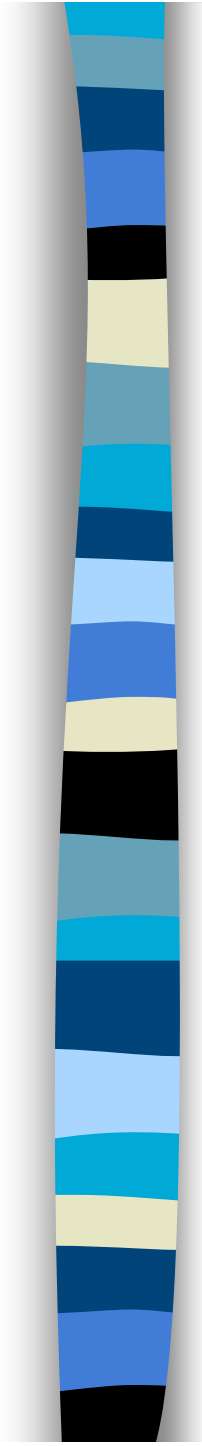


# Les garanties de protection des données personnelles dans le Dossier Médical Personnel



Réunion PRIAM - 2008

Caroline Zorn  
Doctorante en Droit médical  
Université Nancy 2  
(CRDP-Iscrimed)

- 
- I. Les garanties juridiques de protection des données du DMP
    1. Garanties en matière de collecte des données : un consentement “explicite”.
    2. Garantie en matière de conservation des données : du droit de rectification des données au droit à l'oubli.
  
  - II. Des garanties techniques pour une protection effective des données du DMP
    1. La question du recueil du consentement
    2. La question de l'authentification de celui qui consent

Principaux textes applicables au DMP

Pour aller plus loin...

# Qu'est-ce que le DMP?

Le Dossier Médical **Personnel** est

- ✓ un dossier médical électronique
- ✓ ouvert par son titulaire (bénéficiaire d'assurance maladie)
- ✓ accessible en ligne par son titulaire et par les professionnels de santé autorisés (via leurs logiciels)

Le DMP représente donc un traitement automatisé sur une concentration de données personnelles très sensibles...



# Les principes de traitement des données sensibles au niveau communautaire

- **Convention n°108** du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg 1981.
- **Directive 95/46/CE** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.  
**Pour éclairer les dispositions de la directive :**  
Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) produit par le **groupe de travail de l'article 29** sur la protection des données.
- **Convention dite « sur les Droits de l'Homme et la biomédecine », Oviedo 1997.**  
Chapitre III « Vie privée et droit à l'information »,  
Art. 10 : (1) Toute personne a droit au respect de sa vie privée s'agissant des informations relatives à sa santé.
- **Traité sur le fonctionnement de l'Union européenne, Lisbonne 2007**  
Article 16B : (1) Toute personne a droit à la protection des données à caractère personnel la concernant.



# Les principes de traitement des données sensibles au niveau communautaire

- **Directive 95/46/CE** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données:
- **Article 8.1** : Les Etats membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la **santé** et à la vie sexuelle.
- **MAIS... Article 8.4** : Sous réserve de **garanties appropriées**, les Etats membres peuvent prévoir, pour un motif **d'intérêt public important**, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.



# Les principes de traitement des données sensibles en droit interne

- **Loi n° 2004-800 du 6 août 2004** modifiant la loi dite “informatique et libertés” de 1978, transposition de la **Directive 95/46/CE “protection des données”** en droit interne :
  - art. 8 : I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la **santé** ou à la vie sexuelle de celles-ci.
  - II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, **ne sont pas soumis à l'interdiction** prévue au I :
    - 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ; [...]
  - IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, **justifiés par l'intérêt public** et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.



# Application de ces principes au DMP

- Quel est le motif d'intérêt public ? Le DMP a un **double objectif** (validé par le C. Constit, DC 2004-504)
  - Favoriser la coordination, la qualité et la continuité des soins  
= il ne contient que les éléments dont le partage est nécessaire  
= il n'est ni un dossier professionnel, ni un dossier de réseau!
  - Contribuer à la réduction du déséquilibre des comptes de la sécurité sociale (aspect économique aujourd'hui au second plan)
- Art. L.161-36-1 CSS : Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, **chaque bénéficiaire de l'assurance maladie dispose**, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même code, notamment des informations qui permettent le suivi des actes et prestations de soins.



