

Master 2 Professionnel Droit de l'Internet Public
Administration - Entreprises
Présenté et soutenu publiquement
Le 18 septembre 2008

Le dossier personnel médical : Aspects généraux et sécuritaires

Sarah PAULOIN

Sous la direction de Maître C. FERAL-SCHUHL

Membres du jury :

Président du jury : Monsieur Georges CHATILLON, Directeur du Master Droit de l'Internet Public,

Directeur du mémoire : Maître Christiane FERAL-SCHUHL, Avocat spécialisé dans les domaines de l'informatique et des nouvelles technologies,

Maître de stage : Monsieur Pierre PEREZ, Secrétaire général de la Délégation aux Usages de l'Internet.

Avertissement

L'Université Paris I Panthéon – Sorbonne n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

Je souhaite remercier **Maître Christiane FERAL-SCHUHL** pour avoir accepté de diriger ce mémoire et m'avoir fait bénéficier de ses conseils précieux.

Je remercie également **Monsieur Georges CHATILLON**, directeur du Master Droit de l'Internet public, pour ses enseignements sur les nouvelles technologies ainsi que le partage de sa passion.

Merci, enfin, à **Frédéric BARBIER**, développeur-web, pour ses conseils sur les techniques d'hébergement sur Internet, sa patience et sa relecture attentive.

**LE DOSSIER MEDICAL PERSONNEL:
ASPECTS GENERAUX ET SECURITAIRES**

SOMMAIRE

<i>Remerciements</i>	3
<i>Sommaire</i>	5
<i>Chapitre introductif</i>	6
<i>Partie 1 Un projet ambitieux: l'amélioration de la prise en charge des patients</i>	10
<i>Chapitre 1. Un dossier médical partagé</i>	11
<i>Section 1. Une information partagée</i>	11
<i>Section 2. Une information protégée</i>	17
<i>Chapitre 2 Un dossier médical personnalisé</i>	25
<i>Section 1. Un patient au cœur de son dossier médical</i>	25
<i>Section 2. Le passage d'un dossier « partagé » à un dossier « personnalisé »</i>	30
<i>Partie 2 Un projet complexe</i>	37
<i>Chapitre 1 Des contraintes structurelles</i>	38
<i>Section 1. Une mise en œuvre malaisée</i>	38
<i>Section 2. L'impact de l'outil informatique dans la relation médecin-patient</i>	45
<i>Chapitre 2 Des contraintes techniques</i>	51
<i>Section 1. Les standards de la sécurité informatique</i>	51
<i>Section 2. Les choix techniques du dossier médical personnel</i>	58
<i>Conclusion</i>	73
<i>Table des matières</i>	74
<i>Bibliographie</i>	76
<i>Liste des abréviations</i>	82
<i>Annexes</i>	83

CHAPITRE INTRODUCTIF

§1 L'ORIGINE DU DOSSIER MEDICAL PERSONNEL

Outre, la volonté de réduire les dépenses de santé par la « maîtrise médicalisée » de celles-ci, la création d'un dossier médical personnel (DMP) vise à améliorer la prise en charge des patients, en optimisant le partage de l'information médicale grâce à l'association « patient/professionnel de santé ». L'évolution de la technique, notamment le développement de l'Internet, a servi cet objectif et a abouti à la création du dossier médical personnel, outil moderne de communication et de partage de l'information. Grâce au dossier médical personnel, chacun des acteurs du secteur médical, et en premier lieu le patient, peut accéder à l'information qui le concerne.

La conduite opérationnelle du DMP a été confié à un Groupement d'Intérêt Public, intitulé « groupement d'intérêt public du dossier médical personnel » (GIP-DMP), qui regroupe l'Etat, représenté par le Ministère de la santé, l'Assurance maladie(CNAMTS), la Caisse des dépôts et consignations (CDC), et des représentants des professionnels de santé et des patients.

Le GIP-DMP a pour mission d'assurer la maîtrise d'ouvrage du dossier médical personnel, et pour ce faire s'est vu confier la conception, la réalisation, le fonctionnement du DMP ainsi que la gestion de ses probables évolutions.

Initialement, le lancement opérationnel du DMP devait avoir lieu courant 2007, mais des dysfonctionnements affectant la structure même du GIP-DMP ont retardé ce lancement. En effet, le GIP-DMP a été trop longtemps limité dans son activité par des moyens insuffisants et fragilisé par l'instabilité chronique de son équipe.

Le GIP-DMP a décidé de déployer le dossier médical personnel en deux phases successives :

- une phase d'expérimentation, afin de tester les produits et fonctionnalités proposés par les industriels ;
- une phase de généralisation, adaptée en fonction résultats de la première phase.

§2 LES OBJECTIFS DU DOSSIER MEDICAL PERSONNEL

La loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie¹ prévoit en son article 3 qu' « *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 [...] d'un "dossier médical personnel" (DMP), constitué de l'ensemble des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins [...], et notamment des informations qui permettent le suivi des actes et des prestations de soins* ».

La loi précise que le dossier médical personnel sera un dossier médical unique, informatisé et déposé auprès d'un hébergeur de données de santé agréé. Il sera gratuit et, sans être juridiquement obligatoire², aura vocation à être à disposition de tout bénéficiaire de l'assurance maladie.

Le bénéficiaire sera le titulaire du dossier et à ce titre, il désignera l'hébergeur de son choix et aura toute prérogative pour maîtriser les processus d'ouverture, de consultation et d'approvisionnement de son DMP.

A la lecture de la loi du 13 août 2004, dont le DMP est la clé de voûte, les avantages attendus de celui-ci sont les suivants :

- une meilleure coordination des professionnels de santé, de nature à réduire, grâce au partage de l'information, les prescriptions redondantes ou les erreurs résultant d'une mauvaise circulation de l'information ;
- une meilleure qualité des soins dispensés par les professionnels et les établissements de santé grâce à l'accès en temps réel à une information unifiée concernant le patient ;
- une meilleure information des assurés, de nature à les rendre davantage responsables de leur santé ;
- une plus grande maîtrise des dépenses d'assurance maladie, via la diminution des actes redondants, inutiles ou iatrogènes³.

Ainsi, le DMP n'a pas vocation à se substituer aux dossiers des professionnels de santé tels que « le dossier pharmaceutique », le « Web-médecin » (historique des remboursements), le dossier communiquant de cancérologie.

¹L. n° 2004-810, 13 août 2004 relative à l'assurance maladie, JO n°190, 17 août, p.14598. L'article 3 de la loi établit que « Le chapitre Ier du titre VI du livre Ier du code de la sécurité sociale est complété par une section 5 ainsi rédigée : « *Section 5 : « Dossier médical personnel [...]* ». Le texte cité constitue l'art. L. 161-36-1 du CSS créé par ce même article 3.

²La loi ne rend pas obligatoire l'ouverture d'un dossier médical personnel mais elle lie celle-ci au niveau de remboursement du patient, cf infra.

³ « Se dit d'une maladie causée par le traitement médical », in Dictionnaire Hachette, Edition 2008.

§3 LE CADRE LEGAL DU DOSSIER MEDICAL PERSONNEL

Outre la loi n°2004-810 du 13 août 2004 relative à l'assurance maladie qui crée le dossier médical personnel, d'autres lois se rendent applicables.

En premier lieu, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés⁴, conformément à son champ d'application, veille à la mise en place du DMP. Selon l'article 1^{er} de ladite loi, « *l'informatique 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* ». Pour cela, elle met en place un dispositif de protection applicable à tous les traitements automatisés (ou non) de données à caractère personnel.

La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé⁵, dite « loi Kouchner ». L'esprit de cette loi est analogue à celui de la loi « Informatique et Libertés », dans la mesure où il s'agit aussi d'une loi protectrice. Spécifique au secteur de la santé, elle octroie toute une série de droits au malade, parmi lesquels le droit à la protection de sa vie privée.

Le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique⁶, dit décret « hébergeurs », qui précise les modalités de l'agrément des hébergeurs d'informations de santé.

L'article 25 de la loi n°2007-127 du 30 janvier 2007 relative à l'organisation de certaines professions de santé⁷ qui vise à favoriser la bonne utilisation du DMP par les acteurs du projet : médecins et patients en premier lieu. Cette loi fait suite à la phase d'expérimentation et a pour but de faire certains aménagements compte tenu des résultats des expérimentations. Ces évolutions concernent notamment la prise en charge du patient en cas d'urgence et la base légale de tarification.

