Ordre des médecins
Orde van geneesheren

Recommandations relatives à la tenue de bases de données médicales contenant des données nominatives ou identifiables

Les données à caractère personnel relatives à la santé sont devenues l'objet d'enjeux commerciaux[1] et ont acquis une valeur marchande et politique. Il s'agit le plus souvent d'informations médicales issues de bases de données médicales personnelles qui sont ainsi commercialisées et utilisées dans une finalité différente de celle qui a justifié leur recueil.
La majorité des projets de serveurs de données médicales ne concernaient jusque l'an 2000 que des professionnels de la santé. Mais l'apparition de sites auxquels des patients confient volontairement leurs données médicales dans le but d'en faciliter l'accès aux médecins qui seraient amenés à les soigner en situation d'urgence pose de nouvelles questions.
En effet ces données sont confiées à des sociétés commerciales dans des conditions de sécurité qui n'ont pas été évaluées.
En Belgique, le traitement des données à caractère personnel est régi par la loi 8 décembre 1992[2] complété l'arrêté royal 13 février 2001[3]. Elle s'applique également aux dossiers de patients que tiennent les médecins. En France l'utilisation à des fins commerciales de données non identifiables issues de prescriptions médicales peuvent être commercialisées selon des modalités conformes à la législation et à la déontologie dans des cas particuliers expertisés par la CNIL[4]. On peut craindre, ainsi qu'il est pratiqué aux USA, que des sociétés détentrices de données personnelles leur confiées par des patients ne soient tentées un jour de leur racheter des données extraites de ces dossiers.
Les échanges de données médicales personnelles se justifient entre médecins dans l'intérêt des patients. Depuis plusieurs années le Conseil national de l'Ordre à établi des lignes directrices et des techniques de sécurisation à mettre en œuvre pour que la confidentialité des échanges soit assurée[5] dans ces cas.
La cryptologie et la signature digitale certifiée sont incontournables en cette matière. La sécurisation des données fait l'objet d'une abondante littérature internationale.[6] [7]
La multiplication de projets de serveurs de données et de serveurs de bases de données pose de nouveaux problèmes qui ont conduit le Conseil national à réfléchir aux règles déontologiques les concernant.

PRINCIPES GÉNÉRAUX

Une série de règles sont d'application pour tout traitement de données personnelles lors de leur récolte, pendant leur introduction et séjour dans une base de données et pendant leur transfert par voie électronique.

Authenticité des données : c'est à dire la garantie que les données sont conformes à la réalité. L'exactitude de leur contenu doit être certifiée par le médecin qui les a constatées, établies ou qui en est responsable. Le praticien concerné doit être identifié et sa qualification connue grâce à une signature électronique certifiée. De la sorte le praticien traitant le patient sera assuré de l'exactitude des données.

Intégrité des données : c'est-à-dire la garantie que les données sont bien celles du patient indiqué, qu'elles n'ont pas été altérées et sont donc conformes à l'original. Leur protection contre les attaques extérieures ou intérieures doit être totale et actualisée, c'est-à-dire utiliser des techniques de protection régulièrement adaptées en fonction des nouvelles données scientifiques et des progrès en la matière. Les attaques peuvent tenter de pénétrer dans la base de données, d'en extraire des données, d'y apporter des modifications pouvant aller jusqu'à sa destruction. Un relevé des tentatives d'accès non autorisé doit être tenu et contrôlé.

Autorisation d'accès : l'accès à tout ou partie d'un dossier médical est fondamentalement conditionné par le statut de « personne soignante, actuellement en charge du patient ». Il est limité aux données dont la connaissance est nécessaire pour l'administration des soins et pendant la durée de ceux-ci[8]. Une hiérarchisation en fonction des compétences et spécialisation de chacun doit être établie, de même qu'une sélection des données entre elles.
Toute demande d'accès à des données médicales personnelles hébergées sur un serveur doit amener la prise en considération de plusieurs critères ou conditions déterminantes :

L'identité et la qualification du demandeur : il peut s'agir d'un médecin ou d'un professionnel de la santé en charge du patient, d'un médecin de confiance choisi par le patient, ou attaché à un organisme assureur, à une assurance privée ou d'un membre du personnel soignant d'un hôpital, ou du patient lui-même qui souhaite consulter son dossier médical. La signature électronique

certifiée doit être utilisée pour vérifier l'identité et la qualité du demandeur lorsque cette demande se fait par voie électronique.