# I. Les garanties juridiques de protection des données du DMP

## 1. Garanties en matière de collecte des données : un consentement “explicite”.

- Pour être valable, le consentement doit être une « manifestation de volonté libre, spécifique et informée » - article 2, §2, h) de la directive de 1995
- Le groupe de travail de l'article 29 indique que le consentement doit être spécifique : « un accord global de la personne concernée pour la collecte de ses données et pour le transfert ultérieur de ses données médicales passées et futures aux praticiens intervenants dans le traitement n'est donc pas un consentement au sens de l'article 2, paragraphe 2, point h de la directive ».





# I. Les garanties juridiques de protection des données du DMP

## 1. Garanties en matière de collecte des données : un consentement “explicite”.

### Art. L.161-36 CSS :

- Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même code, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention.
- Ce **dossier médical personnel est créé** auprès d'un hébergeur de données de santé à caractère personnel agréé **dans les conditions prévues à l'article L. 1111-8** du même code.



# I. Les garanties juridiques de protection des données du DMP

## 1. Garanties en matière de collecte des données : un consentement “explicite”.

**Art.L.1111-8 CSP :**

- 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 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 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 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**.



# I. Les garanties juridiques de protection des données du DMP

## 1. Garanties en matière de collecte des données : un consentement “explicite”.

### Les limites au principe : accès sans consentement.

#### ■ Art. L.161-36-2-2 CSS (Loi 2007-127 du 30 janvier 2007)

I. - Les professionnels de santé accèdent au dossier médical personnel d'une **personne hors d'état d'exprimer sa volonté, en présence d'une situation comportant un risque immédiat pour sa santé**, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté ou alimenté dans une telle situation.

Le médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente mentionné à l'article L. 6112-5 du code de la santé publique qui reçoit un appel concernant une personne accède, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté dans une telle situation, au dossier médical personnel de celle-ci.

- #### ■ II. - Le professionnel de santé recueille, après avoir informé la personne concernée, son consentement pour qu'un **autre professionnel de santé à qui il serait nécessaire de confier une partie de la prestation** accède à son dossier médical personnel et l'alimente.



# I. Les garanties juridiques de protection des données du DMP

## 1. Garanties en matière de collecte des données : un consentement “explicite”.

**Les limites au principe : pas d'accès même avec consentement.**

**Art. L.161-36-3 CSS:** L'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus aux articles L. 161-36-2 et L. 161-36-2-1, même avec l'accord de la personne concernée.

L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.

Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail.

Tout manquement aux présentes dispositions donne lieu à l'application des peines prévues à l'article 226-13 du code pénal.



# I. Les garanties juridiques de protection des données du DMP

## 2. Garantie en matière de conservation des données : du droit de rectification des données au droit à l'oubli.

### Le droit de rectification des données du DMP :

**Art. L.1111-8 CSP** : Les traitements de données de santé à caractère personnel que nécessite l'hébergement prévu au premier alinéa 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.

**Art. 40 Loi n° 78-17 du 6 janvier 1978** : Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.



# I. Les garanties juridiques de protection des données du DMP

## 2. Garantie en matière de conservation des données : du droit de rectification des données au droit à l'oubli.

- concernant les informations contenues dans le DMP (régime du CSS): Droit de rectification VS intégrité des données?
- concernant les données de santé hébergées ayant appartenu au DMP : L'accès de la personne se fait dans le respect de l'article L.1111-7 CSP.

**Art. L.161-36-3 CSS (LFSS 2008)** : Le dossier médical personnel est conservé pendant une durée de dix années à compter de sa clôture.

En cas de décès du titulaire, les ayants droit peuvent solliciter l'accès au dossier conformément aux dispositions du dernier alinéa de l'article L. 1110-4 du code de la santé publique. L'accès à ce dossier peut également intervenir dans le cadre d'une expertise médicale diligentée aux fins d'administration de la preuve.



# I. Les garanties juridiques de protection des données du DMP

## 2. Garantie en matière de conservation des données : du droit de rectification des données au droit à l'oubli.

- Focus sur le masquage

Définition :

Au regard du DMP, le masquage est l'action de rendre invisible une donnée dans son dossier.

Le masquage "masqué" rend invisible cette action.