Le décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique⁸, dit décret « confidentialité ». Pris en application de l'article L.1110-4 du Code de la santé publique et de l'article L.161-36-1 du Code de la sécurité sociale, il précise les conditions d'usage des données de santé détenues sur support informatique ou transmises par voie électronique.

⁴Loi n°78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°152, 2 juill., p.9559, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

⁵Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JO du 5 mars, p.4118, texte n°1.

⁶Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JO n°4, 5 janv., p.174, texte n°14.

⁷Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique (Titre résultant de la décision du Conseil constitutionnel n° 2007-546 DC du 25 janvier 2007), JO n°27, 1^{er} février, p.1937, texte n°1.

⁸Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), JO n°113, 16 mai, p.9362, texte n°210.

Le décret « identifiant de santé », pris en application de l'article 25 de la loi du 30 janvier 2007, n'est toujours pas paru à ce jour. Il doit prévoir la création d'un nouvel identifiant de santé ainsi que ses modalités d'application, permettant l'accès et l'identification des patients au DMP.

Enfin, le décret le plus attendu, le « décret DMP » prévu par l'article L.161-36-4 du Code de la sécurité sociale, qui doit préciser le contenu du DMP, c'est-à-dire les différentes catégories d'informations médicales dont l'inscription appartient aux professionnels de santé (un avant-projet de ce décret en propose une liste non limitative répartie en données médicales générales, données relatives aux soins reçus, données de prévention, images radiologiques ou tout autre imagerie médicale).

Selon le rapport d'activité 2006/2007 du GIP-DMP⁹, ce décret est en cours d'achèvement. L'avant-projet du décret, préparé par la direction de la Sécurité sociale en collaboration avec le GIP-DMP, a été soumis fin 2006 à la consultation publique sur le site du www.d-m-p.org. Le déploiement du DMP est suspendu à la publication de ce décret qui doit prévoir les conditions d'application de la loi du 13 août 2004 relative à l'assurance maladie, instituant le DMP. Le projet de décret serait dans la phase de consultation qui précède sa publication au Journal Officiel¹⁰.

⁹ Accessible depuis http://www.d-m-p.org/docs/DMP_RA_2006.pdf.

¹⁰ Rapport d'activité 2006/2007 du GIP-DMP.

PARTIE I

UN PROJET AMBITIEUX :

L'AMÉLIORATION DE LA PRISE EN CHARGE DES PATIENTS

CHAPITRE 1. UN DOSSIER MEDICAL PARTAGE

Le dossier médical personnel a pour objectif de partager l'information plus efficacement qu'elle ne l'est aujourd'hui (Section 1) ; cette information, élément propre à l'intimité du patient, doit être protégée à plusieurs titres (Section 2).

SECTION 1. UNE INFORMATION PARTAGEE

La création du dossier médical personnel participe de la volonté d'optimiser le système de santé français, dont le fonctionnement actuel ne cesse d'accroître le déficit de la France. A ce titre, il a pour ambition une information médicale plus efficace car mieux répartie (§1), mais garde les caractéristiques d'un dossier médical, notamment quant à son contenu (§2).

§1. LA NECESSITE D'UNE REPARTITION EFFICACE DE L'INFORMATION MEDICALE

Avec l'avènement de la technologie de nouveaux besoins des professionnels de santé sont en prendre en compte (A), dans le but d'améliorer la continuité et la coordination des soins (B).

A. LA PRISE EN CONSIDERATION DE NOUVEAUX BESOINS

Initialement, le dossier médical personnel était un outil réservé aux professionnels de santé, destiné à favoriser « *la qualité, la continuité et la coordination des soins* ». L'outil informatique ici n'est pas une fin en soi mais un vecteur du développement de nouveaux usages dans le domaine médical. Cette volonté correspond à la nécessité d'établir un partage efficace de l'information médicale dans un contexte de transformation des pratiques médicales. En effet, le nombre de professionnels de santé ne cessent de croître en raison d'une spécialisation accrue des soins. Tous les professionnels de santé doivent pouvoir communiquer entre eux tout en conservant la qualité et la coordination des soins.

Si ces nouveaux besoins sont relativement récents, les problèmes qu'ils vont engendrer sont redoutés depuis quelques années déjà. En 1999, une étude intitulée « Interopérabilité des dossiers de santé informatisés et normalisation » du cabinet Canope affirmait :

« Actuellement, les médecins ne se sont pas encore vraiment appropriés, à la différence d'autres professions, l'usage de l'informatique comme un outil de travail

complètement banalisé. [...] Un médecin traitant un patient dans son cabinet et un établissement devrait pouvoir accéder aux mêmes informations dans les deux localisations et à travers des systèmes éventuellement différents. »

Aujourd'hui, la qualité, la continuité et la coordination des soins sont assurées en premier lieu par le dossier médical, dans sa « version papier », lequel rassemble toute une série d'informations médicales d'un individu. Les règles de communication du dossier médical sont précisées à l'article 45 du Code de déontologie médicale¹¹ (repris à l'article R.4127-45 du Code de la santé publique) qui impose la transmission des éléments utiles à la continuité des soins.

Mais, le dossier médical, peut s'avérer très complexe et contre-productif, notamment en cas de pathologie lourde. Ce sera le cas d'un dossier médical très volumineux dont la gestion peut être difficile, notamment en termes d'extraction et de transmission, d'archivage et même de lecture. Ces difficultés peuvent être résolues plus facilement grâce à la dématérialisation du dossier médical.

Ainsi, le DMP permettra au professionnel de santé de rassembler l'ensemble des documents sur le support électronique unique du DMP, ce qui lui évitera la recherche d'informations éparées et la lourdeur matérielle des échanges sous forme papier pour optimiser son temps.

B. CONTINUITÉ, COORDINATION DES SOINS ET AMÉLIORATION DES TECHNIQUES MÉDICALES

Les avancées techniques et découvertes médicales, ont permis une prise en charge quasi-personnalisée du patient atteint d'une pathologie singulière. Un médecin peut ainsi mettre au point un protocole de soins personnalisé pour son patient. Mais en termes de continuité de soins, des problèmes peuvent apparaître.

Prenons l'exemple d'un patient qui suit un traitement en centre hospitalier pour une pathologie assez rare qui a demandé une phase de recherche assez longue. Que se passerait-il en cas de difficultés nécessitant l'appel en urgence d'un médecin généraliste, par exemple, en cas de voyage à l'étranger ou en l'absence du médecin traitant ? Comment se transmettra l'information relative à la maladie et au traitement entre le médecin traitant et son remplaçant d'un jour ? Par courriel ? Sécurisé, non sécurisé ?

Le dossier médical du patient a également vocation à contenir l'histoire médicale du patient. Dès lors, il participe à l'établissement du diagnostic, contenant antécédents et traitements en cours. Certaines informations contenues dans le dossier médical du patient doivent être connues de tous les médecins consultés. La « mémoire » du dossier médical peut

¹¹ Article 45, Code de déontologie médicale : « *Indépendamment du dossier de suivi médical prévu par la loi, le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques. Dans tous les cas, ces documents sont conservés sous la responsabilité du médecin. Tout médecin doit, à la demande du patient ou avec son consentement, transmettre aux médecins qui participent à sa prise en charge ou à ceux qu'il entend consulter, les informations et documents utiles à la continuité des soins. Il en va de même lorsque le patient porte son choix sur un autre médecin traitant ».*

apparaître une source plus sûre que celle du patient, « mémoire à laquelle les professionnels de santé pourront avoir accès en cas de dématérialisation du dossier médical et de sa mise en réseau. Ce regard ponctuel sur l'état de santé du patient, passé et actuel, permettra sans nul doute une meilleure qualité des soins.

§2 LE CONTENU DU DOSSIER MEDICAL PERSONNEL

L'ensemble du contenu du dossier médical personnel n'a pas encore été défini avec précision. Mais on peut dire, à ce jour, avec certitude qu'il contiendra des données à caractère personnel (A), parmi lesquelles des données dites « sensibles » (B).

A. DES DONNEES A CARACTERE PERSONNEL

L'article 2 de la loi n°78 - 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par loi n°2004-801 du 6 août 2004¹², définit une « donnée à caractère personnel » comme :

« Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

Initialement la loi évoquait la notion de « donnée nominative » et non de « données à caractère personnel » introduite suite à la transposition de la directive du 24 octobre 1995. L'ancien article 4 de la loi de 1978 définissait de manière fonctionnelle la notion de « donnée nominative », définissant comme « toute donnée permettant directement ou non l'identification d'une personne ».

