La Kanzlei

Obligations des prestataires de santé en matière de collecte et d'hébergement de données de santé

Conditions générales
Marques / PI

Gordian Deger

Les données relatives à la santé sont des données sensibles. Leur collecte et leur traitement sont par conséquent très encadrés. Cette lettre d'information propose une présentation synthétique des obligations imposées aux prestataires de santé (médecins, hôpitaux, etc.) en cas de collecte (1) et d'hébergement externe de ce type de données (2).

Dans le cadre de l'exercice de leur activité de prévention, de diagnostic ou de soin, les professionnels et établissements de santé sont amenés à recueillir des données à caractère personnel relatives à la santé de leurs patients. La loi dite « *informatique et libertés* » autorise les traitements de données de santé « *nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé* » sous réserve qu'ils soient effectués dans l'intérêt du patient et mis en œuvre par un membre d'une profession de santé. La constitution de dossiers médicaux, fichiers patients etc. par un prestataire de santé sont donc en principe admis par la loi.

Cependant, avant de procéder au traitement de ces données, les prestataires de santé doivent effectuer certaines démarches. D'une part, ils doivent obtenir l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL) pour ces traitements de données. D'autre part, ils doivent informer chaque patient concerné sur ses droits.

Une fois les données collectées, se posera la question de leur stockage. Les prestataires de santé qui souhaitent faire héberger les données de santé de leurs patients sur les serveurs d'un hébergeur externe devront s'assurer que l'hébergeur choisi a été agrée par le ministre chargé de la santé et recueillir le consentement de chaque patient pour ce stockage externe de ses données de santé.

1. **Obligations en cas de traitement ou de collecte de données de santé à caractère personnel**

En application de l'article 22 de la loi dite « informatique et libertés », le prestataire de santé doit obtenir l'autorisation de la CNIL avant de procéder à tout traitement de données à caractère personnel. Par traitement de données à caractère personnel, on entend « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion de données à caractère personnel ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». Ainsi, le fait de collecter des informations personnelles des patients (informations concernant l'état civil, le domicile, les antécédents médicaux, etc.) constitue un traitement pour lequel le prestataire de santé devra avoir obtenu préalablement l'autorisation de la CNIL selon la procédure dite de déclaration normale. Il faut savoir en effet que le fait de procéder à la collecte et au traitement de données sans l'autorisation de la CNIL est passible de sanctions pouvant aller jusqu'à cinq ans d'emprisonnement et 300.000 Euros d'amende.

En outre, le prestataire de santé est tenu d'informer ses patients des objectifs poursuivis par la collecte et le traitement de ses données, du caractère obligatoire ou facultatif de ses réponses et des modalités d'exercice de son droit d'accès, de rectification et d'opposition. En pratique, cette information peut être assurée par voie d'affichage dans les locaux du prestataire, sur son site internet etc. Dans tous les cas, s'il est remis un questionnaire au patient, celui-ci devra comporter les mentions légales précitées. Selon l'article 7 de la loi « informatique et libertés », le prestataire de santé doit enfin recueillir l'accord préalable du patient à la collecte et au traitement de données le concernant. La collecte et le traitement de données de santé en l'absence de consentement exprès du patient sont en effet sanctionnés par l'article 226-19 du code pénal

2. **Obligations en cas d'hébergement de données de santé à caractère personnel**

Le stockage en interne des données à caractère de santé, c'est-à-dire sur un ordinateur ou serveur placé dans l'établissement du professionnel de santé n'appelle pas de remarques particulières si ce n'est que l'accès à ces données doit être suffisamment sécurisé. Il en va différemment si les données de santé sont stockées chez un prestataire externe. Le professionnel ou l'établissement de santé peut avoir intérêt, pour diverses raisons, à recourir aux services d'un hébergeur externe.

Ceci permet notamment de stocker un volume important des données et de disposer en même temps d'une sauvegarde externe de celles-ci. Depuis quelques années, un grand nombre de services de stockage en ligne du type « cloud computing » est apparu. Par ailleurs, il existe des logiciels de gestion destinés aux prestataires de santé qui fonctionnent en mode hébergé, ce qui signifie que le logiciel lui-même et l'ensemble des données traitées sont stockés sur les serveurs informatiques d'un prestataire externe (solutions dites « SaaS » ou « ASP »).

a. **Confier les données de santé à un hébergeur agrée**

Si l'hébergement externe de donnés de santé présente des avantages techniques et économiques incontestables, il comporte aussi des risques considérables pour la confidentialité et l'intégrité de ces données. De ce fait, le praticien doit se montrer vigilant dans le choix de l'hébergeur à qui il confiera les données de santé de ses patients.

