Claire Debost
Doctorante CIFRE

Les données de santé

La sécurité des consultations et partages de l'information médicale numérisée

Essor des TIC dans le secteur de la santé : quelles opportunités ?

« *Les technologies de l'information et de la communication font désormais partie intégrante de l'environnement professionnel des médecins. Elles offrent des possibilités d'exploitation des données et des connaissances difficilement imaginables il y a 15 ans à peine. En favorisant l'**échange** et le **partage de documents médicaux,** elles jouent un rôle important dans la **coordination des soins**. Elles contribuent, de façon générale, à **l'amélioration de la qualité des soins** en facilitant l'accès, sans perte de temps, aux données nécessaires à la prise de décision et à la continuité de la prise en charge. L'informatisation de la pratique médicale apporte, enfin, les moyens de dégager du temps pour l'écoute et les soins aux*

Quelles conséquences ?

- Aujourd'hui, une prise en charge induit une multiplication de collectes d'informations personnelles

= succession de traitements de données concernant la personne

- Ex : la constitution et la gestion de dossiers médicaux, la transmission d'information médicale, la gestion des rendez-vous, etc…

Quels risques ?

- « *D'abord, parce que le risque de piratage à distance des banques de données, s'il est techniquement difficile, peut affecter, par une seule intrusion, des milliers de dossiers médicaux. De plus, les points d'accès aux systèmes informatiques seront nécessairement disséminés. L'objectif n'est-il pas, dans le cadre du DMP, de permettre à chaque professionnel de santé consulté par un malade d'avoir accès à l'ensemble des données le concernant ?* ***A l'improbable cambrioleur dérobant la fiche cartonnée du médecin de famille pourrait succéder le hacker constituant des fichiers médicaux sur des groupes sociaux, des clientèles commerciales ou des salariés d'entreprises****. L'établissement d'une carte électronique individuelle interrégimes, dite Sésame vitale 2, comportant des informations médicales offrira, même si l'impact ne pourrait être qu'individuel, une autre possibilité de détournement d'informations personnelles*. » (D. Tabuteau)

- « *L'informatisation croissante des données médicales de santé s'inscrit dans un* ***contexte culturel de méfiance****. Le fait que l'avantage d'une plus grande facilité de communication interpersonnelle est contrebalancé par une plus grande insécurité est un sentiment très répandu*. » (CCNE, 2008)

Un risque d'atteinte à la vie privée de la personne

- La Cour européenne des droits de l'homme

  « *la notion de vie privée est large et englobe notamment des aspects de l'identité physique et sociale d'un individu comme le droit à l'autonomie personnelle, le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur* » (Aff. Pretty c/ R.U 2002)

- Le Sénat

  « *le droit au respect de la vie privée est le droit pour une personne d'être libre de mener sa propre existence avec le minimum d'ingérences extérieures, ce droit comportant la protection contre […] tout ce qui relève du comportement intime*. » (R. La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information, 2009)

Quelles sont les composantes de la vie privée du salarié ?

- Ses mœurs et convictions religieuses, son orientation sexuelle, ses relations familiales, amicales, les documents nommés comme étant personnels sur son ordinateur, …

- Et les informations concernant sa santé

La vie privée de la personne est protégée par le droit

- Art. 9 Code civil : « *Chacun a droit au respect de sa vie privée ».*

- Art. 1er Loi Informatique et Libertés : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*. »

Quelle protection pour le salarié ?

- La connaissance de l'état de santé d'une personne constitue une information qui relève de l'intimité de sa vie privée (= information à caractère secret) et qui est protégée par le secret professionnel (art. 226-13 code pénal)

- Art. L. 1110-4 CSP : « ***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****.* »

Existe-t-il un droit adapté aux TIC Santé pour protéger les informations concernant la santé des personnes ?

Le code de la santé publique (lois et décrets) ?

La Loi Informatique et Libertés ?

L’accès à une donnée de santé

Qu'est-ce qu'une donnée de santé ?