Pour autant, lors de la transposition de la directive 95/46/CE du 24 octobre 1995¹³, la loi du 6 août 2004 n'a pas repris fidèlement la définition de la notion de « donnée à caractère personnel » posée par la directive, réduisant du même coup son champ d'application. Alors que la directive vise l'ensemble des moyens susceptibles d'être « raisonnablement » mis en œuvre pour identifier une personne, la loi française ne reprend pas l'adverbe « raisonnablement » afin de « prévenir (toute) difficultés d'interprétation »¹⁴ et échappe à l'ambiguïté d'une telle interprétation.

¹²Loi n°78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n° 152, 2 juill., p.9559, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

¹³Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, J.O.C.E n° L.281 du 23 novembre 1995, p. 31 à 50.

¹⁴TÜRK, Alex. Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n°367, Sénat, déposé le 23 juin 2004, p.16 de 121.

Le champ d'application de la notion de « donnée à caractère personnel » est large. Le rattachement direct ou indirect de la donnée à la personne visée suffit à remplir la condition d'identification posée dans la loi. Seule l'anonymisation empêchant tout lien entre la donnée et la personne permet de sortir de la définition de « donnée à caractère personnel ».

A ce titre, on fait une distinction entre les données « directes » et les données « indirectes ». Sont des données « directes », par exemple le nom, le prénom, l'adresse postale, le numéro de sécurité sociale. Mais le numéro de téléphone, le système de contrôle d'accès par badge, les adresses de courrier électronique sont qualifiées de données « indirectes ».

Qu'en est-il des données contenues dans le dossier médical personnel ? Selon la loi n°2004-810 du 13 août 2004 relative à l'Assurance maladie¹⁵, le contenu envisagé du DMP informatisé est appelé à recevoir, sous réserve du consentement de son titulaire, outre les données d'identification, l'ensemble des informations « *concourant à la coordination, la qualité, la continuité des soins et la prévention* ». Concrètement, ceci recouvre :

- les données médicales générales (antécédents, allergies et intolérances reconnues, vaccinations, historiques des consultations, synthèses, etc.) ;
- les données de soins (résultats d'examens, compte rendus d'actes diagnostiques et thérapeutiques, bilans, traitements prescrits et administrés, protocoles de soins, etc.) ;
- les données de prévention (facteurs de risque individuels, comptes rendus, traitements préventifs, etc.) ;
- des documents d'imagerie médicale ;
- un espace d'expression du titulaire.

Comme les données contenues dans le dossier médical personnel sont des données susceptibles d'identifier la personne visée, elles doivent être qualifiées de « données à caractère personnel ». Ainsi, le DMP entre dans le champ d'application de la loi « Informatique et Libertés » au titre de « fichier de données à caractère personnel ». A ce propos, l'article 2 de la loi du 6 août 2004 modifiant la loi de 1978, définit un « fichier de données à caractère personnel » comme « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* ». Il précise également la notion de « traitement de données à caractère personnel » qui est « *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 ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ».

Il faut souligner que la simple collecte de données à caractère personnel est qualifiée de « traitement » par la loi et que la liste des traitements concernés par la loi « Informatique et Liberté » n'est pas exhaustive. En effet, l'automatisation n'est plus une condition nécessaire

¹⁵L. n° 2004-810, 13 août 2004 relative à l'assurance maladie, JO n°190, 17 août, p.14598.

pour entrer dans le champ d'application de la loi et tout traitement, même manuel, peut être concerné.

A la notion de « données à caractère personnel » est attaché un régime déclaratif. Le responsable du traitement, automatisé ou non, de données à caractère personnel doit effectuer une déclaration auprès de la Cnil dans les conditions définies par la loi n°78-17 du 6 janvier 1978 modifié. Le responsable du traitement est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens¹⁶.

B. DES DONNÉES DITES « SENSIBLES »

Certaines données à caractère personnel bénéficient d'un régime spécial car elles sont dites « particulièrement sensibles ». A ce titre, elles sont interdites de collecte, sauf dérogations prévues par la loi. Elles rassemblent des catégories d'information faisant apparaître directement ou indirectement:

- les origines raciales;
- les opinions politiques, philosophiques ou religieuses;
- les appartenances syndicales des personnes;
- les informations relatives à la santé ou à la vie sexuelle¹⁷;
- ou relatives aux infractions, condamnations ou mesures de sûreté.

Concernant précisément les données personnelles de santé, le principe d'interdiction de collecte et de traitement de ces données souffre quelques exceptions limitativement énumérées par l'article 8 de la loi dite « Informatique et Libertés »:

- Dérogation au consentement des personnes concernées: il peut être dérogé à cette interdiction de principe pour les traitements pour lesquels la personne concernée a donné son consentement exprès, donné de préférence par écrit, sauf si la loi prévoit que l'interdiction ne peut être levée par ce consentement ;
- Sauvegarde de la vie humaine: dérogation pour les traitements qui sont nécessaires à la sauvegarde de la vie humaine mais pour lesquels le consentement de la personne est juridiquement ou matériellement impossible à obtenir¹⁸;
- Intérêt direct du patient: La Cnil considère en effet que les traitements de

¹⁶L. n°78-17, 6 janvier 1978 modifiée, art. 3, I.

¹⁷L. n°78-17, 6 jan.1978, modifiée, art. 8.

¹⁸L. n°78-17, 6 janv. 1978, modifiée art. 8, 2°.

données personnelles de santé sont légitimes lorsqu'ils ont pour finalité de permettre aux professionnels de santé de mieux assurer le suivi médical des patients et de faciliter leur prise en charge par les organismes d'assurance maladie obligatoire. Elle a admis que, dans le cadre de ces finalités, les données de santé à caractère personnel puissent être communiquées sous certaines conditions à des destinataires et tiers¹⁹. Aussi les professionnels de santé sont-ils autorisés à échanger des informations relatives à un même patient, sauf opposition de sa part, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge possible ;

- Intérêt de la santé publique: Les traitements de données personnelles de santé sont légitimes lorsqu'ils ont pour finalités de permettre aux professionnels de santé de participer aux actions de prévention et de veille sanitaire poursuivies par les autorités de santé et de contribuer aux travaux de recherche médicale²⁰. Plus encore, les professionnels de santé sont contraints, dans certaines circonstances, de communiquer certaines informations aux autorités sanitaires, par exemple pour certaines maladies infectieuses qui exigent une intervention urgente ou dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique (C. santé publ., art. L.3113-1). Cette obligation revêt même un caractère pénal puisque les professionnels de santé sont ainsi tenus de déclarer aux autorités judiciaires, médicales ou administratives, certaines situations dont ils ont connaissance (C. pén., art. 226-14 – et C. santé publ., art. L.2112-6).
- Recherche médicale: la recherche médicale justifie la transmission de données personnelles de santé (pharmacovigilance, études épidémiologiques, observationnelles, essais cliniques, etc.), sous réserve du droit d'opposition des patients concernés²¹.

Ce régime d'interdiction a été renforcé, notamment, par l'article 226-13 du 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 15 000 euros d'amende* »²², sous réserve des dérogations énumérées à l'article 226-14 du même code.

Et par le Code de la santé publique qui interdit en toutes circonstances la constitution et l'utilisation à des fins de prospection ou de promotion commerciale de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des données personnelles de santé (même rendues anonymes à l'égard des patients) dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel

¹⁹Cnil, délib.n°97-008, 4 févr. 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel, JO 12 avril., p.5606.

²⁰*Ibidem*.

²¹L. n°94-548, 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°152, 2 juill., p.9559.

²²C. pén., 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 15000 euros d'amende.* »

prescripteur²³.

Conformément à ce qui précède, le traitement informatisé des données de santé mis en place à travers le dossier médical personnel n'est pas contraire à la loi. L'objectif d'assurer une meilleure « *qualité, continuité et coordination des soins* » qui fonde la création du dossier médical personnel, correspond aux exigences posées par la loi « Informatique et Libertés » pour entrer dans le cadre des exceptions relatives à l'intérêt direct du patient et à l'intérêt de santé publique.

SECTION 2. UNE INFORMATION PROTEGEE

Les informations contenues dans le dossier médical personnel sont protégées à double titre : en tant qu'informations contenues dans un traitement automatisé (§1) et en tant qu'informations de santé (§2).

§1 ENTANT QU'INFORMATION D'UN TRAITEMENT AUTOMATISE

Le traitement des données à caractère personnel est limité tant au niveau du droit interne (B) qu'au niveau du droit européen (A).

