurseur, en la matière.

DMI — DMP

Dossier Médical Personnel

En France, le Dossier Médical Informatisé (DMI) s'appelle, après de multiples évolutions, le Dossier Médical Personnel (DMP). D'autres pays n'ont pas atteint à ce point de finesse et de maturité. De nombreux concepts ont été implémentés dans le domaine de la santé pour et autour du DMP :

- la carte de Professionnel de Santé (CPS) ;
- la carte Vitale ;
- des Réseaux de soins thématiques ;
- le Dossier Pharmaceutique (DP) ;
- des Dossiers médicaux Régionaux ;
- le Dossier Communiquant de Cancérologie (DCC) ;
- le Dossier Médical Électronique Partagé (DMEP), précurseur du Dossier Médical Personnel (DMP).

Le DMP serait sans doute très vite nécessaire et même hautement indispensable dans les cas suivants :

- des pathologies chroniques ;
- des asthmatiques ;
- des diabétiques ;
- des gens qui auraient besoin de nombreux épisodes de soins.

Diverses expérimentations et mises en œuvre ont été menées et le DMP est désormais officiellement opérationnel. Mais quelle confiance peut-on accorder au DMP : il est censé être médical ; il est souvent décrit, à tort, comme très lié à une maîtrise comptable et lié à l'Assurance-maladie ?

Dans l'optique de préserver l'intimité du patient et de respecter sa vie privée, il est possible de masquer certaines informations dans le DMP. Ces informations sont-elles inavouables ou absentes ? absentes parce que non demandées, non fournies ou tout simplement non renseignées ?

Dans ces circonstances : quelle est la fiabilité ou la confiance dans un tel système ?
Qui veut vraiment avoir un DMP ?
Pourquoi, disons, 80 à 100 % de la population devraient absolument avoir un DMP ?
Pour réduire le déficit de la sécurité sociale ?
Pour avoir un meilleur contrôle et une meilleure maîtrise de notre santé publique ?
Ce sont autant de questions qui se posent régulièrement autour de la légitimité et de l'exploitation d'un DMP à la française.

L'exemple réussi du Projet ELFE

L'INED a piloté le projet ELFE, Étude Longitudinale des Familles et de l'Enfance. Ils ont démarré une cohorte qui sera suivie pendant 10, 20 peut-être 30 ans avec un système très sécurisé. On y capte des données dès la naissance du nouveau-né (poids, taille, extrait de sang du cordon ombilical…), s'il fait partie de la cohorte.

Le but est de faire des études scientifiques en tous genres. Il sera possible de croiser les données de façon anonyme. Chaque équipe de chercheurs doit être habilitée. Chaque thématique de recherche doit être habilitée. Chaque requête adressée à la base de données de ELFE doit être habilitée. Il est alors possible de croiser la santé avec la scolarité, avec le social et avec toutes sortes de données qui peuvent aider à mieux comprendre certaines pathologies. On parle alors d'appariements dits « sécurisés ». Il n'y a pas de base centrale directement exploitable, car le but n'est pas de savoir quel individu a quelle pathologie, mais de faire des études statistiques sur cette cohorte, afin d'en tirer des enseignements pour, notamment, améliorer les démarches de santé publique.

Le rapport AFNOR FDS 97-560 – « Fascicule de Documentation de Santé – Glossaire et Terminologie pour l'anonymisation dans la santé » avait décrit la méthodologie générale d'anonymisation. Il y était proposé toutes ces techniques d'anonymisation et, quinze ans plus tard, ces notions sont implémentées dans le projet ELFE, en utilisant autant d'anonymisations chaînables que nécessaire : on parle de pseudonymes et cela permet de retrouver un peu de la confiance qui avait peut-être été perdue, dans ce genre de système.

Parmi les échanges avec la salle

Identifiant de santé

Un identifiant de santé spécifique va être créé. Certains pays abandonnent l'identifiant de santé spécifique, considérant que c'est une charge inutile n'apportant pas de sécurité. Ce sont les données qui doivent être protégées. Dans le système bâti autour du DMP, on met toutes les informations ensemble alors que dans d'autres pays, on va chercher les données là où elles sont protégées et quand on en a besoin. Ce serait plutôt dans la logique du projet ELFE.

L'identifiant de santé est une problématique manifestement très complexe, du point de vue sociétal entre autres ; il s'est successivement appelé :

- IPP — Identifiant Permanent Patient ;
- IPS — Identifiant Permanent Santé ;
- INS — Identifiant National Santé :
  - INSC — calculé (dans un premier),
  - INSA — aléatoire (dans un proche avenir).

C'est une alternative au N° INSEE qui a été créé sous Vichy et qui ne peut juridiquement pas servir d'identifiant de santé. En 1999, il a été décidé que le N° INSEE ne servirait jamais comme identifiant santé. Dans la carte SESAM VITALE, l'identifiant est actuellement encore familial ; en fait on parle de « donnant droits » envers ses « ayants-droits ». Pourtant, le N° INSEE est généré à la naissance pour chaque individu et, ainsi, quand on a mis en place l'anonymisation du PMSI, il reposait, en partie, sur le numéro dit, abusivement, « de Sécurité Sociale » famille (celui du « donnant-droits »).

Loi Kouchner

La France est le seul pays à avoir précisé, avec la loi Kouchner de 2002, que les données étaient sous le contrôle des individus, ce qui donne, en théorie, à chacun un libre accès à ses propres données médicales : Cela ne pose-t-il pas là aussi un problème de confiance dans les données restituées si l'on sait qu'elles le seront.

