Sécurité des systèmes d'information dans le milieu médical

ARGAUS accompagne l'ensemble des acteurs du monde médical dans leur formation et la sécurisation de leurs données. Cette fiche présente les objectifs à atteindre pour les professionnels de ce secteur.
Elle s'adresse : aux directeurs d'hôpitaux, de cliniques, aux responsables de systèmes d'information, cadres et professions libérales de la santé, et chefs de service paramédicaux.

C'est en 1810 que le Code Pénal officialise pour la première fois le secret en le liant au corps médical. Précisé dans le Code de déontologie médicale, sa rédaction au sein du Code de la Santé Publique (CSP) lui confère d'abord une portée réglementaire. L'article R4127-4 CSP dispose ainsi que « Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi. ». Si cette obligation vise la communication et la transmission de ces données en les assortissant d'une sanction pénale (art 226-13 et -14 Code pénal), le stockage de ces dernières sur des supports numériques a engendré de nouveaux enjeux.

L'encadrement général fixé par la loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été ces dernières décennies revu et précisé afin de garantir dans l'usage des systèmes informatisés tant le droit au respect de la vie privée que le secret médical.

Si l'ensemble du dispositif législatif et réglementaire est globalement satisfaisant, sa mise en œuvre et l'émergence de nouvelles technologies démontrent certaines limites. Fondée sur le respect de la vie privée et le secret médical, la protection des données personnelles des patients fait ainsi l'objet d'une protection légale ancienne et efficace (I). Si elle a été progressivement complétée en vu d'assortir de garanties l'usage de nouvelles technologies, la réglementation actuellement en vigueur est appliquée de façon parfois lacunaire au sein des établissements (II).

I) Fondée sur le respect de la vie privée et le secret médical, la protection des données personnelles à caractère médical fait l'objet d'une protection légale ancienne et efficace

A) Le droit au respect de la vie privée et au secret des informations médicales du patient implique pour le professionnel de santé de garantir leur confidentialité

La loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés pose ainsi les principes de bases concernant le traitement des données revêtant un caractère personnel. L'objectif général est d'assurer le respect de la vie privée des administrés dès lors que ces informations font l'objet d'un processus de stockage et de transmission. Elle vise l'ensemble des services exerçant une mission de service public (établissements publics de santé, administrations, cliniques...). Son article 34 impose notamment que des dispositions soient prises pour assurer la sécurité des traitements et informations, ainsi que la garantie des secrets protégés par la loi. Cette obligation légale d'assurer personnellement la sécurité des traitements impose aux professionnels de santé le respect de référentiels de sécurité.

En pratique, ces derniers doivent prendre toutes précautions utiles pour empêcher que les données ne soient modifiées (*intégrité de l'information)*, effacées par erreur (*disponibilité*), ou que des tiers non autorisés aient accès au traitement (*confidentialité*). Ils sont donc tenus de mettre en œuvre :

- des mesures de sécurité physique par un accès contrôlé aux locaux hébergeant les serveurs et par la mise en œuvre d'une procédure permettant de restreindre l'accès aux seules personnes habilitées ;
- des mesures techniques par la protection des serveurs via des pare-feux, filtres anti-spam et anti-virus, l'accès aux postes de travail par des mots de passe individuels régulièrement renouvelés, l'utilisation de la Carte de Professionnel de Santé pour accéder aux données, le chiffrement des données, etc. [1]

La Commission Nationale Informatique et Liberté (CNIL), Autorité Administrative Indépendante (AAI) créée par cette même loi de 78 assure aux côtés des tribunaux le respect et la sanction des manquements à ces obligations.

Le respect du secret médical est l'autre principe qui guide l'évolution des normes encadrant le traitement des données médicales. Défini dans la partie réglementaire du Code de la Santé Publique (CSP Art. R4127-1) comme s'imposant à tout médecin et couvrant tout ce qui est venu à sa connaissance dans l'exercice de sa profession, le principe a été ensuite élevé au niveau législatif par sa codification à l'article L 1110-4 du CSP (loi du 4 Mars 2002 « Kouchner »).