A. LE CORPUS JURIDIQUE EUROPEEN

La protection juridique des individus vis-à-vis du traitement automatisé de leurs données à caractère personnel, est également assurée au niveau européen par la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Adoptée le 28 juin 1981, elle a été ratifiée par l'ensemble des Etats membres de l'Union européenne et est entrée en vigueur le 1^{er} octobre 1985. Précisons, qu'elle est libellée « Convention » et non « Convention européenne » afin de ne pas se limiter à la seule adhésion d'Etats européens.

La Convention n°108 part du postulat que certains droits de la personne doivent être protégés au regard de la liberté de circulation de l'information. Ce principe est déjà présent au sein de l'article 10 de la Convention de sauvegarde des droits de l'homme et des libertés

²³C. santé publ., art. L.4113-7.

fondamentales²⁴ (CESDH) et de l'article 19 du Pacte international sur les droits civils et politiques²⁵.

Pour autant, la Convention pose certaines restrictions ou conditions à l'exercice de la liberté de circulation d'informations. Elle aménage ainsi l'application de cette liberté en raison de la protection d'autres droits et libertés individuels, notamment le droit au respect de la vie privée et familiale²⁶.

La Convention prévoit un « noyau dur » de droits consacrant un minimum de protection des personnes au regard du traitement automatisé de données à caractère personnel. Il en résulte une harmonisation des législations en vigueur au sein des pays parties à la Convention, visant ainsi une meilleure gestion des conflits de lois. Par exemple, dans son Chapitre III, la Convention règlemente la pratique des flux transfrontières de données en conciliant le principe de libre circulation des informations et celui de la protection des données.

Dans le même esprit de la loi française de 1978, la Convention considère « les données à caractère personnel relatives à la santé » comme des données particulièrement sensibles ; cela recouvre les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu, mais aussi les informations sur un individu bien portant, malade ou décédé²⁷.

Enfin, l'article 6 de la convention prévoit que « *les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées...* ». Il s'agit ici de catégories particulières de données qui sont considérées comme étant particulièrement sensibles, quelque soit l'Etat membre. Les risques d'atteintes aux droits et intérêts des individus, que fait courir le traitement des données va ainsi dépendre de la nature même de ces données, considérées comme « sensibles », et non de leur contexte d'utilisation, ne va pas dépendre du contexte d'utilisation.

Au niveau européen, la réglementation posée par la Convention n°108 aurait pu suffire. Mais dans un contexte de marché commun, de libre concurrence et libre circulation des biens, la Commission européenne a jugé bon la mise en place d'une législation commune sur les données personnelles. En effet, le marché intérieur commun mis en place par l'Union européenne appelle une coordination de la protection des données personnelles dans le but d'éviter les entraves aux flux transfrontières de données.

La Convention n°108, bien qu'ayant valeur de traité international, n'a pas été jugée suffisante en raison de l'absence de ratification de certains pays membres de l'Union européenne. Et afin de concilier « vie privée » et « liberté d'entreprise », Bruxelles a élaboré la directive

²⁴CESDH, art. 10, Liberté d'expression: « *1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.* ».

²⁵PIDCP, art. 19 : « *1. Nul ne peut être inquiété pour ses opinions.*

2. Toute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix.».

²⁶Notamment posé par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales : « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »

²⁷ Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ; <http://conventions.coe.int/Treaty/FR/Reports/Html/108.htm>, au 15 juin 2008.

européenne 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données²⁸. Entrée en vigueur le 25 octobre 1998, elle a pour objectif d'harmoniser les législations des Etats-membres en matière d' « Informatique et Libertés », en établissant un cadre réglementaire.

L'article 8 de la directive interdit tout traitement des données de santé à caractère personnel. Néanmoins, il prévoit des dérogations reposant sur le consentement explicite de la personne concernée et moyennant l'introduction de garanties appropriées. En outre, il donne la possibilité aux Etats membres de prévoir d'autres dérogations dans leur législation interne pour un motif d'intérêt public important.

Enfin, elle institue un groupe de travail regroupant les représentants de chaque autorité de protection des données de l'Union européenne. Ce groupe est intitulé « groupe article 29 »²⁹ ou « G29 ». Cette autorité a, notamment, pour mission de rendre des avis à la Commission européenne au nom des Etats membres sur les questions relatives à la protection des données et publie un rapport annuel d'activité dans ce domaine. Le « G29 » contribue également à l'élaboration de règles européennes en matière de protection des données personnelles. Le 17 avril 2007, Alex TÜRK, président de la Cnil, a été élu vice-président du « Groupe de l'article 29 » pour une durée de deux ans. Les 28 délégations des autorités nationales de protection des données représentées l'ont élu à l'unanimité.

La France a été l'un des derniers pays à transposer la directive, suite à de vives critiques des dispositions de la directive qui apparaissaient comme remettant en cause la loi française « Informatique et Libertés ». Le 11 janvier 2000, la Commission européenne a alors engagé une procédure d'infraction³⁰, pour non-notification des mesures de transposition nationale de la directive sur la protection des données, contre la France mais aussi le Luxembourg, les Pays-Bas, l'Allemagne et l'Irlande.

La directive européenne remet principalement en cause la distinction public/privé et modifie le dispositif français des formalités préalables : en principe, tout fichier doit être déclaré ou faire l'objet d'une demande d'avis, mais la directive a pris le parti d'alléger cette procédure jugée trop contraignante. En outre, la directive ne parle plus de « données nominatives » mais de « données à caractère personnel ».

La loi française de transposition³¹ de la directive n'interviendra que 9 ans après l'adoption de la directive, par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés³².

²⁸Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, J.O.C.E n° L.281 du 23 novembre 1995, p. 31 à 50.

²⁹Par référence à l'article de la directive européenne qui l'institue.

³⁰Article 226 CE : « Si la Commission estime qu'un Etat membre a manqué à une des obligations qui lui incombent en vertu du présent traité, elle émet un avis motivé à ce sujet, après avoir mis cet Etat en mesure de présenter ses observations. Si l'Etat en cause ne se conforme pas à cet avis dans un délai déterminé par la Commission, celle-ci peut saisir la Cour de Justice ».

³¹L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°182, 7 août, p. 14063, texte n°2.

³²L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°182, 7 août, p. 14063, texte n°2.

B. LA LOI FRANÇAISE « INFORMATIQUE ET LIBERTÉS »

La loi n°78-17 du 6 janvier 1978 dite loi « Informatique et Libertés »³³ trouve à s'appliquer à la mise en œuvre du DMP, comme cela a été évoqué ci-dessus.

Cette loi met en place un système de protection des individus contre l'atteinte à leurs libertés résultant de la collecte et du traitement de leurs données à caractère personnel. Elle impose alors au responsable du traitement plusieurs obligations. Il doit soumettre ses traitements à des conditions de licéité reposant sur une collecte loyale et licite, effectuée pour des finalités déterminées, lesquelles n'excluent pas, sous certaines conditions, un traitement ultérieur à des fins statistiques ou à des fins de recherche scientifique. Il doit également recueillir le consentement de la personne concernée par ledit traitement.

Préalablement à la mise en œuvre des traitements, le responsable du traitement doit remplir certaines formalités : les traitements doivent faire l'objet d'une déclaration ou être soumis à autorisation. Cette obligation ne s'applique pas aux traitements de tenue de registre qui en sont dispensés. En cas de traitements de données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR), le responsable du traitement doit obtenir une autorisation par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'Informatique et des libertés (Cnil).

Il lui est interdit de collecter les informations dites « sensibles », sous réserve des dérogations prévues par la loi³⁴.

La loi du 6 janvier 1978 a mis en place la Commission nationale de l'informatique et des libertés (Cnil), autorité administrative indépendante chargée de veiller au respect de la loi « Informatique et Libertés ». L'avis de la Cnil doit être sollicité par le Gouvernement avant toute transmission au Parlement d'un projet de loi créant un traitement automatisé de données nominatives. Les traitements de données à « risques » sont soumis à son autorisation.

Un des secteurs phares de son contrôle sont les applications informatiques. Elle est particulièrement attentive dans la surveillance de la sécurité des systèmes d'informations afin de s'assurer que toutes les précautions sont prises pour éviter la déformation ou la communication des données à des personnes non autorisées.

Elle veille à l'application de la loi « Informatique et Libertés » grâce à son pouvoir de contrôle par le biais de l'exigence de formalités préalables. Des moyens répressifs ont été mis à sa disposition et renforcés par la loi du 6 août 2004³⁵ : contrôle sur place et sur pièces, demande de communication des documents, transmission au parquet des infractions constatées, amendes dans de rares cas.