Le type de données concernées : une sélection doit être faite entre les données : données d'urgence, hypothèses documentées, hypothèses confirmées, hypothèses de travail, données génétiques, psychiatriques, données sensibles…

Le degré de confidentialité que leur auteur ou le patient leur aura attribué doit être respecté. Le consentement du patient doit être pris en compte et matérialisé numériquement.

La finalité de la demande doit être clairement définie par le demandeur : gestionnaire du dossier médical global du patient (médecin de famille), médecin appelé à le soigner pour un problème précis (médecin de garde ou médecin spécialiste), situation d'urgence, médecin-conseil d'un organisme assureur, médecin contrôleur, médecin du travail, médecin expert auprès d'une assurance ou d'un tribunal, médecin inspecteur de l'INAMI, etc.

La durée de cet accès est strictement limitée, pour les médecins en charge du patient, à la période pour laquelle le patient consulte le demandeur. Pour les autres médecins l'accès se limite aux données nécessaires à l'exécution de leur mission légale.

La conception d'un projet de serveur de données médicales devra intégrer ces divers facteurs dans une grille matricielle au travers de laquelle la demande d'accès sera filtrée afin de protéger la vie privée des patients et de respecter le secret du médecin.

Traçage des accès. Il est important de conserver une trace probante des transactions électroniques afin de pouvoir prouver, le cas échéant, qu'elles ont eu lieu. Pour y parvenir, seul un notariat électronique peut garantir un traçage des transactions. Ce notariat devrait être réalisé non au sein du serveur mais auprès d'un organisme tiers qui pourra jouer le rôle de témoin de l'échange de documents. L'identité du demandeur lui sera transmise.

Confidentialité des données : les données personnelles des patients sont couvertes par le secret professionnel du médecin (code pénal art 458, code déontologie art.55 à 70). C'est la sécurisation et la grille des droits d'accès aux données qui conditionnent leur confidentialité. Les médecins ne sont pas autorisés à confier des données personnelles à des systèmes informatiques qui n'offrent pas ou insuffisamment ces conditions.

Contenu : seules les données objectives concernant un patient font partie de son dossier et peuvent être conservées dans une base de données médicales nominative. Il est d'importance particulière que le dossier médical informatisé d'un patient soit tenu à jour. Ceci implique l'accès des médecins actuellement en charge du patient à ce dossier et l'accord des parties d'y ajouter les nouvelles données objectives.
Pérennité de la base de données sur Internet : La durée de conservation des données médicales est actuellement de 30 ans[9] après le dernier contact avec le patient, sauf situation particulière. La conservation du dossier informatisé dans une base de données centrale doit être d'une durée au moins identique. La question se pose donc du devenir des données collectées en cas de disparition de l'organisme collecteur. Une société civile ne peut garantir sa propre durée d'existence. L'on ne peut admettre la collecte de données nominatives dans un but thérapeutique par des sociétés qui ne seraient pas à même d'en assurer la conservation pendant les délais légaux et déontologiques.

Déclaration des fichiers : La loi 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel prévoit les conditions auxquelles ces traitements doivent satisfaire.[10] Le traitement automatisé doit être déclaré auprès de la commission de protection de la vie privée. Cette déclaration doit comprendre notamment la finalité pour laquelle ces données sont recueillies.

Responsabilité médicale : l'enregistrement par le médecin de données personnelles médicales dans une base de données engage la responsabilité du médecin qui a la charge du patient. Il est donc recommandé de se limiter aux données objectives documentées, datées et dont l'auteur est identifié.

Standards informatiques : un cadre commun d'interopérabilité pour les échanges et la compatibilité des systèmes doit être mis en œuvre. Il s'agit ici d'une initiative qui relève des pouvoirs publics. De la sorte l'échange de données entre divers utilisateurs sera rendu possible.

Systèmes destinés à l'information des services d'urgence

Il s'agit de renseignements médicaux jugés utiles, accessibles sur Internet par des médecins inconnus qui seraient amenés à donner des soins urgents aux patients participant au système. L'accès se fait habituellement au moyen d'un code en possession du patient.
Sans nier son utilité dans certains cas, il importe de noter qu'aucune preuve scientifique d'amélioration de la qualité des soins urgents n'a été apportée[11] grâce à cette méthode. En effet, tous les services d'urgences vérifient toujours immédiatement une série de paramètres tels le groupe sanguin, la glycémie, l'ecg, etc. Par contre une information des médecins, urgentistes ou autres, est indiscutablement utile dans d'autres cas urgents tels les réactions anaphylactiques graves, les épilepsies… Une mention de ces pathologies sur un document conservé par le malade auprès de ses documents d'identité répond avantageusement à ce besoin : meilleure sécurité, simplicité d'accès.

