COURTOIS LEBEL

Communiqué de presse
14 février 2013

Haro sur l'hébergeur de données de santé : un champ d'application large pour un statut rigide

Dans un contexte de développement des technologies de l'information, les risques liés à la sécurité et à la confidentialité des données de santé se sont considérablement accrus.
En effet, les professionnels de santé, les mutuelles et les organismes de sécurité sociale ont été amenés, notamment pour les besoins de la médecine, de la gestion des soins ou l'administration du système de santé, à échanger, à partager, à transférer et même à sous-traiter des informations médicales susceptibles de concerner directement leurs patients. Arnaud Tessalonikos, associé, et Camille Diotel, avocat au sein du département IT du cabinet Courtois Lebel, expliquent pourquoi les hébergeurs doivent se conformer strictement à la réglementation.

L'externalisation est très réglementée

L'externalisation des données de santé auprès d'une personne morale ou physique (l'hébergeur de données de santé), distincte d'un professionnel de la santé exerçant la médecine sur un patient, est placée sous contrôle strict. Dès lors, ces personnes devront être agréées à cette fin.

Selon la CNILi, le but de ces procédures strictes et rigides est d'offrir des garanties fortes de sécurité et de confiance pour les patients comme pour les professionnels de la santé. La CNIL a d'ailleurs récemment prononcé un avertissement à l'encontre d'une société qui, lors de la procédure d'agrément, avait déclaré, à tort, chiffrer les données de santé hébergéesii. Lors d'un contrôle sur place, la CNIL avait pu constater que les données de santé hébergées n'étaient pas chiffrées et qu'elles étaient accessibles aux administrateurs informatiques de la société (et non pas seulement au personnel de santé habilité).

C'est la raison pour laquelle une société prestataire de ce type de services souhaitant percer sur les marchés des établissements de santé ou des médecins (engageant des transferts ou des traitements de données de santé), doit vérifier si elle bénéficie ou non du statut d'hébergeur de données de santé. Les avocats spécialistes IT ont là un rôle important de conseil à jouer.

Les enjeux juridiques, financiers, techniques et assurantiels du statut d'hébergeur de données de santé font de cette profession particulière, un domaine spécifique et rigide qui ne laisse pas la place au hasard.

Qu'est-ce qu'une donnée de santé ?

D'après l'article 8 de la loi du 6 janvier 1978, dite loi « Informatique et Libertés », la collecte ou le traitement de données à caractère personnel « sensibles » sont interdites. Cette interdiction résulte de la nature intime de ces données qui rend leur traitement particulièrement "sensible" et requiert, de ce fait, une protection renforcée.

Les données à caractère personnel dites sensibles recouvrent, selon l'article 8 de la loi « Informatique et Libertés », cinq catégories distinctes parmi lesquelles appartiennent les données de santé.

L'expression relativement extensible de « données de santé » permet de faire bénéficier de "garanties appropriées", comme le recommandait la CNIL dès 1997iii, des informations aussi variées que celles portant sur le groupe sanguin ou les prescriptions médicales. De façon générale, il est entendu que les données de santé englobent toutes informations relatives aux aspects tant physiques que psychiques de la santé d'une personne.

Dans ce contexte, une société peut être relativement facilement amenée à héberger des données de santé. Cette notion étant largement entendue, il convient donc de faire preuve de vigilance quant aux données transférées à l'entreprise (et notamment par un client).

Qu'est-ce que l'hébergement de données de santé ?

La loi française définit l'activité d'hébergement de données de santé à caractère personnel. Ainsi, les professionnels de santé (les médecins, les spécialistes, etc.), les établissements de santé (les hôpitaux) voire les personnes directement concernées (les patients eux-mêmes) peuvent faire héberger (déposer) les données de santé les concernant ou recueillies à l'occasion de leur activité de soin, de prévention ou de diagnostic. L'hébergement de ces données de santé se fera donc chez un tiers et quel que soit le support, papier ou informatiqueiv.