³³Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°152, 2 juill., p.9559, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

³⁴Cf. supra B. Des données sensibles.

³⁵Art.3, L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°182, 7 août, p. 14063, texte n°2.

Des sanctions pénales sont également prévues par les articles 226-16 à 226-24 du Code pénal en cas d'infraction à la loi « Informatique et Libertés ».

Conformément aux dispositions de la loi « Informatique et Libertés », la Cnil est intervenue à tous les stades du projet de dossier médical personnel : avis sur le projet de loi créant le DMP³⁶, sur les projets de décret, sur les agréments des hébergeurs de données, sur les conventions relatives aux expérimentations et à l'occasion des contrôles qu'elle a effectués sur ces dernières, sur les autorisations relatives aux applications informatiques utilisées³⁷.

§2 ENTANT QU'INFORMATION DE SANTE

Les données de santé bénéficient d'un cadre législatif de protection assez complet, notamment par le biais des lois du 4 mars 2002 et du 13 août 2004 (A), mais aussi en raison du respect du secret médical (B) imposé aux professionnels de santé.

A. LES LOIS RELATIVES A LA PROTECTION DES MALADES ET A L'ASSURANCE MALADIE

Informations d'un traitement automatisé, mais surtout informations de santé, les données contenues au sein du DMP bénéficient à ce titre de l'application des dispositions protectrices de la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, et de la loi n°2004-810 du 13 août 2004 relative à l'assurance maladie³⁸.

Codifiée à l'article L. 1110-4 du code de la santé publique, l'article 3 de la loi relative à la protection des malades³⁹ affirme que : « *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* ».

³⁶Cnil, délib., n°04-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie ; Cnil, Avis sur le dossier médical personnel, 12 juillet 2004 [http://www.cnil.fr/index.php?id=1613&news\[uid\]=178&cHash=844a59142b](http://www.cnil.fr/index.php?id=1613&news[uid]=178&cHash=844a59142b) ; Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel ; Cnil, Conclusions des missions de contrôles relatives à l'expérimentation du DMP.

³⁷Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel ; Cnil, Conclusions des missions de contrôles relatives à l'expérimentation du DMP.

³⁸L. n° 2004-810, 13 août 2004 relative à l'assurance maladie, JO n°190, 17 août, p.14598.

³⁹Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JO du 5 mars, p.4118, texte n°1. Cette disposition figure également à l'article L. 161-36-1 A du Code de la sécurité sociale.

La loi du 4 mars 2002 fixe un régime de protection analogue à celui de la loi « Informatique et Libertés ». Mais ces deux régimes sont bâtis sur une logique inverse : alors que la première octroie certains droits aux patients, la seconde exige du responsable du traitement l'accomplissement de certains devoirs.

Une correspondance entre les deux lois peut ainsi être établie:

- Le droit à l'information du patient sur son état de santé et sur l'ensemble des traitements envisagés (article L.1111-2 du code précité⁴⁰);

- Le droit à la confidentialité des informations médicales à caractère personnel (Article L. 1110-4 du code de la santé publique)
et
l'obligation faite au responsable du traitement informatique de veiller à la sécurité des données et d'empêcher l'accès de tiers non autorisés (Article 34 de la loi Informatique et Libertés) ou le droit pour une personne d'obtenir de ce responsable que les données la concernant soient « *selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées* » (article 40 de la loi « Informatique et Libertés) ;

- Le droit à l'information du patient (article L. 1111-2 du code de la santé publique)
et
l'obligation faite au responsable du traitement informatique de fournir des informations sur la finalité de son action et sur les droits de la personne concernée par les informations traitées ainsi que sur les moyens qu'elle a de s'y opposer (article 32 de la loi « Informatique et Libertés) ;

- Le droit d'accès aux informations médicales personnelles (article L. 1111-7 du code de la santé publique)
et
le droit de se faire communiquer les données à caractère personnel faisant l'objet d'un traitement informatique (article 39 de la loi Informatique et Libertés).

⁴⁰ C. santé publ., art. L.1111-2 : «*Toute personne a le droit d'être informée sur son état de santé. Cette information porte sur les différentes investigations, traitements ou actions de prévention qui sont proposés, leur utilité, leur urgence éventuelle, leurs conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent ainsi que sur les autres solutions possibles et sur les conséquences prévisibles en cas de refus. Lorsque, postérieurement à l'exécution des investigations, traitements ou actions de prévention, des risques nouveaux sont identifiés, la personne concernée doit en être informée, sauf en cas d'impossibilité de la retrouver. Cette information incombe à tout professionnel de santé dans le cadre de ses compétences et dans le respect des règles professionnelles qui lui sont applicables. Seules l'urgence ou l'impossibilité d'informer peuvent l'en dispenser.[...]* ».

Le droit d'accès prévu par l'article L.1111-7⁴¹ vise toutes les informations détenues par les professionnels et les établissements de santé, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé. Le malade peut accéder à ces informations directement ou par l'intermédiaire d'un médecin dans un délai qui ne peut excéder huit jours suivant sa demande, mais qui ne peut être inférieur à un délai, dit de « réflexion », de deux jours. La présence d'une tierce personne est recommandée lorsque l'information est particulièrement sensible, comme l'annonce d'une maladie grave.

Enfin, le stockage des données de santé à caractère personnel doit être entouré de garanties relatives à leur intégrité et à leur confidentialité. L'article L. 1111-8 du Code de la santé publique encadre très strictement l'activité des hébergeurs de données de santé, en instituant une responsabilité spécifique relative à la protection des données de santé. La prestation d'hébergement est régie par le contrat. Le consentement du patient est toujours requis, en cas de relation contractuelle, relatif à l'hébergement, entre un professionnel de santé ou un établissement de santé et un hébergeur. Les articles R. 1111-9 à R. 1111-16, introduits par le décret du 4 janvier 2006⁴², précisent les conditions d'agrément des hébergeurs.

B. LA REGLE DU SECRET MEDICAL

Avant d'être une obligation légale, le secret médical était une règle morale professionnelle fondée sur le serment d'Hippocrate⁴³. Autrefois, le secret médical revêtait un caractère religieux, le médecin étant alors le confesseur des maladies du corps. Aujourd'hui, il n'est fondé que sur les seules considérations laïques: l'intérêt de la santé publique, l'intérêt de la profession médicale ou l'intérêt du patient. Il a fallu attendre le Code pénal de 1810, et son article 378 réprimant la violation du secret médical, pour qu'il soit reconnu juridiquement.

Conformément à la jurisprudence⁴⁴, les informations sur la santé d'un individu relèvent

⁴¹ C. santé publ., art. L.1111-7 : « Toute personne a accès à l'ensemble des informations concernant sa santé 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 des résultats d'examen, comptes 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 ».

⁴² Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique, J.O. du 5 janvier, texte n°14.

⁴³ 500 av. J.-C.: « Quoique je voie ou entende dans la société pendant l'exercice ou même hors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas », Œuvres complètes, traduction par Littré, éd. Baillière, 1844, t. 4, p. 630.

⁴⁴ Notamment, l'affaire du livre écrit par le Docteur GUBLER, *Le grand secret* : le médecin personnel de François MITTERRAND y décrit le suivi médical du président tout au long de ses mandats présidentiels. Deux jours après sa publication, *Le Grand secret* est retiré de la vente à la demande de la famille de l'ancien président. Le juge des référés estime qu'il constitue « une intrusion particulièrement grave dans l'intimité de la vie privée et familiale » du président. Le 23 octobre, le tribunal de grande instance de Paris maintient l'interdiction de vente du livre et condamne le Dr GUBLER et les éditions Plon à verser 340 000 francs de dommages et intérêts à la famille de l'ancien chef d'État. Ce jugement sera confirmé par la Cour d'appel et la Cour de cassation. En mai 2004, la Cour européenne des droits de l'homme condamne la France, estimant que l'interdiction du livre aurait dû être levée après quelques mois, au nom de la liberté d'expression. Suite à cette décision, le livre est réédité en février 2005.

de sa sphère d'intimité, inviolable. Le secret médical ayant pour fonction de protéger cette intimité, il est alors possible de le qualifier de règle protectrice de la vie privée attachés aux droits de la personnalité⁴⁵. Ce que nous confirme le Code de la santé publique en plaçant le secret médical parmi les droits de la personne⁴⁶. Ainsi, au-delà d'être une obligation pesant sur les professionnels de santé, le secret médical peut aussi être considéré comme un droit du patient. L'article L.1110-4 du Code de la santé publique semble l'instaurer en disposant que « *toute personne prise en charge par un professionnel, un établissement, 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 le concernant* ».