Authenticité des données :
a. Les données introduites par le patient peuvent être sujettes à caution. En effet le patient n'est pas nécessairement informé quant à leur importance, leur pertinence, leur signification, leur exactitude. Par exemple, s'il peut être vital de connaître les grandes allergies médicamenteuses on ne peut se baser sur une liste d'allergies signalées par le malade qui risque de donner soit des renseignements inexacts, soit trop de renseignements. Du reste les documentations des sociétés concernées « conseillent de se faire aider par son médecin traitant habituel ».
b. La validation médicale est en effet indispensable. Elle engage la responsabilité du médecin et doit être matérialisée sur le serveur par sa signature.
c. Si les données sont introduites par un médecin la responsabilité de ce dernier peut être engagée. Le médecin doit au moins avoir la certitude que les données n'ont pu ou ne pourront être altérées. Il doit se limiter aux données objectives documentées et s'identifier.
d. Le problème de l'actualisation permanente des données n'est pas résolu lorsque le patient en assume la responsabilité. Elle pourrait l'être lorsque cette tâche est à la charge du médecin, qui l'aurait acceptée.

Confidentialité des données : la protection des données personnelles identifiées doit être assurée pendant leur circulation sur Internet (cryptage et signature certifiée) tout comme durant leur séjour sur le serveur de la base de données : protection contre les accès non autorisés, les attaques de hackers, contre toute modification non autorisée, mais également contre la violation de la vie privée du patient par la société responsable elle-même.
Un simple code d'accès constitue une protection insuffisante. De plus lorsque le patient est le détenteur du code il pourrait être obligé, sous contrainte morale ou par manque d'information, de fournir le contenu de son dossier dans un but non thérapeutique.
Responsabilité médicale de l'utilisateur des données : Le médecin qui sera amené à utiliser ces données lorsqu'il dispense ses soins, engage dangereusement sa responsabilité s'il base son attitude thérapeutique sur des données qui n'ont pas été validées. D'où besoin de sécurité, d'authenticité et de confidentialité.
Les problèmes liés à la pérennité de la base de données et à la déclaration des fichiers sont également d'application pour ces systèmes.

Systèmes de transfert de Données confidentielles entre médecins
L'envoi de documents médicaux sous forme numérique se développe et tend à se substituer progressivement aux classiques échanges postaux. L'attention a été maintes fois attirée sur l'insécurité des échanges par voie électronique. Plusieurs recommandations du Conseil national sont consacrées aux conditions requises en vue d'assurer la sécurité de ce type de transmission[12] [13].
La communication électronique de documents entre médecins peut être directe ou se faire par l'intermédiaire d'un fournisseur de services de courrier (messagerie électronique).
Dans les deux cas les règles de sécurité doivent être respectées. Parmi celles-ci la cryptographie et la signature électronique certifiée occupent la première place.

L'encryptage doit être asymétrique et faire appel à des algorithmes éprouvés ; la clé de cryptage doit être de longueur suffisante. Lors de leur utilisation le logiciel doit contenir toutes les mesures nécessaires à la protection de la clé privée.

La signature électronique du médecin doit être certifiée conformément aux dispositions légales[14] [15].
Cette signature, apposée sur un document numérisé, doit authentifier l'identité et la qualité du médecin au même titre que sa signature manuelle sur papier. Elle offre l'avantage complémentaire de certifier l'intégrité du document signé.
Dans l'état actuel, malgré les recommandations et législations, les systèmes commerciaux de messagerie électronique ne fournissent pas de signature électronique certifiée conforme à la législation et ne permettent pas l'envoi de documents médicaux en dehors de leur propre cercle de clients. L'échange de données est donc très limité sur le terrain faute d'interopérabilité. Ceci entraîne une limitation sévère dans la distribution