- **Dans la loi Informatique et Libertés**

  La réforme intervenue en 2004 de la loi du 6 janvier 1978 encadre strictement les traitements concernant les données de santé sans définir la notion de donnée de santé.

  Un seul élément : la donnée relative à l'état de santé = « catégorie particulière de données » (Art. 8)

  (donnée sensible).

- **Dans le code de la santé publique ?**

Art. L.1111-7 : « *informations concernant sa santé* »

« ***informations détenues, à quelque titre que ce soit, par des professionnels*** *et établissements* ***de santé****, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment résultats d'examen, compte rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers* ».

- Art. L. 1111-8 :

  « *données de santé à caractère personnel, recueillies ou* ***produites à l'occasion des activités de prévention****, de diagnostic ou de soin* ».

« ***Les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée ;***

les informations relatives à l'enregistrement du patient pour la prestation de services de santé*; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales; toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient; ou* ***toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical,*** *un traitement clinique ou l'état physiologique ou biomédical de la personne concernée,* ***indépendamment de sa source****, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve*

- Une donnée de santé c'est « ***toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne*** »

  Art. 4, Proposition de Règlement du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final, le 25.1.2012

Données de santé au travail ?

- Antécédents médicaux
- Résultats des examens médicaux complémentaires pratiqués
- Les risques professionnels ?

Toutes les données de santé n'ont pas systématiquement de lien avec l'état de santé…
Mais ces données sur les conditions de travail peuvent y être assimilées dans la mesure où elles peuvent être combinées avec les données médicales pour circonstancier les résultats …

Où est stockée la donnée de santé ?

- « ***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****.*
- *Les professionnels et établissements de santé peuvent, par dérogation […], utiliser* ***leurs propres systèmes*** »

(Art. L. 1111-8 CSP)

- *« La détention et le traitement sur des supports informatiques de données de santé à caractère personnel par des professionnels de santé, […] des hébergeurs de données de santé à caractère personnel sont subordonnés à l'utilisation de systèmes d'information conformes aux prescriptions adoptées en application de l'article L. 1110-4* (= respect vie privée et secret des informations) *et aux référentiels d'interopérabilité et de sécurité arrêtés par le ministre chargé de la santé après avis* [de l'ASIP Santé]. »

(Art. L.1111-8 CSP)

2 SOLUTIONS 1 INVARIANT

- Hébergement auprès d'un hébergeur agréé ou sur un serveur interne
- Obligation d'assurer la sécurité et la confidentialité des données stockées

Pr rappel : Art. D. 4626-33 CT : « *Toutes dispositions sont prises pour assurer le secret médical et l'inviolabilité du fichier tenu par le médecin.* »

Et la HAS rappelle que les données :

« *doivent être cryptées selon des algorithmes dûment expertisés et l'accès rendu possible uniquement par un système de clés de chiffrement. Les données administratives et médicales doivent être cryptées selon un algorithme différent* » (HAS 2009 DMST p. 13)

Pourquoi un agrément ministériel pour l'hébergement des DS ?

A partir du dossier de demande d'agrément, une étude attentive par la CNIL et l'ASIP santé, en vue d'assurer :

- La sécurité des données sensibles dont l'hébergement est externalisé
- Le respect de la disponibilité, intégrité, confidentialité, auditabilité des données de santé

A quelles conditions ?

- « L'hébergeur de données doit respecter la réglementation spécifique (art. R. 1111-9 CSP) » (HAS DMST p. 14)

= Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel sur support informatique et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :

compétences des acteurs,

confidentialité sécurité des données,

information sur l'activité, etc.

- Et l'impératif recueil du consentement du patient (L. 1111-8 CSP)

- Ex : un société a été agréée pour une prestation d'hébergement d'applications en mode Saas, fournies et maintenues par le client et gérant des données de santé à caractère personnel produites par des services de santé au travail.

  (http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agree)

Qui peut accéder à une donnée de santé ?

