Village de la Justice Village-justice.com

Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé. Par Betty Sfez, Avocat.

jeudi 21 novembre 2013

Adresse de l'article original :
http://www.village-justice.com/articles/Donnees-sante-obligations-securite,15638.html

Les données de santé sont considérées comme des informations sensibles, et à ce titre, sont soumises à un haut niveau de sécurité, physique et technique. Toutefois, les médias rapportent régulièrement l'existence de fuites de données de patients, par des centres hospitaliers ou des laboratoires d'analyses médicales, retrouvées sur la Toile. [1]

Les professionnels et établissements de santé sont ainsi légalement tenus de préserver la sécurité et la confidentialité des données de leurs patients, le recours à la sous-traitance pour certains traitements de données ou leur hébergement, ne déchargeant pas les professionnels des obligations, comme vient de le rappeler la CNIL.

1. Les obligations de sécurité et de confidentialité des données des patients pesant sur les professionnels de santé

Les informations relatives à l'état de santé physique et psychique d'un patient sont considérées par la loi comme des données sensibles. Le traitement de ces données, notamment leur collecte, utilisation, communication, stockage, destruction, est soumis à des conditions particulières définies dans la loi Informatique et Libertés (art. 8, 34 et 35) et le Code de la santé publique.

Les professionnels et établissements de santé sont tenus de respecter les obligations relatives aux traitements de données à caractère personnel, en leur qualité de responsable du traitement. Parmi ces obligations, la sécurité des données constitue un impératif.

Le Code de la santé publique dispose, en outre, que toute personne prise en charge par un professionnel ou un établissement de santé a droit au respect de sa vie privée et au secret des informations la concernant. Les professionnels de santé, ainsi que ceux intervenant dans le système de santé, sont soumis au secret médical (art. L.1110-4).

Le Code de la santé publique impose aux professionnels de santé le respect de référentiels de sécurité. En pratique, ces professionnels doivent prendre toutes précautions utiles pour empêcher que les données ne soient modifiées, effacées par erreur, ou que des tiers non autorisés aient accès au traitement. 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 d'habilitation permettant de restreindre l'accès aux seules personnes habilitées, et

- *des mesures techniques* par la protection des serveurs par des firewalls, filtres anti-spam et anti-virus, l'accès aux postes de travail par des mots de passe individuels et régulièrement renouvelés, l'utilisation de la carte de professionnel de santé pour accéder aux données, le chiffrement des données, etc.

Afin de garantir la sécurité et la confidentialité des données, il est recommandé aux directeurs d'établissements de santé, publics comme privés, de sensibiliser leur personnel aux bonnes pratiques à adopter. Cette sensibilisation passera par exemple, par des plans internes de formation à la sécurité informatique et l'adoption d'une charte informatique adaptée aux outils et autres moyens informatiques mis à la disposition du personnel.

L'absence de déploiement de mesures de sécurité technique ou la négligence dans le

déploiement de mesures adaptées 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€ d'amende - article 226-17 du Code pénal). La violation du secret médical est punie d'un an d'emprisonnement et 15.000€ d'amende.

2. Les obligations de sécurité et de confidentialité des données de santé en cas d'externalisation

L'externalisation est entendue comme la sous-traitance à un prestataire tiers de certains types de traitements sur les données ou l'hébergement des données. Ces prestations restent soumises aux mêmes obligations de sécurité et de confidentialité. L'établissement de santé, considéré comme le responsable du traitement, doit donc s'assurer que son sous-traitant agit en conformité avec les obligations légales.

La sous-traitance - Le professionnel ou l'établissement de santé peut 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. A ce titre, le professionnel de santé doit faire héberger les données de ses patients chez un prestataire agréé par le ministre chargé de la santé, conformément aux articles L.1111-8 et R.1111-9 du Code de la santé publique.

L'obtention de l'agrément est soumise à la mise en œuvre (i) de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données hébergées, et (ii) 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.