Afin d'assurer que les données de santé soient hébergées dans de bonnes conditions, l'article L.1111-8 du Code de la santé publique dispose que tout hébergeur de données de santé à caractère personnel doit avoir obtenu l'agrément du ministre de la santé. Cet agrément est délivré après avis de la CNIL et du Comité d'agrément des hébergeurs (CAH) et atteste d'un haut niveau de sécurité, notamment :

- l'authentification du professionnel de santé lors de la connexion au moyen d'une carte de professionnel de santé (dite CPS) ou un dispositif équivalent ;
- l'établissement d'un protocole journalier des accès et des actions effectuées par les intervenants connectés ;
- le chiffrement des données et des canaux au moyen d'un algorithme fort ;
- la sécurisation des moyens de télécommunication ;
- la sauvegarde et l'archivage des données de manière à assurer leur pérennité.

L'agrément est également nécessaire lorsque le professionnel ou l'établissement de santé utilise un logiciel de gestion fonctionnant en mode hébergé. Concernant ces logiciels fonctionnant en mode hébergé, on peut distinguer deux cas :

- Si l'éditeur du logiciel héberge lui-même les données de santé de ses clients, il doit disposer de l'agrément du ministre de la santé.
- Si l'éditeur du logiciel sous-traite la prestation d'hébergement des données à un prestataire tiers, ce tiers devra être agrée.

Il est à noter que l'article L.1115-1 du Code de la santé publique punit le fait de proposer une prestation d'hébergement de données de santé sans être titulaire de l'agrément prévu par la loi par trois ans d'emprisonnement et 225.000 Euros d'amende, s'il s'agit d'une personne morale.

De son côté, le professionnel de santé qui confie les données de santé à caractère personnel de ses patients à un hébergeur non agréé engage sa responsabilité civile à l'égard de l'intéressé, notamment dans le cas où ses données viendraient à être volées, diffusées, perdues ou consultées par des tiers non autorisés, et sera donc tenu de réparer le préjudice ainsi causé. De plus, il engagera sa responsabilité pénale fondée sur l'article 226-22 du Code pénal, qui prévoit une peine de trois ans d'emprisonnement et de 100.000 Euros d'amende pour celui qui, par imprudence ou négligence, porte à la connaissance d'un tiers n'ayant pas qualité pour recevoir ces informations des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée.

Par conséquent, le prestataire de santé doit s'assurer que l'hébergeur choisi figure sur la liste des hébergeurs agrées publiée par l'ASIP Santé5 . Il en découle en outre que les distributeurs commercialisant des logiciels professionnels auprès des prestataires de santé ont le devoir d'informer leurs clients sur les exigences réglementaires en matière d'hébergement de données de santé et de les conseiller en conséquence. La vente d'une solution logicielle qui ne garantirait pas le stockage des données de santé dans des conditions conformes pourra être considérée comme fautive et engager la responsabilité du distributeur.

b. **Recueil du consentement du patient**

Concernant l'hébergement de données de santé à caractère personnel, la loi précise par ailleurs qu'il ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. Le professionnel de santé doit donc recueillir le consentement de ses patients concernant le fait que leurs données feront l'objet d'un hébergement externe. Il existe une dérogation à cette obligation : dès lors que l'accès aux données hébergées est limité au seul professionnel de santé ou établissement qui les a déposées, le consentement exprès du patient n'est pas exigé. Le patient dispose toutefois d'un droit d'opposition et de rectification conformément aux dispositions de la loi dite « informatique et libertés ».

Cette obligation ne doit pas être prise à la légère car la collecte et le traitement de données de santé en l'absence de consentement exprès du patient sont sanctionnés pénalement (cf. supra, note n° 4).

- - -

Pour aller plus loin :

- *Site Internet de* la CNIL
- *Site Internet de* l'ASIP Santé

PDF Download

29.01.2014

Qivive
Rechtsanwalts GmbH

qivive.com

Köln[D]
Konrad-Adenauer-Ufer 71
D – 50668 Köln
T + 49 (0) 221 139 96 96 - 0 F + 49 (0) 221 139 96 96 - 69
koeln@qivive.com

Paris[F]
50 avenue Marceau
F – 75008 Paris
T + 33 (0) 1 81 51 65 58 F + 33 (0) 1 81 51 65 59
paris@qivive.com

Lyon[F]
10 –12 boulevard Vivier Merle
F – 69003 Lyon
T + 33 (0) 4 27 46 51 50 F + 33 (0) 4 27 46 51 51
lyon@qivive.com