La jurisprudence avait eu l'occasion de se prononcer sur la portée de ce principe en conférant au secret médical un caractère général et absolu. La Cour de Cassation l'a affirmé la première, dès le XIX° siècle (1885, arrêt Watelet) et surtout dans un arrêt de la chambre criminelle du 8 mai 1947 (Degraene) :

«L'obligation du secret professionnel s'impose aux médecins comme un devoir de leur état. Elle est générale et absolue et il n'appartient à personne de les en affranchir». Cette portée générale et absolue du secret médical est reconnue également dans les arrêts du Conseil d'État (arrêt d'assemblée du 12 avril 1957 – Deve). [2]

Le dispositif visant la sécurisation du matériel destiné à recevoir ce type d'information est lui fondé sur un système de certification et d'agrément par des AAI :

- les logiciels permettant la facturation et la télétransmission des données ainsi que le lecteur de carte Vitale (SESAM) doivent faire l'objet d'un agrément ;
- la Carte de Professionnel de Santé, permettant de signer électroniquement les actes et d'avoir accès aux informations contenues dans la carte vitale est délivrée par les Agences Régionales de Santé ;
- les fichiers patients doivent impérativement être déclarés à la CNIL. [3]

Si ce système permet d'assurer un certain niveau de sécurité, il n'a pas empêché récemment la divulgation de données médicales (révélation de données d'une patiente des Hôpitaux de Marseille, de l'hôpital Foch de Suresne ou encore du Pôle de santé de Plateau). Ces dernières étant dues le plus souvent à des négligences humaines, l'effort déjà entrepris dans la formation des cadres devrait être accentué en direction du personnel. L'utilisation des dispositifs classiques (plan interne de formation, charte informatique) est à ce titre un bon moyen de sensibiliser les collaborateurs pour réduire le risque humain.

B) Le manquement aux obligations légales concernant le stockage comme la transmission non autorisée de données fait l'objet de sanctions pénales dissuasives

L'absence de déploiement de mesures de sécurité technique ou la négligence dans leur déploiement sont considérées comme des atteintes graves à la protection de la vie privée des personnes et sont sanctionnées pénalement (jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende – Art. 226-17 du Code pénal). La violation du secret médical est quant à elle punie d'un an d'emprisonnement et de 15.000 euros d'amende.

La loi Kouchner de 2002 pose également le principe suivant lequel seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier : il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des tiers autorisés ayant qualité pour les recevoir de façon ponctuelle et motivée.

L'atteinte à la confidentialité de ces données est qualifiée et punie par deux incriminations : l'infraction visée par l'article 226-22 du Code Pénal est constituée lorsque d'une part, des informations sont communiquées à des personnes non autorisées (punition de 5 ans d'emprisonnement et 300.000 euros d'amende), d'autre part lorsqu'elles sont divulguées par imprudence ou négligence (punition de 3 ans d'emprisonnement et 100.000 euros d'amende).

Concernant l'échange de données entre professionnels, la garantie de la confidentialité des informations médicales est assurée en soumettant les systèmes de conservation sur support informatique et de transmission par voie électronique aux règles préconisées par le Conseil d'État. Les mesures à respecter sont définies par décret, après avis public et motivé de la CNIL. Le fait d'obtenir ou de tenter d'obtenir la communication de ces données en violation de cette disposition est puni d'un an d'emprisonnement et de 15.000 euros d'amende. (Art. L1110-4 CSP). [4]

II) Progressivement complété en vu d'assortir de nouvelles garanties l'usage de nouvelles technologies, le dispositif actuellement en vigueur révèle certaines limites dans sa mise en œuvre

A) La sécurité de la Carte de Professionnel de Santé fait l'objet d'un encadrement rigoureux en raison de son contenu stratégique

Le contenu de la carte est précisé à l'article R161-52 du Code de la Sécurité Sociale. Cette dernière contient ainsi les identifiants du professionnel de santé ainsi qu'un « Domaine Assurance Maladie » contenant des données relatives aux situations d'exercices et de facturation. Ces informations conventionnelles et de nature financière sont à l'usage exclusif de l'Assurance Maladie. La carte permet en outre d'accéder au Dossier Médical Patient (DMP). Sur le plan juridique, elle peut être utilisée pour effectuer des signatures électroniques. [5]

Au vu de cet usage stratégique et des risques de divulgations de données, la mise en circulation et le contrôle de l'utilisation de cette carte sont strictement encadrés.