- L'article L. 1111-8 limite l'accès aux données hébergées :
  - ✓ Au patient
  - ✓ Aux professionnels de santé ou établissements de santé qui les prennent en charge et qui sont désignés par le patient

Or l'article L4624-2 du code du travail prévoit que le DMST puisse être consulté par :

- le salarié,
- le médecin du travail (personnels infirmiers du travail, collaborateurs du médecin du travail sous la responsabilité du médecin du travail et avec l'accord du médecin du travail, dans le respect du secret professionnel et dans la limite de ce qui est nécessaire à l'exercice de leur mission)
- le médecin inspecteur régional du travail
- un autre médecin du travail dans la continuité de la prise en charge sauf refus du salarié dument informé
- les ayant-droits du salarié en cas de décès conformément aux dispositions des articles L. 1110-4 et L 1111-7 CSP

- Des divergences …

- Un invariant … les non professionnels de santé ne peuvent pas accéder au dossier médical (ex : les psychologues, l'assistant social, etc).

Comment accéder à une donnée de santé ?

- Avec une carte de professionnel de santé

- Art. L. 1110-4 CSP :

« Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale ou un dispositif équivalent agréé par l'organisme chargé d'émettre la carte de professionnel de santé est obligatoire. La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins. »

- Le décret nº 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique complète cette disposition législative.

- Art. R. 1110-3. − *En cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire.*

La CPS

- Elle permet à un professionnel de santé d'accéder à un système d'information de santé dans le respect des droits de sa fonction.
- La CPS permet la signature électronique. La CPS garantit donc, l'identité et la qualité du titulaire de la carte, mais également, l'intégrité du document signé.

→Son apport est majeur dans la circulation de l'information médicale et le respect des principes de sécurité inhérents à cette nouvelle pratique.

Explication simplifiée des mécanismes de sécurité

Authentification

1) La personne se connecte à un serveur en utilisant le système CPS

3) Si le certificat est valide le serveur donne l'autorisation d'accès

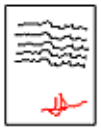
2) Le serveur vérifie la validité du certificat

Liste de référence des certificats valides

Signature électronique

1) L'expéditeur signe son message en utilisant le système CPS

2) Il envoie le message signé



3) Le destinataire vérifie la validité du certificat (optionnel)

4) Le destinataire lit le message

Chiffrement

1) L'expéditeur chiffre son message

2) Il envoie le message chiffré

3) Le destinataire déchiffre le message avec le système CPS

Le partage d’une donnée de santé

Le secret … Ce n'est plus un secret médical

Ni subjectivement :

- s'impose aux professionnels de santé, tout membre du personnel des établissements ou organismes, toute autre personne en relation « de par ses activités » avec ces établissements ou organismes.
- s'impose à tout professionnel de santé ainsi qu'à tout professionnel intervenant dans le système de santé. (Art. L1110-4 CSP)

→ **Sont donc impliqués professionnels et non-professionnels de santé**.

Ni objectivement :

- Secret couvre l'ensemble des informations concernant la personne venues à la connaissance des débiteurs de secret. (Art. 4 CDM)

→ **Sont donc protégées toutes les informations, et pas seulement les informations médicales**

Mais un secret professionnel

Article 226-13 code pénal :

> « *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 15000 euros d'amende.* »

Partage de secret ? D'informations ?

Art. L1110-4 CSP : « *secret partagé* » deux réalités :

- Deux ou plusieurs professionnels de santé peuvent toutefois, **sauf opposition de la personne** dûment avertie, échanger des informations relatives à une même personne prise en charge, **afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible**.

- Lorsque la personne est prise en charge par **une équipe de soins dans un établissement de santé**, les informations la concernant sont **réputées confiées par le malade à l'ensemble de l'équipe.**

Avec qui le médecin du travail peut-il échanger des informations concernant la santé du salarié ?