Conclusions du rapport FAGNIEZ de janvier 2007 :

- accompagnement du patient dans le masquage préférable
- le masquage non masqué n'a pas de sens
- le masquage ne doit pas être opposable à l'auteur de la donnée
- le masquage doit pouvoir « sauter » en cas d'urgence

La loi renvoie au décret DMP le soin de définir les modalités du masquage.



# I. Les garanties juridiques de protection des données du DMP

## 2. Garantie en matière de conservation des données : du droit de rectification des données au droit à l'oubli.

Focus sur le droit à l'oubli :

Notion purement doctrinale => aucune sanction sur ce fondement!

Pourtant notion très utilisée par la CNIL qui demande :

- La suppression automatique des données au bout d'un délai déterminé en fonction des finalités du traitement;
- La mise à jour des informations.

=> suppression acceptée uniquement pour un motif légitime,

=> suppression non prévue si le traitement répond à une obligation légale



# I. Des garanties techniques pour une protection effective

## 1. La question du recueil du consentement

### ■ Rappel des principes

- En droit : Nécessité d'un recueil de consentement **explicite** à la collecte des données de santé du titulaire dans un "DME"
- En fait : Nécessité de ne pas entraver la relation patient - PS par un processus de recueil de consentement trop compliqué

### ■ Expériences récentes de partage de données de santé

- **Dossier pharmaceutique** (L.161-36-4-2 CSS issu de la loi n°2007-127 du 30 janvier 2007)



Expérimentation est autorisée sur tout le territoire (délibération CNIL 2008-041 du 14 février 2008)

=> consentement recueilli par signature du formulaire d'ouverture.

- **Historique de remboursement** (R. 162-1-10 CSS issu du décret n° 2006-143 du 9 février 2006)

=> Le consentement du patient est réputé obtenu par l'utilisation de sa carte vitale qui permet d'accéder au service avec la CPS du professionnel.



# I. Des garanties techniques pour une protection effective

## 1. La question du recueil du consentement

Pour le DMP..

Rapport Door (janvier 2008)

“Le patient doit également donner son consentement à chaque fois qu’un professionnel de santé demande accès à son DMP.

Le législateur a par ailleurs prévu de laisser au patient la possibilité de contrôler à tout moment les accès aux informations de son dossier: après avoir donné son consentement à l’accès à son DMP, puis à son alimentation, le patient pourra décider de « masquer » telle ou telle information inscrite dans son DMP à tel ou tel professionnel de santé autorisé à accéder à son dossier.

Cette faculté n’est pas dirigée contre les professionnels



# I. Des garanties techniques pour une protection effective

## 1. La question du recueil du consentement

- Rapport « Mission Gagneux » (mai 2008), p. 54

Le groupe estime que dans cette phase transitoire – et relativement longue –, il est nécessaire de prendre en considération la réalité des faits et d'opter pour **des solutions pragmatiques, fondées sur une relation de confiance entre le praticien et son patient**. Et ce dès lors, il convient d'y insister, que **des garanties fortes sont par ailleurs apportées à ce dernier**.

Ces garanties sont les suivantes :

- le patient doit toujours avoir le moyen de refuser l'accès d'un professionnel de santé particulier au dossier partagé ;
- son consentement à l'ouverture du DMP et au système de fonctionnement qu'il entraîne est explicite et éclairé ;
- il dispose du droit de masquer certaines données au nom de son droit au secret, à l'oubli et à être protégé des risques de discrimination (cf. infra) ;
- la traçabilité de tous les accès est totale et immédiate, et l'historique des accès est conservé (cf. infra) ;
- des sanctions pénales lourdes doivent être prévues en cas d'accès illicite ou abusif aux données de santé d'une personne (cf. infra) ;
- un comité de surveillance éthique des systèmes d'informations de santé doit être créé.



# I. Des garanties techniques pour une protection effective

## 1. La question du recueil du consentement

p.52 **En toute hypothèse, la procédure d'ouverture doit rester simple, et dans toute la mesure du possible ne nécessiter aucun échange sous forme papier entre la personne concernée et le gestionnaire du système DMP.**

En cible, la carte Vitale 2 pourrait permettre à son titulaire de signifier son accord par saisie d'un code. Dans un premier temps, et dans l'attente de ce type d'outil, l'accord du patient se limiterait à un accord oral donné au professionnel de santé, au service d'accueil de l'établissement de santé ou au guichet public habilité.