Il est d'ailleurs à noter que, dans une décision du 26 septembre 2012v, la 1ère Chambre Civile de la Cour de Cassation a affirmé avec fermeté que « les articles L. 1111-8 et R. 1112-7 du code de la santé publique » sont des « prescriptions, qui sont d'ordre public » et qui « s'opposent à ce que les données concernant la santé des patients soient conservées selon d'autres modalités ». Aussi, la Cour d'appel qui a considéré que les dispositions « qui visent la protection des malades, poursuivent ainsi un intérêt privé et ne peuvent être considérées comme étant d'ordre public », viole donc les articles L. 1111-8 et R. 1112-7 du code de la Santé Publique, ainsi que l'article 6 du Code civil (« On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs »).

Selon l'Agence des Systèmes d'Information Partagés de Santé (l'ASIP Santé)vi : « Une entité est soumise à l'obligation d'être hébergeur agréé dès lors qu'elle conserve des données de santé de personnes pour lesquelles elle n'intervient pas dans la prise en charge médicale. Un établissement de santé ou un professionnel de santé n'est pas soumis à la procédure d'agrément pour héberger les données de santé des patients pour lesquels il intervient dans des activités de prévention, de diagnostic ou de soins. »

Pour la CNILvii, l'activité d'hébergement des données de santé peut être définie comme « toute activité d'externalisation, de détention et de conservation des données personnelles de santé recueillies ou produites à l'occasion d'un acte de prévention, de diagnostic ou de soins confiées à un tiers qui n'a pas eu pour missions de les collecter ».

Dès lors, il serait possible de dégager trois conditions cumulatives pour bénéficier de la qualification d'hébergeur de données de santé. Il faut :

que les données autour desquelles se déroule l'activité soient considérées comme des données de santé ;

que ces données de santé aient été collectées lors d'un acte de prévention, de diagnostic ou de soins (donc d'un acte médicalviii) ;

que ces données de santé soient déposées à des fins de conservation chez une personne tierce qui ne les a pas collectées.

En conséquence, il apparaît que la qualification d'hébergeur de données de santé est

relativement large et est donc susceptible de s'appliquer dès lors qu'une société conserverait des données de santé à caractère personnel qu'elle aurait reçu d'un établissement de santé ou d'un médecin (voire du patient lui-même).

A titre illustratif, la question de la qualification d'hébergeur de données de santé semblerait donc se poser avec une acuité toute particulière, dès lors que, par exemple, une société conserverait, sur ses serveurs, des données médicales transférées par un établissement de santé.

Quelles sont les obligations de l'hébergeur de données de santé ?

L'agrément

A titre liminaire, il convient de préciser que l'obligation de bénéficier d'un agrément est issue de l'article L.1111-8 alinéa 3 du Code de la Santé Publique (ci-après « CSP »). La procédure d'agrément en elle-même étant définie dans la partie réglementaire du CSP (issue du Décret du 4 janvier 2006).

L'agrément est délivré par le ministre chargé de la Santé, après avis motivé d'un comité d'agrément et de la CNIL, pour une durée de trois ans (tout silence valant décision de rejet dans ce cas).

La procédure d'agrément n'est pas applicable pour tous. En effet, l'ASIP (Agence des systèmes d'informations partagées de santé) Santé rappelle ce pointix. A titre d'exemple, pour l'ASIP santé, dans la mesure où l'établissement héberge lui-même les dossiers hospitaliers, il n'a pas besoin d'obtenir un agrément. En revanche, si l'établissement met son système d'hébergement au service d'autres établissements de santé, il est soumis à la procédure d'agrément (en effet, il deviendrait alors lui-même un hébergeur de données de santé tiers par rapport à l'autre établissement de santé).

La procédure d'agrément de l'hébergeur de données de santé peut se synthétiser en cinq grandes étapes :

La constitution de la demande d'agrément ;

Le dépôt du dossier de demande d'agrément ;

L'avis de la CNIL ;

L'avis du Comité d'Agrément des Hébergeurs (CAH) ;

La décision du ministre en charge de la Santé ;

A ce jour, quarante-cinq agréments ont été délivrés à des hébergeurs de données de santé, par le ministre en charge de la Santéx. La procédure est longue, complexe et ne porte que sur des prestations limitées pour une durée de trois ans (renouvelable dans les mêmes conditions). Aussi, et au moins durant cette procédure, un accompagnement juridique du candidat à l'agrément est vivement conseillé afin de maximiser ses chances d'obtention du convoité sésame.