- **Avec les membres de l'équipe pluridisciplinaire** ? Avec les seuls PS participant au suivi du salarié (le médecin collaborateur, l'infirmier, l'interne médecin)

  Dans le respect du consentement du patient.
- **Avec le médecin traitant ?**

  Article R. 4412-56 CT

  Dans le respect du consentement du patient (car hors cadre de l'équipe de soins qui ne connait une existence légale que dans le cadre de l'hospitalisation, les maisons et centres de santé. (Art. L1110-4 CSP).
- **Assurément pas avec l'employeur**

Comment ?

Obligation d’assurer la sécurité et la confidentialité des données de santé :

- Par **la CPS**
- Par **la messagerie sécurisée** :

Ces messageries doivent permettre à tous les professionnels de santé d'échanger entre eux par email, rapidement et en toute sécurité, des données personnelles de santé de leurs patients dans le respect de la réglementation en vigueur.

https://www.mssante.fr/

Quelles sanctions ?

- **La sanction prévue sur le fondement de l'article L. 1110-4 CSP al 5**

- *« le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article [article L 1110-4 alinéa 1 du Code de la santé publique] est puni d'un an d'emprisonnement et de 15 000 euros d'amende ».*

- **Les sanctions prévues par le Code pénal**

- Art. 226-13 C. pénal : violation secret professionnel

Limite : la révélation d'une information à caractère secret peut ne pas engager la responsabilité pénale de son auteur (Art. 226-14)

Autorisation de divulgation d'une information à caractère secret pour :

1° celui qui informe les autorités […] de privations ou de sévices, […], dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique ;

2° le médecin qui, avec l'accord de la victime, porte à la connaissance du procureur de la République les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. […]

3°les professionnels de la santé ou de l'action sociale qui informent le préfet et, à Paris, le préfet de police du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une.

Le signalement aux autorités compétentes effectué dans les conditions prévues au présent article ne peut faire l'objet d'aucune sanction disciplinaire.

- Obligation de divulgation d'une information à caractère secret :
  - pour les maladies contagieuses, qui doivent faire l'objet d'une déclaration à l'autorité sanitaire par les médecins et les responsables des services et laboratoires d'analyses de biologie médicale publics et privés,
  - déclarations de naissance aux services de l'Etat civil,
  - déclaration aux fins de sauvegarde de justice des patients hospitalisés pour troubles mentaux ....

→ Le médecin du travail ne peut donner aucune information à l'employeur ni sur l'état de santé d'un salarié, ni même sur le fait qu'un salarié l'a sollicité. Il ne peut donner aucune information qui permettrait à l'employeur d'identifier le salarié venu signaler une situation préoccupante pour la santé

Les sanctions pénales des atteintes aux droits de la personne résultant des traitements de données à caractère personnel (art. 226-16 et s. Code pénal)

- Ne pas mettre en œuvre les mesures de sécurité prescrites par l'article 34 de la loi I&L,
- Collecter de manière frauduleuse, déloyale ou illicite les données,
- Procéder au traitement des données malgré l'opposition de la personne concerner, hors les cas prévus par la loi,
- Recueillir, à l'occasion de leur enregistrement, de leur classement, de leur transmission, ou d'une autre forme de traitement, des DCP dont la divulgation aurait pour effet de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas la qualité pour les recevoir,
- Mettre ou de conserver en mémoire informatisé, hors les cas prévus par la loi, et sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, sont relatives à la santé

est puni de 5 ans d'emprisonnement et de 300 000 € d'amende.

Focus sur le DMP

- Son hébergeur est la société agréée Santéos.
- Le patient est le seul avoir accès garanti à son dossier complet
- L'accès des PS au DMP de leur patient est subordonné à l'autorisation du titulaire. Cet accès est sécurisé par l'utilisation conjointe de la CPS et de la carte vitale présentée par le patient.
- N'ont pas accès au DMP les médecins du travail, les médecins des assurances privées, les mutuelles, les services de police, l'employeur.