Elément de la protection de la vie privée, le secret médical peut également être apprécié à travers l'article 9 du Code civil qui porte sur le droit au respect de la vie privée. A ce titre, l'état de santé d'une personne est considéré comme une composante du domaine exclusif de sa vie privée. Le droit au respect du secret médical illustre le droit à la vie privée relatif aux informations médicales, personnelles et confidentielles que le professionnel de santé est amené à connaître et à collecter dans le cadre de la relation avec son patient. De ce fait, le principe du secret médical tire son origine du principe de liberté personnelle fondé sur l'article 8 de la Convention Européenne des Droits de l'Homme⁴⁷.

Le champ d'application de l'obligation de secret médical couvre l'ensemble des informations concernant la personne connues du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, par ses activités, avec ces établissements ou organismes⁴⁸.

Le secret médical va au-delà du diagnostic médical et vise notamment les rapports de filiation ou certaines infirmités découvertes, toutes les informations concernant l'état physique et mental d'une personne, y compris les données génétiques. Le médecin, tenu au secret médical en cas de diagnostic d'une anomalie génétique grave, ne pourra en informer la famille du patient sans autorisation expresse de celui-ci⁴⁹.

Le respect de cette règle du secret professionnel s'impose quel que soit le mode d'exercice de la profession: médecin libéral ou salarié, ou qu'il s'agisse également d'un médecin du service public hospitalier. De même, les praticiens-conseils et les personnels des caisses de sécurité sociale qui sont amenés à avoir connaissance d'un certain nombre de documents comportant des informations pouvant leur donner des indications sur l'état de santé de l'assuré social sont également soumis au secret professionnel⁵⁰.

Enfin, le législateur a étendu le secret médical à toutes les personnes pouvant avoir à connaître, de par leur rôle, des informations sur une personne. Cela inclut non seulement les professionnels de santé et les professionnels du système de santé, mais aussi les représentants des usages ou les bénévoles pouvant intervenir pour apporter un soutien à toute personne accueillie dans l'établissement de santé⁵¹. De surcroît, l'obligation du respect du secret médical ne cesse pas en cas de radiation du professionnel de l'ordre⁵².

⁴⁵ P. KAYSER, La protection de la vie privée, PUAM, 1995, n°212 s.

⁴⁶ Art. L.1110-4 CSP institué par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

⁴⁷ CEDH, 27 août 1997, D.2000, jurispr. p. 521, note I. Laurent-Merle.

⁴⁸ Art. L.1110-4, alinéa 2, CSP.

⁴⁹ Art. L.1131-1 du Code de la santé publique.

⁵⁰ Art. R.166-1 du code de la sécurité sociale.

⁵¹ L'article L.1112-5 rappelle que ces personnes sont tenues au secret médical.

⁵² CE, 17 juin 1998, Juris-Data n°1998-043654, RJF, 7/98, n°827.

CHAPITRE 2 UN DOSSIER MEDICAL PERSONNEL

Initialement dossier médical « partagé », le DMP est devenu un dossier médical « personnalisé », faisant du patient l'acteur principal du DMP (Section 1) ; mais cette évolution terminologique comme juridique n'est pas sans conséquences (Section 2).

SECTION 1 UN PATIENT AU CŒUR DE SON DOSSIER MEDICAL

L'accès au DMP est conditionné à l'accord de son titulaire, le patient (§1), qui bénéficie d'un certains nombre de droits à son égard (§2).

§1 LE RECUEIL DU CONSENTEMENT DU PATIENT SUR LA COLLECTE ET LE PARTAGE DE SES DONNÉES MÉDICALES

Seuls les professionnels dûment autorisés par le patient peuvent accéder au DMP (A) mais ils n'ont pas pour autant accès à toutes les informations contenues sur le DMP (B).

A. UN FREIN À L'ACCÈS AU DOSSIER MEDICAL PERSONNEL

L'article L.1110-4 du Code de la santé publique⁵³, repris dans les mêmes termes à l'article L.161-36-1 A du Code de la sécurité sociale, exige expressément le recueil du consentement de la personne concernée pour l'échange entre deux ou plusieurs professionnels de santé d'informations relatives à la même personne⁵⁴. Pour autant, le consentement exprès du patient n'est pas requis lorsque l'accès aux systèmes de données est réservé au professionnel ou à l'établissement de santé qui y a lui-même déposé ces données, et au patient concerné⁵⁵. On veut éviter ici que le médecin qui a confié ses données à un hébergeur soit obligé de requérir le consentement du patient pour consulter les données qu'il a lui-même

⁵³Art. L.1110-4, C. Sant. Publ. : « Toute personne prise en charge par un professionnel, un établissement, 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 le concernant ».

⁵⁴Il existe une exception à ce principe en cas d'hospitalisation, « 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 toute l'équipe ». Dans ce cas, la règle du secret s'impose à tous les membres de l'équipe.

⁵⁵C. sant. publ., article L.1111-8, alinéa 5 nouveau.

déposées.

Ces dispositions résultent de la nécessité de préciser les modalités d'application de la règle du consentement à la communication des données imposées par le DMP.

Dans son avis du 12 juillet 2004⁵⁶, la Cnil a notamment rappeler que compte tenu de la nature des données de santé, relevant de l'intimité de la vie privée, l'accord de la personne au partage des données médicales, en premier lieu, est nécessaire. En outre, dès lors qu'il s'agit d'informations médicales, et en vertu du principe de confidentialité qui leur est applicable, la mise en ligne est subordonnée au consentement du patient.

En application de ces règles, la création du DMP et tout accès à celui-ci reposent sur le consentement exprès du patient. Ainsi, il doit consentir à chaque fois qu'un professionnel de santé demande accès à son DMP et à l'alimentation de celui-ci; il a la possibilité de contrôler à tout moment les accès aux informations de son dossier. En outre, il contrôle le contenu du DMP en ce sens qu'il décide ce qui peut y être déposé ou non.

Cette liberté de consentir ou non paraît bien atténuée à l'occasion de la décision de l'ouverture d'un dossier médical personnel. En effet, la loi a prévu que seuls les patients procédant à l'ouverture de leur dossier médical personnel se verraient octroyer un meilleur remboursement⁵⁷. Cette pratique n'est pas nouvelle; elle existe déjà au niveau du parcours des soins et prévoit que seuls les patients ayant déclaré à la sécurité sociale un médecin comme leur médecin traitant sont mieux remboursés⁵⁸.

Peut-on considérer que le consentement de la personne est réellement libre dès lors que le projet créant le DMP lie le niveau de remboursement à l'accès au DMP ?

La Cnil s'est prononcée sur cette situation, qui peut paraître surprenante, et a estimé que :

« les dispositions du projet de loi instituant le dossier médical personnel et liant le niveau de remboursement des soins à l'accès du professionnel de santé à ce dossier sont justifiées par un motif d'intérêt public important qui est [...] la coordination, la qualité et la continuité des soins et l'amélioration de la pertinence du recours au système de soins, l'ensemble du projet de loi visant à sauvegarder l'assurance maladie »⁵⁹.

Le Conseil constitutionnel a également validé le dispositif⁶⁰, estimant que le législateur avait opéré une « conciliation non déséquilibrée » entre les diverses exigences constitutionnelles : d'une part les exigences relatives à la garantie de la protection de la santé ainsi qu'au respect de la vie privée et du secret des informations de santé à caractère personnel et d'autre part, celles qui s'attachent à l'équilibre financier de la sécurité sociale qu'a introduites la révision

⁵⁶ Cnil, avis sur le dossier médical personnel, 12 juillet 2004,

[http://www.cnil.fr/index.php?id=1613&news\[uid\]=178&cHash=844a59142b](http://www.cnil.fr/index.php?id=1613&news[uid]=178&cHash=844a59142b).

⁵⁷ C. Séc. Soc., article L.161-36-2, alinéa 2. Le 3^e alinéa du même article prévoit également que pour les professionnels de santé, l'usage du DMP des patients, conditionne leur conventionnement avec l'Assurance maladie.

⁵⁸ Le « parcours de soins coordonnés » a été créé en France par la loi du 13 août 2004 qui a réformé l'Assurance maladie. Il vise à mieux coordonner les soins et à éviter les gaspillages. Il repose sur le choix d'un médecin traitant qui permet d'entrer dans ce parcours de soins. Ce système s'applique à tous les assurés sociaux et prévoit des pénalités en cas de non respect (remboursement des dépenses de santé moins élevé par majoration du ticket modérateur, la part des frais non remboursée par la Sécurité sociale).