3. Le rappel des conditions de la protection des données de santé par la CNIL

Malgré ces obligations fortes, de nombreux professionnels et établissements de santé peinent à se mettre en conformité avec la réglementation. Les professionnels des milieux hospitaliers (médecins, infirmiers, etc.), par exemple, ne sont pas toujours informés ni sensibilisés aux règles particulières devant être respectées en matière de sécurité des données. Des données de santé de patients identifiés sont régulièrement accessibles par des sous-traitants intervenant en milieu hospitalier ou dans des laboratoires d'analyses, ou ont même été rendues accessibles en ligne, par simple négligence.

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.

En l'espèce, suite à un contrôle réalisé au sein du centre hospitalier, la CNIL a constaté qu'un des prestataires avait accédé, avec l'accord de l'établissement, aux dossiers médicaux de plusieurs centaines de patients, en méconnaissance totale des dispositions du Code de la santé publique et de la loi Informatique et Libertés relatives au respect de la vie privée des patients et à la sécurité de leurs données.

Le sous-traitant avait été mandaté par le centre hospitalier pour une mission de codage des actes médicaux et paramédicaux. En effet, lors de la prise en charge d'un patient par un centre hospitalier, les actes pratiqués sont codés selon une nomenclature particulière,

correspondant au code de remboursement par l'assurance maladie.

Le Code de la santé publique prévoit que les établissements doivent procéder à une analyse de leur activité pour détecter d'éventuelles erreurs de codage. Ces analyses sont généralement sous-traitées par les établissements de santé à des sociétés privées.

Or, la loi soumet le traitement de données à caractère personnel à des fins d'évaluation ou d'analyse des activités de soins et de prévention, à l'obtention d'une autorisation. La CNIL veille ainsi, par le biais de contrôles sur place, dans les établissements de santé, à ce que ces traitements ne portent pas sur les données nominatives des malades.

La mise en demeure prononcée par la CNIL a imposé au centre hospitalier de prendre des mesures garantissant la sécurité et la confidentialité des dossiers médicaux des patients pris en charge et de veiller à ce que ces dossiers ne puissent pas être accessibles aux tiers. En outre, l'établissement de santé devait justifier du respect de cette injonction auprès de la CNIL sous 10 jours.

Dans un communiqué du 17 octobre 2013, la CNIL a annoncé que le centre hospitalier s'était mis en conformité suite à la mise en demeure en mettant en oeuvre plusieurs mesures telles que la suppression de l'accès, par le sous-traitant, aux dossiers médicaux des patients, qui demeurent désormais sous la seule autorité du médecin responsable de l'information médicale de l'établissement, et la formalisation d'une politique stricte de sécurité des systèmes d'information. [2].

Compte tenu de cette mise en conformité, la CNIL a décidé de clôturer la procédure à l'encontre du centre hospitalier de Saint-Malo.

Betty SFEZ Avocat au Barreau de Paris Cabinet Sfez Avocats http://www.avocats-sfez.fr

[1] Voir notamment les articles intitulés "Des centaines de résultats d'analyses médicales accessibles sur internet", publié sur www.rue89.com, le 10 janvier 2012 et "Fuite de données concernant une quarantaine de centres hospitaliers français", publié sur http://www.datasecuritybreach.fr/, le 31 octobre 2013.

[2] Délibération CNIL n°2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo, et Communiqué CNIL intitulé "Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo" du 17 octobre 2013

Comentarios:

données de santé à caractère personnel, abdallah, *16 juin 2014*

Bonjour j'aurai souhaité avoir votre avis sur une situation un peu partciulière Selon la loi L.1111-8 du Code de la Santé Publique il est prévu un agrément des hébergeurs de données de santé (via l'ASIP Santé - Agence des Systèmes d'Information Partagés de Données de Santé).
Avez-vous connaissance de cette loi ? Savez-vous si elle s'applique à la recherche ? à la Pharmaco-vigilence ?
merci d'avance
cdmt

archivage papier données de santé, vmc2001, *18 septembre 2014*

Bonjour,

Votre article ne parle pas des conditions pour le stockage physique des données de santé.
Est-il également soumis à agrément ? Y'a-t-il des contraintes particulières prévues ?
Merci de votre aide.
Cordialement

Hebergement des données patients sur interface web, Pierrp, *2 octobre 2014*

Bonjour,

Savez-vous s'il faut absolument héberger les données patient sur un serveur agrée ASIP ?
Si c'est le cas, le serveur doit-il être obligatoirement en France ?