Le consentement préalable du patient

La loi précise que, hormis quelques exceptions, l'hébergement de données de santé à caractère personnel « [...] ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. [...] » notamment lorsque les contractants d'un service d'hébergement sont des professionnels de santé ou des établissements.

L'obligation de conclure un contrat

L'article L.1111-8 du CSP impose la conclusion d'un contrat entre l'hébergeur de données

de santé et l'établissement de santé ou la personne concernée (« La prestation d'hébergement, quel qu'en soit le support, fait l'objet d'un contrat »).

Toutefois, la loi ne préconise pas de forme contractuelle particulière.

Sur ce point, l'ASIP Santé fournit sur son site internet un seul modèle contractuel afin d'éclairer ce point. Il s'agit d'un exemple de clauses pouvant être insérées au contrat de travail d'un salarié exerçant les fonctions de « médecin de l'hébergeur » auprès des hébergeurs agréésxi.

Le modèle fourni par l'ASIP Santé serait donc transformable et adaptable relativement aisément. De plus, il est à noter que si l'ASIP Santé avait voulu imposer une typologie contractuelle stricte, elle aurait pu facilement le faire en rédigeant un modèle de contrat plutôt qu'un modèle de clauses (insérables dans tous les contrats).

Le secret professionnel et l'obligation de sécurité

D'après l'article L.1111-8 du CSP, les hébergeurs de données de santé à caractère personnel (et donc leur personnel et leurs sous-traitants) sont « astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 223-13 du Code pénal ». Les dispositions légales sur le secret médical sont opposables à l'hébergeur de données de santé (et notamment l'article L.1110-4 du CSP).

Enfin, le dépôt de la demande du candidat à l'agrément est profondément conditionné par les garanties que ce dernier apporte concernant le respect de normes de sécurité. Un formulaire entier de la demande d'agrément est d'ailleurs dédié à la description des mesures et des politiques de sécurité dont dispose le candidat à l'agrément.

La CNIL elle-même, dans son article du 9 janvier 2012 informant de l'avertissement sanctionnant la déclaration mensongère de l'hébergeur de données de santéxii, estime que le procédé de « chiffrage fort » déclaré par le candidat, « constituait l'un des atouts de cette candidature ».

Il est donc essentiel pour le candidat qu'il fonde sa demande d'agrément sur le plus grand nombre de mesures de sécurité qui pourront être prises par lui en tant qu'hébergeur de données de santé (authentification, habilitations, procédures de sauvegarde, traçabilité ou encore chiffrement des canaux et des données elles-mêmes, etc.). Cela représentera donc un investissement financier très important tant en amont de la demande d'agrément que durant toute la durée de son activité d'hébergeur de données de santé. De plus, et dans la mesure où le candidat souhaiterait une assistance juridique dédiée, il serait donc opportun que ce dernier prenne bonne garde à s'entourer d'avocats maîtrisant ces problématiques de sécurité informatique... Il semble donc évident que seules les sociétés disposant des moyens financiers suffisants pourront supporter ces coûts.

Des sanctions sévères pour les hébergeurs non conformes

L'article L. 1115-1 du CSP définit les sanctions encourues par une personne physique ou morale qui exercerait une activité d'hébergement de données de santé sans être agréée à ce titre : trois ans d'emprisonnement et 45 000 euros d'amende.

Le business de l'IT est polymorphe et peut sembler s'adapter à tous les secteurs. Toutefois, il apparaît que bien qu'attractif et potentiellement lucratif, le domaine de la gestion informatisée des données de santé est strictement régi par la loi et la réglementation française. L'essor donné à cette profession nouvelle est donc tout à fait relatif.