électronique du courrier médical et constitue un obstacle sérieux à l'extension et à l'universalisation de ce service. De plus, le recours à des systèmes notoirement insuffisants d'identification des médecins expose à des failles de sécurité.
Les recommandations du Conseil national[16]restent d'application actuelle :
1. Seul un médecin, personne physique, peut transmettre et recevoir des données médicales couvertes par le secret professionnel du médecin. Au sein d'une institution, le médecin qui transmet ou reçoit des données médicales, ne peut le faire qu'en son nom. C'est donc la signature personnelle du médecin expéditeur responsable, tout comme sur un document papier, qui doit valider et certifier le contenu du document expédié.
2. Le cryptage par un système à double clé, encore dénommé système mathématique asymétrique, assure une sécurité satisfaisante.
3. Le médecin génère lui-même les clés sur son ordinateur personnel au moyen d'un logiciel obtenu auprès d'un fournisseur indépendant.
4. Afin d'authentifier la signature électronique, la clé publique de signature devra être certifiée par un prestataire de service de certification délivrant des certificats qualifiés et indépendant du serveur de messagerie.
5. L'accès à la clé secrète est définitivement limité au seul propriétaire de celle-ci.
6. L'algorithme utilisé doit être connu et de longueur suffisante tant pour sa partie symétrique que pour la partie asymétrique.
7. Le cryptage et le décryptage des données seront réalisés respectivement dans l'ordinateur de l'expéditeur et du destinataire. En aucun cas, ces opérations ne pourront avoir lieu au sein d'un ordinateur intermédiaire consacré ou lié à la messagerie.
Le Conseil national a mis sur pied une infrastructure de clés publiques permettant à chaque médecin inscrit d'obtenir une clé certifiée conformément aux dispositions légales et en recommande l'utilisation dans l'échange de données médicales par voie électronique. Chaque médecin est invité à prendre contact avec son Conseil provincial afin d'entamer la génération de son identification numérique certifiée par l'Ordre des médecins et d'inviter son service télématique à utiliser cette identification.

Serveurs de Bases de données médicales

Les données peuvent être conservées selon le cas sur le disque d'un ordinateur individuel, au sein d'un système d'archivage central dans les institutions de soins ou au sein d'un serveur centralisé destiné à la distribution de services.
Dans tous les cas des **mesures de sécurisation** fiables doivent être d'application. Elles concernent tant la protection physique des installations tout comme la protection contre la destruction accidentelle de données ou contre les accès non autorisés aux données stockées. De même la pérennité de la base de données doit être garantie.
L'importance des **mesures de contrôle des accès** est proportionnelle au nombre et aux qualifications diverses des individus susceptibles d'avoir autorisation d'accès. Il en va de même pour les mesures de protection.

[1] La commercialisation des informations médicales est-elle « déontologiquement correcte » ?Conseil National de l'Ordre des médecins, France 29-30 juin 2000.
[2] Loi du 8 décembre 1992 relative à l'égard des traitements de données à caractère personnel
[3] Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. 13 février 2001.
[4] Commission Nationale Informatique et Liberté. France.
[5] Recommandations relatives à la protection de la confidentialité lors de la transmission de données couvertes par le secret médical. Bull. Conseil Nat., 92 p4, 17 février 2001.
[6] Hanka, R., Buchan, I.E. : Security measures in open communication systems. hanka@medschl.cam.ac.uk
[7] CEN/TC 251/Wi 6.10: Framework for Security of Health Care Communication.
[8] Droits d'accès au dossier, Dossier Médical Global informatisé. Bull. Conseil Nat.,84,p13. 12 décembre 1998.
[9] Code de déontologie médicale, art. 46.
[10] Voir à ce propos, l'avis du Conseil national du 18.01.1997, Bull. Conseil Nat. 75 p: 13.
[11] Commission Télématique du Ministère de la Santé Publique, 12 novembre 2001.
[12] Communications électroniques. Bull. Conseil Nat. 69 p. 13, 22 février 1995
[13] Recommandations relatives à la protection de la confidentialité lors de la transmission de données couvertes par le secret médical. Bull. Conseil Nat, 92 p4, 17 février 2001.
[14] Directive 1999/93/CE du Parlement européen et du Conseil, du 3 décembre 1999, sur un cadre communautaire pour les signatures électroniques
[15] Loi relative à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques. 14 juin 2001.

[16]Recommandations relatives à la protection de la confidentialité lors de la transmission de données couvertes par le secret médical. Bull. Conseil Nat, 92 p4, 17 février 2001