Dans le code déontologique du médecin il est rappelé que : « Le médecin doit, à son patient, une information claire, loyale et appropriée sur son état et les soins qu'il lui propose. La pratique de la médecine est sans but lucratif. ».
Quelle confiance accorder à des systèmes dont il est parfois dit que certains praticiens feraient deux rapports, un pour le patient, un pour eux-mêmes (à travers leurs notes personnelles ou pour communiquer avec leurs confrères) ?

Hébergeur de données de santé

Pour être hébergeur de données de santé, un organisme doit être agréé. Il doit respecter un cahier des charges, inspiré par l'ISO 27002.

Volet d'urgence du dossier médical électronique

En cas d'accident, un volet d'Urgence existe, qui comporte les allergies, les antécédents, les pathologies chroniques ; mais il faut pouvoir savoir (traçabilité, opposabilité) qui a accédé, quand, comment, pourquoi et à quoi.

Accès à un dossier

Lorsqu'on ne peut pas créer un DCC (Dossier Communiquant de Cancérologie), c'est qu'il existe déjà électroniquement ; mais cela donne déjà une information. Il devrait y avoir création d'une enveloppe vide indépendamment de son utilisation future. C'est également une bonne raison pour que tout le monde possède un DMP ; car il faut assurer la confidentialité du message (le contenu) et la confidentialité de l'enveloppe (le contenant). Quelle confiance accorder à de tels systèmes, si cette précaution n'y figure pas ?

AFCDP

L'Association Française des Correspondants à la Protection des Données à caractère Personnel que l'on pourrait appeler Association Française des Correspondants Informatique et Liberté, est étroitement liée à la révision du 6 août 2004 de la Loi Informatique et Libertés : Cette loi a en effet prévu des systèmes d'accréditation ou de certification des experts, produits, systèmes, outils et dispositifs divers (par exemple : un système d'anonymisation) permettant de garantir la vie privée des personnes et la protection des leurs données à caractère personnel. Cette loi a également permis la création officielle de la fonction de CIL – Correspondant Informatique et Libertés.

Depuis 2004, un CIL (ou CPDC : Correspondant à la Protection des Données à Caractère Personnel) peut être ainsi désigné par une organisation (entreprise privée ou administration publique) qui manipule certaines quantités de données à caractère personnel. Cette désignation est proposée à la CNIL qui a la possibilité de l'accepter ou non. Le CIL est le garant de l'absence d'abus sur les données à caractère personnel et doit s'assurer de la conformité à la loi Informatique et Libertés.

L'AFCDP, fédérée autour du métier du CIL, est composée de nombreux juristes et avocats, de quelques spécialistes en sécurité des S.I. et de qualiticiens.

Il avait d'ailleurs été dit, à l'époque, que le CIL était « un mouton à cinq pattes » ; mais le métier prend corps et la corporation s'organise grâce à l'AFCDP et autour de la CNIL.

Open data

Autour de l'émergence de l'Open data, il est désormais considéré que les données générées par les services publics sont des données publiques car ce sont des faits, puisqu'il n'y a pas de création de l'esprit. Un DMP est par conséquent un système contenant des données publiques… mais qui sont soumises au secret médical et donc non publiables : il faudra donc veiller à toujours faire la distinction fondamentale entre « donnée publique » et « donnée publiable », à condition de s'appuyer sur les fondements du secret médical et des lois existantes.

Conclusion

Les propos de Gilles Trouessin placent souvent la barre assez haut tant la sensibilité des données concernées l'exige.

Car s'il est rapidement assez compliqué d'anonymiser tout et toujours efficacement ; il devient assez vite complexe d'essayer de désanonymiser, sauf à avoir construit un système qui croyait anonymiser (au vrai sens du terme), et de conclure : ***« une donnée anonymisée n'est pas pour autant toujours parfaitement anonyme ! ».***

En Californie, en Angleterre, en Espagne, des systèmes d'informations de santé, de gestion de dossiers médicaux se sont fait pirater.
Nous sommes parmi les meilleurs systèmes, en France.
Quel conseil citoyen nous donneriez-vous pour conclure ?
On sait faire beaucoup de choses mais nous n'en sommes encore qu'à la préhistoire de l'informatique dans certains domaines de la santé et à l'âge de pierre de la sécurité par endroits. Pour conclure : ***« évitons de trop souvent et trop gravement tomber malades… !*** » ▲

gilles.trouessin@scassi.com
gilles.trouessin@orange.fr
veronique.pelletier@adeli.org

Sigles et acronymes

ALD	Affection Longue Durée
ANAP	Agence National d'Appui à la Performance des établissements de santé et médico-sociaux
ASIP	Agence des Systèmes d'Information de Santé
CNAM-TS	Caisse Nationale Assurance-maladie – Travailleurs Salariés
CNIL	Commission Nationale de l'Informatique et des Libertés
CPS	Clé Privée de Signature, Carte de Professionnel de Santé
DICA	Disponibilité, Intégrité, Confidentialité, Auditabilité
DMEP	Dossier Médical Électronique Partagé
DMI	Dossier Médical Informatisé
DMP	Dossier Médical Personnel
GIE	Groupement d'Intérêt Économique
GIP	Groupement d'Intérêt Public
GMSIH	Groupement sur la modernisation des Systèmes d'Information de Santé
HAS	Haute Autorité de Santé
INSEE	Institut National de la Statistique et des Études Économiques
MAINH	Mission Nationale d'Appui à l'Investissement Hospitalier
MEAH	Mission nationale d'Expertise et d'Audit Hospitaliers
MMEDS	Maîtrise Médicalisée de l'Évolution des Dépenses de Santé
PMSI	Programme de Médicalisation des Systèmes d'Information
PSSI	Politique de Sécurité du Système d'Information
SI	Système d'information
SIH	Système d'Information Hospitalier
SIS	Système d'Information de Santé
SSI	Sécurité du Système d'Information
TIC	Technologie de l'Information et de la Communication