les ateliers e-santé

PROTECTION DES DONNEES PERSONNELLES DE SANTE

TEXTES FONDATEURS & NOTIONS-CLÉS

Les données personnelles de santé sont des données sensibles. Elles bénéficient dans les textes d'une protection particulière (code de la santé publique, code de la sécurité sociale et code pénal).

RAPPELS :

- **La donnée à caractère personnel :** toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement.
- **Le traitement de données à caractère personnel :** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé.

I. LE DROIT COMMUN DE LA PROTECTION DES DONNÉES PERSONNELLES DE SANTE

A. Il est posé par la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et par la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

La protection des données s'appuie sur cinq principes clés que doivent respecter les responsables de traitement :

- une finalité déterminée et légitime
- des données pertinentes et mises à jour
- une durée de conservation limitée
- une information préalable et précise
- des mesures de sécurité adaptées

B. La Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante, est chargée de faire respecter ces principes.

Elle définit, à l'occasion de l'examen de projets qui lui sont soumis, les conditions d'une mise en œuvre respectueuse des dispositions de la loi du 6 janvier 1978, en particulier au regard des droits de la personne (droit d'accès, droit de rectification, droit de suppression et droit d'opposition) et des mesures de sécurité permettant de garantir la protection de la personne et de ses données. L'adoption de mesures de sécurité physique et logique restent déterminées en fonction de l'architecture technique utilisée et de la nature des données collectées.

PRÉSERVER LES DROITS DES PATIENTS : LE RÔLE DE LA CNIL ET DU CISS

Institution indépendante, la CNIL veille au respect de l'identité humaine, de la vie privée et des libertés. La mondialisation des échanges de données et les innovations technologiques incessantes constituent pour la CNIL autant de défis majeurs : l'institution doit s'assurer que ces modernisations sont compatibles avec une protection efficace de la vie privée. Parallèlement, le Collectif interassociatif sur la santé (CISS) regroupe plus de 30 associations : l'organisme représente et défend les intérêts communs à tous les usagers du système de santé. Le CISS se mobilise pour une prise en charge optimale des patients, et l'amélioration de leur accueil quelle que soit la structure.

II. DES DISPOSITIONS PARTICULIERES QUI RENFORCENT CETTE PROTECTION

A. La sanctuarisation des données personnelles de santé

Le code pénal sanctionne l'accès non autorisé à des données personnelles de santé en dehors de toute relation de soins.

Article 226-13 : *« La révélation d'une information à caractère secret par une personne qui en est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15.000 euros d'amende. »*

asip santé
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

«Comment garantir aujourd'hui en France la protection des données de santé ?»
Mardi 22 juin 2010

→ La violation du secret professionnel est sanctionnée. Seule une loi peut déroger et autoriser un professionnel de santé à accéder à des données de santé à caractère personnel en dehors de la relation de soins qui peut l'unir à son patient.

Les données de santé ne peuvent être communiquées et utilisées dans les conditions déterminées par la loi, que dans l'intérêt direct du patient (assurer son suivi médical, faciliter sa prise en charge par l'assurance maladie obligatoire…) ou pour les besoins de la santé publique.

Quelques exemples :

- **L'équipe soignante** (loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé)
- **La sécurité sociale** (article L. 161-29 du code de la sécurité sociale)
- **La recherche médicale** (loi du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé, chapitre IX de la loi informatique et libertés)
- **L'évaluation ou l'analyse des pratiques ou des activités de soins et de prévention** (loi du 27 juillet 1999, chapitre X de la loi informatique et libertés)

B. La confidentialité des données de santé

1. Le principe est posé par l'article L.1110-4 du code de la santé publique.

Article L.1110-4 : *« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant. »*

Il offre aux personnes une protection juridique, en lien avec le secret professionnel, et en définit les conditions. Les outils de la protection juridique qui assurent cette confidentialité sont l'information préalable, le recueil du consentement et le droit d'opposition du patient.

2. Les conditions d'application sont précisées par le décret « Confidentialité » du 15 mai 2007

Il détermine les exigences de confidentialité et de sécurité à respecter par les professionnels de santé, les établissements de santé, les réseaux de santé, et tout organisme participant au système de santé, qui conservent sur support informatique et échangent par voie électronique des données de santé à caractère personnel. Ces exigences s'appliqueront dans tous les cas et notamment au Dossier Médical Personnel.

Il détermine les cas où l'utilisation de la CPS ou d'un dispositif équivalent agréé par l'ASIP Santé est obligatoire.

Il rend obligatoire le respect de référentiels définis par arrêté du ministre chargé de la Santé, qui décriront les règles de sécurité et de confidentialité destinées à garantir en toutes circonstances le secret médical.

3. La loi de juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires positionne l'ASIP Santé comme l'autorité compétente de référence pour définir et imposer des systèmes conformes aux référentiels de santé et d'interopérabilité.

Article L.1111-8 alinéa 4 du code de la santé publique : *« …la détention et le traitement sur des supports informatiques de données de santé à caractère personnel par des professionnels de santé, des établissements de santé ou des hébergeurs de données de santé à caractère personnel sont subordonnés à l'utilisation de systèmes conformes […] aux référentiels d'interopérabilité et de sécurité arrêtés par le ministre chargé de la Santé après avis [de l'ASIP Santé]. »*

C. L'hébergement des données de santé à caractère personnel

1. La loi du 4 mai 2002 relative aux droits des malades et à la qualité du système de santé a instauré une procédure d'agrément des hébergeurs de données de santé à caractère personnel, qui vise à garantir la sécurité des données personnelles de santé lorsqu'elles sont hébergées par un organisme distinct du professionnel ou de l'établissement de santé qui soigne le malade.

Article L.1111-8 du code de la santé publique : *« Les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée.*

Les traitements de données de santé à caractère personnel que nécessite l'hébergement prévu au premier alinéa, quel qu'en soit le support, papier ou informatique, doivent être réalisés dans le respect des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La prestation d'hébergement, quel qu'en soit le support, fait l'objet d'un contrat. Lorsque cet hébergement est à l'initiative d'un professionnel de santé ou d'un établissement de santé, le contrat prévoit que l'hébergement des données, les modalités d'accès à celles-ci et leurs modalités de transmission sont subordonnées à l'accord de la personne concernée. […] ».

2. Le décret du 4 janvier 2006 précise les conditions de cet agrément qui fait intervenir la CNIL et un comité d'agrément des hébergeurs placé auprès du ministère chargé de la Santé. L'ASIP Santé a pour mission l'instruction des dossiers de demande d'agrément ainsi que le secrétariat du comité d'agrément.