⁵⁹ Cnil, avis sur le dossier médical personnel, 12 juillet 2004,

[http://www.cnil.fr/index.php?id=1613&news\[uid\]=178&cHash=844a59142b](http://www.cnil.fr/index.php?id=1613&news[uid]=178&cHash=844a59142b).

⁶⁰ Conseil Constitutionnel, Décision n° 2004-504 DC, du 12 août 2004 sur la loi du 13 août 2004 relative à l'assurance maladie, accessible sur <http://www.conseil-constitutionnel.fr/decision/2004/2004504/index.htm> au 15 juillet 2008.

constitutionnelle du 22 février 1996 en inscrivant les lois de financement de la sécurité sociale dans l'article 34 de la Constitution.

B. LE DROIT AU « MASQUAGE » DES INFORMATIONS MÉDICALES

Selon la même logique, le patient peut décider de « masquer » telle ou telle information inscrite dans son dossier médical personnel, à tel ou tel professionnel de santé autorisé à accéder à son dossier. Ce droit au « masquage » est la conséquence du principe du respect de la vie privée et la traduction informatique du droit du malade de ne pas tout dire à son médecin.

Ce droit au « masquage » a fait débat, notamment lors de la discussion du projet de loi de financement de la sécurité sociale pour 2008.

Au départ, un simple décret⁶¹, devait prévoir cette faculté. Mais on y a préféré une loi. L'article 55 de la loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008⁶² a ainsi introduit dans l'alinéa 1 de l'article L. 161-36-4 de la sécurité sociale, le principe selon lequel « *Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé fixe [...] les conditions dans lesquelles certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical personnel ou son représentant légal ainsi que les modalités selon lesquelles le professionnel de santé accédant au dossier médical personnel a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal* ».

Cet article prévoit également la possibilité pour le médecin de savoir si le DMP consulté est incomplet, autrement dit contenant des informations masquées par son titulaire.

La question du droit au masquage ne fait pas l'unanimité auprès du corps médical craignant de ne pas avoir accès à des données médicales pertinentes nécessaires au diagnostic. A travers l'article 55, le législateur ne les apaise que partiellement, car les modalités de la mise à disposition des médecins des indications associées à la traçabilité du masquage ne seront fixées que par décret. D'autant plus que la ministre de la santé, Roselyne BACHELOT, a indiqué que le décret ne serait pris qu'à la suite de la saisie du Comité consultatif national d'éthique pour les sciences de la vie et de la santé de cette question éthique. Celui vient de rendre son avis, le 29 mai dernier⁶³. Ainsi, en réponse à la question de Monsieur Jean-Pierre DOOR, rapporteur pour l'assurance maladie et les accidents du travail, la ministre de la santé, relative au calendrier de relance du DMP et à la publication du décret prévu par l'article 55, Madame la ministre est sereine :

« *Après un audit ayant démontré la nécessité de le conserver tout en changeant*

⁶¹Le décret d'application de la loi du 13 août 2004 relative à l'assurance maladie.

⁶²Loi n°2007-1786 de financement de la sécurité sociale pour 2008, du 19 décembre 2007, JORF n°0296, 21 déc., page 20603, texte n° 1.

⁶³CCNE, avis n°104 Le « dossier médical personnel » et l'informatisation des données de santé.
<http://www.ccne-ethique.fr>.

d'approche, j'ai mandaté un groupe d'experts afin de définir un plan de relance. Le rapport qui m'a été remis est excellent, quant au diagnostic comme aux préconisations. Je vais donc prochainement relancer le DMP sur la base de grandes orientations stratégiques en vue de sa généralisation progressive en 2012. Je rappelle toutefois que l'article 55 de la loi de financement de la sécurité sociale pour 2008 sur le DMP garde toute sa pertinence : le portail de confiance pour l'accès au DMP est conservé, de même que le droit de masquage. Nous pourrions également avancer s'agissant de l'arrêté prévu par cet article concernant les conditions de mise à disposition des fonctions de ce portail de confiance pour d'autres réseaux de santé. Un décret sur le DMP sera par ailleurs soumis à concertation avant d'être transmis au Conseil d'État. »⁶⁴

§2 LES DROITS DU PATIENT À L'ÉGARD DU DOSSIER MÉDICAL ÉLECTRONIQUE

La nature des droits du patient à l'égard de son dossier médical n'a pas changé (A) mais d'autres s'y rajoutent (B).

A. DES DROITS ÉQUIVALENTS À CEUX EXISTANT POUR LE DOSSIER MÉDICAL VERSION PAPIER

Dès à présent, il faut souligner que les droits du patient à l'égard de son dossier médical sont les mêmes, que celui-ci soit sous en version papier ou électronique. En effet, l'informatisation et la dématérialisation d'un dossier ne modifie en rien les obligations légales qui résultent de son caractère médical. La dématérialisation du dossier médical ne lui fait pas perdre sa valeur de fichier à caractère nominatif contenant des données de santé personnelles. A ce titre, le dossier médical dématérialisé est toujours passible de la loi « Informatique et Libertés » de 1978.

On peut dès lors faire état des droits accordés au patient vis-à-vis de son dossier médical électronique :

- le droit à l'information du patient ;
- le droit à la communication du contenu du dossier médical informatisé;
- le droit à la confidentialité des informations portées au dossier informatisé ;

⁶⁴ Commission des affaires culturelles, familiales et sociales de l'Assemblée nationale, Compte rendu n°48 du Mardi 17 juin 2008, Séance de 17 heures.

<http://www.assemblee-nationale.fr/13/cr-cafc/07-08/c0708048.asp>

- la définition du contenu du dossier médical permettant d'apprécier la qualité de sa tenue (Art R 1112-2 du Code de la santé publique) ;
- un droit à la conservation des informations par le gestionnaire du dossier médical pendant une durée définie par la loi (Art R 1112-7 et R 1112-9 du Code de la santé publique) ;
- un droit de rectification des informations contenues dans le dossier, résultant de l'article 40 de la loi « Informatique et Liberté ».

On peut s'interroger sur la propriété des informations portées dans le dossier médical, papier ou électronique. Le patient est-il propriétaire des informations contenues dans son dossier médical ou, résultant de son travail intellectuel, appartiennent-elles au médecin ? Cette question se pose d'autant plus que les données de santé ont une valeur économique non négligeable et suscitent un fort intérêt pour les laboratoires pharmaceutiques ainsi que les sociétés d'assurance. Cette possibilité de monnayer ses données personnelles de santé a été prohibée par le législateur français contrairement aux lois en vigueur aux Etats-Unis. Les données de santé des patients ont également une valeur économique pour les médecins eux-mêmes. Ces derniers, en détenant l'histoire médicale de leurs patients, peuvent les empêcher de changer de médecin traitant. De ce fait, la loi doit aménager la possibilité de transmettre un dossier médical d'un médecin à un autre, selon la volonté du patient.

La loi ne se positionne pas sur la question de la propriété du dossier médical mais elle assure au patient la maîtrise de son dossier, comme s'il en était propriétaire, en précisant le contenu et la procédure de communication des pièces du dossier médical. Autrement dit, on peut considérer que le patient est propriétaire du contenu du DMP, les informations du dossier médicales, alors que le médecin reste maître de la gestion du contenant, le support du dossier médical lui-même.

B. LES DROITS DU PATIENT SPECIFIQUES AU DMP

La loi du 13 août 2004 relative à l'assurance maladie, qui crée le DMP, n'a pas révolutionné la législation relative aux dossiers médicaux, papiers ou électroniques. Concernant la propriété du dossier médical, la situation reste inchangée : le dossier médical est mis à la disposition de l'utilisateur⁶⁵. Comme tous les dossiers médicaux, le patient a la maîtrise des informations de santé qui le concernent.

⁶⁵C. Séc. Soc., art. L.161-36-1 : « 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. »

Mais compte tenu de sa nature électronique, le dossier médical personnel comporte des particularités :

- L'accès à l'information est immédiat dans le cadre du DMP, lorsque pour les dossiers version papier le délai de transmission est de deux jours minimum et huit jours maximum à compter de la demande ;
- Contrairement à tout dossier médical, le DMP n'est pas détenu par un professionnel de santé, mais par un organisme agréé par l'État ;
- L'Etat est également gestionnaire du DMP et en définit l'organisation ;
- Le DMP permet un droit au masquage par le patient de certaines informations y contenues.