De plus, une entreprise du secteur de l'IT peut être rapidement amenée à être contactée ou à contacter des responsables de traitement de données de santé à caractère personnel ;

par exemple une clinique démarchant des prestataires IT afin de lui gérer son système de messagerie électronique interne. Dans ce cas précis, il est tout à fait possible que certains e-mails de la clinique comportent des données de santé. Dans la mesure où la loi et la réglementation française ne dessineraient pas plus précisément les contours de l'hébergement de données de santé, de nombreuses sociétés du secteur IT pourraient potentiellement être considérées comme hébergeurs de données de santé sans pour autant en avoir fait leur cœur de métier…

Courtois Lebel en bref

Cabinet d'avocats d'affaires français fondé en 1969, **Courtois Lebel** offre à une clientèle de dimension internationale une large gamme de prestations juridiques dans les principaux domaines du droit des affaires avec une réelle dimension internationale.

Le Cabinet compte aujourd'hui une trentaine d'avocats dont 10 associés

Nos domaines d'activités

- Assurance
- Banque et Bourse
- Conformité / Regulatory
- Concurrence
- Contentieux
- Corporate / M&A
- Distribution
- Données personnelles
- Financement immobilier
- Fiscalité
- Immobilier
- Informatique & réseaux
- Internet
- Management package
- Marketing direct / Consommation
- Outsourcing
- Propriété Intellectuelle
- Restructuring
- Social

Courtois Lebel est membre de deux réseaux de cabinets d'avocats : AEL, réseau européen, et ALFA, réseau international d'envergure.

Contacts presse :

Corinne Coman
Responsable Marketing & Communication
Courtois Lebel
15 rue Beaujon - 75008 Paris
Tél : 01 58 44 92 92
ccoman@courtois-lebel.com

Nicole Coiffard et Florence Laurent-Bellue
Agence de presse Cordiane
Tél : 01 39 62 33 42
ncoiffard@cordiane.com flaurentbellue@cordiane.com

[i] Guide CNIL 2011 « Professionnels de Santé ».

[ii] http://www.cnil.fr/la-cnil/actualite/article/article/la-cnil-sanctionne-une-declaration-mensongere-dun-hebergeur-de-donnees-de-sante/#

[iii] Voir la Délibération CNIL n° 97-008, du 4 février 1997

[iv] Article L 1111-8 alinéa 1du Code de la Santé Publique, tel que modifié par la Loi n°2009-879 du 21 juillet 2009.

[v] Cour de Cassation, 1ère Chambre Civile, 26 septembre 2012, Pourvoi n° 11-17.962 - Arrêt n°1036 (Rejet)

[vi] http://esante.gouv.fr/sites/default/files/PAHDS_Presentation_generale_v1.0.1.pdf

[vii] Guide CNIL 2011 « Professionnels de Santé ».

[viii] A la lecture de l'article L 4161-1 du CSP (sanctionnant l'exercice illégal de la médecine), « l'acte médical » se définit comme l'acte qui recouvre à titre principal l'établissement d'un diagnostic ou le traitement d'une maladie. Le diagnostic se définit comme « l'acte par lequel médecin, groupant les symptômes qu'offre son patient, les rattache à une maladie » (Dictionnaire abrégé des termes de médecine, Delamare, 3e éd., éd. Maloine). La jurisprudence entend largement la notion de diagnostic. Le traitement se définit comme « l'ensemble des prescriptions employées pour combattre une maladie » (Dictionnaire abrégé des termes de médecine, Delamare, 3e éd., éd. Maloine). Il résulte de la jurisprudence qu'un grand nombre de traitements entrent dans la catégorie des traitements soumis à l'article L. 4161-1 du Code de la santé publique. Le Code de la Santé Publique subordonne ensuite la légalité de l'acte médical par le fait qu'il soit réalisé par un médecin (voir article L.4111-1 et suivant du CSP), ou d'autres sous réserve de conditions stricte (par exemple, un étudiant en médecine).

[ix] http://esante.gouv.fr/services/referentiels/securite/hebergement-faq

[x] Pour voir la liste de ces établissements : http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

[xi] http://esante.gouv.fr/sites/default/files/Modele_contrat_hebergeur_V0.1.pdf

[xii] Cf. note n°2