Ainsi, la création, la consultation et l'alimentation du DMP s'opèrent via une connexion sécurisée. Les données sont conservées sous forme chiffrée sur un serveur national géré par un hébergeur agréé par le ministère en charge de la santé : l'Hébergeur de données de santé à caractère personnel. Ce dernier agit sous le contrôle et la responsabilité de l'Agence des Systèmes d'Information Partagés (ASIP) de Santé. Il ne peut pas accéder aux données d'un DMP. Celles-ci ne sont accessibles qu'aux seuls professionnels de santé autorisés par le patient.

L'accès au DMP de tout autre acteur (médecins du travail, employeurs, assurances…) est formellement interdit et constitue conformément à l'article 323-1 du Code Pénal un délit passible d'une amende de 15.000 euros et d'un an d'emprisonnement. [6]

B) Malgré des obligations légales fortes pesant sur les données externalisées, le niveau de sécurité atteint dans leur stockage demeure perfectible

Deux modalités organisent l'externalisation des données de santé :

- *la sous-traitance* : le professionnel ou l'établissement de santé peuvent décider d'externaliser une partie du traitement des données des patients. Dans ce cas, le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité telles que prévues par la loi. A ce titre, le contrat conclu entre le sous-traitant et le professionnel de santé doit détailler les obligations du sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoir que le sous-traitant ne peut agir que sur instruction du responsable du traitement ;

- *l'hébergement de données de santé par un tiers :* en cas d'hébergement par un tiers, le professionnel ou l'établissement de santé devra s'assurer que le prestataire met en œuvre des mesures de sécurité suffisantes. À ce titre, ce dernier doit faire héberger les données de ses patients chez un prestataire agréé par le ministre chargé de la santé, conformément aux articles L1111-8 et r1111-9 du CSP.

L'obtention de l'agrément est soumise à la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données hébergées ainsi que d'une politique de confidentialité et de sécurité. L'hébergeur doit ainsi démontrer sa capacité à assurer la confidentialité, la sécurité, l'intégrité et la disponibilité des données de santé qui lui seront confiées par les professionnels de santé. La prestation d'hébergement fait l'objet d'un contrat avec le professionnel ou l'établissement de santé, détaillant notamment les prestations fournies et les modalités d'accès aux données. [7]

L'application de cette réglementation présente toutefois des lacunes. D'une part des données de santé de patients identifiés sont ainsi régulièrement accessibles par des sous-traitants intervenant en milieu hospitalier, dans des laboratoires d'analyses, ou ont été rendues accessibles en ligne. La cause se trouve souvent dans une négligence du personnel. A titre d'illustration, la CNIL, par une délibération du 25 septembre 2013, a mis en demeure publiquement le centre hospitalier de Saint-Malo pour non-respect de la confidentialité des données.

D'autre part le fait que rien ne s'oppose à ce qu'une base de données de santé à caractère personnel soit hébergée en dehors du territoire national peut également poser une limite quant au contrôle de leur sécurité. En effet la directive communautaire 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données établit un cadre de protection des données à caractère personnel équivalent à l'ensemble des pays membres de l'Union européenne. Cette directive a été transposée en France par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

De plus le transfert de données de santé à caractère personnel vers un pays tiers à l'Union européenne peut être exceptionnellement autorisé sur la base des articles 68 et 69 de la loi du 6 janvier 1978. En principe interdit, ce transfert est rendu possible à travers des mécanismes permettant de s'assurer du niveau de protection adéquat des données :

- la Commission européenne a reconnu comme présentant un niveau de protection adéquat, les pays suivants : Canada, Suisse, Argentine, territoires de Guernesey, de Jersey et de l'Ile de Man ;