Le principe d'une ouverture librement consentie implique la capacité du titulaire de pouvoir fermer son DMP. Les modalités de clôture restent à définir précisément en vue être traduites dans le décret à paraître ; elles doivent rester simples pour les utilisateurs tout en étant sûres, afin d'éviter des clôtures « à tort ».

p.55 En cible, le consentement du patient devra pouvoir être validé par signature électronique, au moyen de la carte Vitale 2 (cf. supra) par exemple. En attendant, c'est le professionnel qui atteste que le titulaire du DMP est son patient et que celui-ci l'a autorisé à accéder à son dossier.



# I. Des garanties techniques pour une protection effective

## 2. La question de l'authentification de celui qui consent

- L'identification du patient grâce à l'INS  
=> Art. L.1111-8-1 CSP

p.61

Conformément aux recommandations de la CNIL, un identifiant spécifique, un **identifiant national de santé (INS)**, sera conçu et mis en œuvre pour le fonctionnement du DMP et des dossiers partagés.<sup>27</sup> Son principe et son champ d'application en ont été précisés par la loi du 30 janvier 2007, qui prévoit l'utilisation d'un identifiant de santé pour la conservation, l'hébergement et la transmission de toutes les données de santé à caractère personnel. Cela étant, un identifiant sert à éviter les confusions (comme l'existence de plusieurs dossiers pour la même personne ou, plus grave, d'un même dossier pour plusieurs personnes). Ce n'est pas une clé d'accès : il ne suffit pas de connaître l'identité ni l'identifiant de santé d'une personne pour accéder à son DMP.

- Authentification du patient par OTP?
- L'identification et l'authentification du PS grâce à sa CPS  
=> Décret « hébergeur » du 4 janvier 2006



# I. Des garanties techniques pour une protection effective

## 2. La question de l'authentification de celui qui consent

p.61 **L'authentification du patient pour l'accès au DMP doit être forte.** L'authentification d'un individu consiste à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes suivantes :

- ce qu'il sait (exemple : mot de passe, code) ;
- ce qu'il possède (exemple : carte à puce, certificat électronique, carte à mot de passe unique...) ;
- ce qu'il est (exemple : caractéristique physique, biométrie...) ;
- ce qu'il sait faire (exemple : geste, signature...).

L'authentification forte repose sur la présentation de deux au moins de ces éléments.

Dans un futur plus lointain, il est vraisemblable que les techniques bio-métriques connaîtront un grand développement. Leur coût et leur complexité ne permettent pas d'en faire une solution de masse dans l'immédiat.

A moyen terme, la future carte Vitale 2 pourrait constituer un vecteur approprié d'authentification (cf. supra).

Dans la phase initiale du projet, le GIP DMP devra mettre en place une solution transitoire. Parmi les dispositifs existants, la délivrance d'un certificat logiciel (à domicile ou sur un support nomade) ou d'un mot de passe à usage unique (transmis par mél ou SMS -« short message service ») sont deux solutions possibles. La seconde a aujourd'hui la préférence du GIP DMP.



# Principaux textes applicables au DMP

- La loi 2004-810 du 13 août 2004 => création du DMP (L. 161-36-1 et s. CSS)
  - La loi 2007-127 du 30 janvier 2007 => DP (L.161-36-4-2 CSS), accès sans consentement au DMP et consentement “en cascade” (L.161-36-2-2 CSS), création de l’INS
  - La loi 2007-1786 du 19 décembre 2007 => INS uniquement pour les BAM (L.1111-8-1 CSP)
    - + Décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel
    - + Décret 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique
- Publication prévue (...) après une large consultation des instances syndicales et ordinales et des associations patients :
- + Décret « identifiant » relatif aux conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et pour la tenue du DMP
  - + Décret « DMP » relatif notamment aux conditions d'accès aux différentes catégories d'informations qui figurent au DMP



## Pour aller plus loin...

- [www.d-m-p.org](http://www.d-m-p.org)
- Rapport Gagneux disponible sur  
[<http://www.sante-jeunesse-sports.gouv.fr/publications-documentations/>]
- [www.conseil-national.medecin.fr/](http://www.conseil-national.medecin.fr/)
- [www.gmsih.fr](http://www.gmsih.fr)
- [www.gip-cps.fr](http://www.gip-cps.fr)
- [www.cnil.fr](http://www.cnil.fr)