- les Biding Corporate Rules (BCR) ou règles internes d'entreprises : règles adoptées au sein d'un groupe multinational. Elles doivent revêtir un caractère contraignant et être respectées par les filiales du groupe ;

- les Clauses Contractuelles Types : ce sont des modèles de clauses contractuelles adoptées par la Commission européenne permettant d'encadrer les transferts de données à caractère personnel ;

- le Safe Harbor : c'est un ensemble de principes de protection concernant les entreprises

étasuniennes négociés par les autorités et le Commission européenne en 2001. Les entreprises adhérentes au Safe Harbor doivent se conformer à un ensemble d'exigences de protection des données et assurent ainsi un niveau de protection adéquat. [8]

En conclusion, s'il semble que le dispositif légal encadre de façon cohérente la problématique de la transmission et du stockage des données de santé, il se pose néanmoins le problème de sa déclinaison au sein des équipes. Dans la mesure où le risque est avant tout humain, rendre obligatoire une sensibilisation poussée des salariés permettrait de réduire efficacement ce dernier.

Sur un autre plan, la possibilité ouverte par la directive de 95 d'externaliser les données médicales en dehors du territoire national, voire même européen, pose le problème de l'évaluation de leur niveau de sécurité. Sa transposition ayant donné lieu à des interprétations différentes au sein des États, les législations nationales sur ce point apparaissent fragmentées. L'initiative de la Commission de publier une proposition de règlement le 25 Janvier 2012 peut être saluée dans la mesure où ce dernier permettrait un encadrement plus strict de ces données stratégiques au sein des États. Si ce dispositif réglementaire se révèle plus rigoureux, il ne sera pleinement efficient que s'il est couplé avec une uniformisation des formations à destination du personnel.

Auteurs

Nicolas SAILLEAU	Chargé de développement, ARGAUS SAS	Rédacteur	v1.1 – 07/08/2014
Maxime ALAY-EDDINE	Président, ARGAUS SAS	Relecteur	v1.1 – 07/08/2014

Bibliographie

[1] http://www.village-justice.com/articles/Donnees-sante-obligations-securite,15638.html
[2] http://www.conseil-national.medecin.fr/article/article-4-secret-professionnel-913
[3] http://esante.gouv.fr/services/espace-cps/qu-est-ce-que-la-carte-cps
[4] http://esante.gouv.fr/services/reperes-juridiques/le-cadre-juridique-du-partage-d-informations-dans-les-domaines-sanitaire
[5] http://esante.gouv.fr/services/espace-cps/qu-est-ce-que-la-carte-cps
[6] http://www.installation-infirmiere.fr/index.php/logiciel-et-teletransmission/59-la-teletransmission
[7] http://www.village-justice.com/articles/Donnees-sante-obligations-securite,15638.html
[8] http://esante.gouv.fr/services/referentiels/securite/hebergement-faq#13

Textes de loi

- Art r4127-4 Code de santé publique
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006912862&cidTexte=LEGITEXT000006072665
- Art 226-13 Code pénal
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417945&cidTexte=LEGITEXT000006070719
- Art 226-14 Code pénal
http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417946&dateTexte=&categorieLien=cid
- Art L 1110-4 Code de santé publique
http://www.legifrance.gouv.fr/affichCodeArticle.do;?idArticle=LEGIARTI000020886954&cidTexte=LEGITEXT000006072665
-Art 226-17 Code pénal
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417964&cidTexte=LEGITEXT000006070719
- Art 226-22 Code pénal
http://www.legifrance.gouv.fr/affichCodeArticle.do;?idArticle=LEGIARTI000006417984&cidTexte=LEGITEXT000006070719
- Art r161-52 Code de la sécurité sociale
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006747430&cidTexte=LEGITEXT000006073189
- Art 323-1 Code pénal
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719
- Art L 1111-8 Code de santé publique
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719
- Art L 1111-9 Code de santé publique
http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000006685785&dateTexte=&categorieLien=cid
- Délibération CNIL n°2013-271
http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Bureau/2013-271_bureau_Publicite_Med_CH_ST-MALO.pdf
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995
http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046
- Loi du loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&categorieLien=id