S'il est une différence vis-à-vis des autres dossiers médicaux, il s'agit du droit octroyé au patient de masquer des informations contenues dans le DMP. En effet, ce droit rompt avec les dispositions de l'article 40 de la loi « Informatique et Libertés » relatif au droit de rectification. Généralement, la Cnil ne permettait pas à un patient de demander à son médecin l'effacement de données qui ne seraient ni inexactes, ni incomplètes, ni équivoques ou périmées, sans motifs légitimes de sa part. Avec le droit au masquage, le législateur satisfait la demande des patients qui souhaite contrôler le contenu de leur dossier médical et la connaissance qu'en ont les différents médecins consultés.

SECTION 2. LE PASSAGE D'UN DOSSIER « PARTAGE » A UN DOSSIER « PERSONNALISÉ »

D'un dossier médical « partagé » à usage des professionnels de santé, y succède un dossier médical « personnalisé », avec pour conséquences le changement de son régime juridique (§1) et la nécessité d'en revoir les contraintes techniques (§2).

§1 DES CONSÉQUENCES JURIDIQUES

Deux catégories de conséquences peuvent être observées : celles relatives au régime juridique du DMP (A) et celles relatives à sa finalité (B).

A. QUANTAUREGIMEJURIDIQUEDUDOSSIERMEDICAL PERSONNEL

Lors de l'élaboration du dossier médical personnel, objet de cette étude, rien ne laissait présager qu'il deviendrait un dossier à l'usage des patients. Ainsi, le Professeur M. Fieschi, dans le cadre de la mission de réflexion sur le DMP⁶⁶ qui lui a été confié, le considérait comme un dossier patient partagé à l'usage principal des professionnels de santé. Mais la loi du 13 août 2004 relative à l'assurance maladie crée un « dossier médical personnel », détenu par l'assuré social, au lieu d'un simple dossier médical dématérialisé.

S'il faut rechercher les causes de cette évolution, ce sera sans doute dans la loi du 4 mars 2002, relative aux droits des malades et à la qualité du système de santé⁶⁷. En effet, l'article 11⁶⁸ de la loi définit les principes et les règles régissant les droits des patients à l'égard de leur santé :

- « droit d'être informé sur son état de santé » et sur la nature, les conséquences et les risques des « investigations, traitements ou actions de prévention qui lui sont proposés » ;
- droit de prendre en toute connaissance de cause les « décisions relatives à leur santé » ;
- droit d'« accès à l'ensemble des informations détenues par des professionnels et des établissements de santé, qui sont formalisées... ou ont fait l'objet d'échanges écrits entre professionnels de santé » ;
- droit de subordonner à son consentement exprès le dépôt (l'hébergement) de données de santé qui le concernent auprès d'une « personne ou un organisme agréé à cet effet ».

Nous pouvons trouver un élément de réponse dans les propos des services du ministère de la santé qui expliquent cette évolution comme résultant d'une *simple* « décision politique ». Le passage d'un outil au service des professionnels de santé à un dossier mis à disposition du patient et centré sur ses droits individuels (d'accès, de consultation, de communication, etc.), ont modifié la nature et l'usage de ce dossier attendu par les professionnels de santé.

⁶⁶ « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », Rapport au ministre de la Santé, de la Famille et des Personnes handicapées, M. FIESCHI, janvier 2003. Professeur de Santé publique à la faculté de médecine de Marseille.

⁶⁷ Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JO du 5 mars, p.4118, texte n°1.

⁶⁸ Codifiés aux articles L.1111-1 à L.1111-9 du Code de la santé publique

B. QUANT A LA FINALITE DU DOSSIER MEDICAL PERSONNEL

Bien que la France soit de loin le premier pays à mettre en place un dossier médical informatisé, le choix politique, et donc stratégique, de faire bénéficier tout assuré social d'un tel dossier unique, la place dans une situation originale et fait peut être d'elle un précurseur. Chacun est conscient que tout projet unique, innovant juridiquement et techniquement, porte en son sein toute une série de complications, dont certaines sont imprévues ou n'ont pas été anticipées. La mise en œuvre du DMP a elle aussi pâti de ces difficultés entraînant ainsi des retards en cascade jusqu'au report de la date de lancement du DMP.

Choix politique qu'est le glissement de la notion de dossier médical partagé à celle de dossier médical personnel ; mais choix politique prématuré sans doute, tant les conséquences d'un tel changement n'ont pas été mesurées ni même anticipées. Faire du patient le principal acteur du DMP doublé d'une mise en réseau sur Internet a contraint à accroître le niveau de sécurité par rapport au projet initial. Ce qui n'est pas sans inconvénients. A titre d'exemple :

- *Le contenu du dossier* : rassembler la totalité des données de santé d'un individu dans un dossier unique pose, en termes de libertés publiques et de sécurité, des risques considérables dont la prise en compte ne cesse de compliquer le projet et d'en retarder la mise en œuvre. On l'a vu à propos du choix de l'identifiant de santé pour le DMP mais aussi pour les processus d'authentification, d'identification, de transmission et d'hébergement des données de santé.
- *La finalité du DMP* : selon l'article L.161-36-1 du Code de la sécurité sociale, le dossier médical vise à « favoriser la coordination, la qualité et la continuité des soins ». Ces objectifs ne peuvent être atteints sans la mise en place de protocoles et de systèmes d'information permettant aux professionnels de santé d'échanger et de mettre en commun des informations sélectionnées et formatées pour faciliter leur exercice professionnel et améliorer la qualité de la prise en charge du patient.

Or, le dispositif actuel du DMP fait du patient le seul titulaire de son dossier médical « personnel », inévitablement le régime de celui-ci est modifié :

- Seul le patient a la responsabilité d'ouvrir son DMP ;
- Le patient a le droit de choisir le contenu de son DMP : il peut s'opposer au report dans son dossier d'informations nécessaires à sa bonne prise en charge, et peut rendre invisible sa décision de masquer des informations (le « droit au masquage du masquage ») ;
- Le patient choisit les destinataires de son DMP : il peut rendre son dossier inaccessible à certains professionnels de santé ;
- Le patient choisit l'organisme assurant l'hébergement de son dossier ;

Au vu de ces éléments, la question de la finalité du DMP est incontournable. Comment fournir aux professionnels de santé un outil efficace pour améliorer le partage et la circulation

des informations médicales utiles à la coordination et à la qualité des soins, et garantir au patient sa maîtrise sur le contenu et la gestion de son dossier médical ?

§2 DES CONSEQUENCES TECHNIQUES

Le passage d'un outil au service des professionnels de santé à un outil au service du patient, a eu pour conséquence la centralisation du DMP sur le réseau Internet dans un souci d'accessibilité. Mais cela a dû contraindre à renforcer la sécurité entourant le DMP (A), notamment par la mise en place d'un « tiers de confiance » (B).

A. UN NECESSAIRE RENFORCEMENT DE LA SECURITE

Le passage à un « dossier médical personnel » a pour conséquence le recours au réseau Internet et à une base de données centralisée pour en faciliter l'accès. Ce qui n'a pas manqué d'inquiéter la Cnil sur le niveau de sécurité requis dans un tel cas.

Ainsi, dans un avis du 12 juillet 2004, la Cnil indique que le fait de « *recourir au réseau internet pour permettre l'accès au DMP, compte tenu des risques de divulgation, ne pourrait être admis que dans la mesure où des normes de sécurité extrêmement strictes sont imposées* »⁶⁹. La Cnil estime que la sécurité doit être assurée par l'utilisation de la carte CPS (Carte de professionnel santé) pour les professionnels de santé et par celle de la carte Vitale 2 pour les patients. Il faut souligner la dissymétrie des exigences de sécurité dans le cas de la consultation du DMP par un professionnel de santé en présence du patient et dans le cas de la consultation directe par le patient, en dehors de la présence d'un médecin et hors du cabinet médical.

La Cnil estime également que, conformément à l'article 8 de la directive européenne du 24 octobre 1995⁷⁰, le dispositif juridique relatif au DMP devrait être complété par la mention selon laquelle les données susceptibles d'être contenues dans le DMP sont couvertes par le secret professionnel et que quiconque aura obtenu ou tenté d'en obtenir la communication en violation de cette obligation s'exposera à des sanctions pénales, de même que quiconque aura modifié ou tenté de modifier les informations portées sur ce même dossier.

Le CCNE⁷¹ a également jugé que la mise sur le réseau Internet du DMP accroissait le sentiment d'insécurité tant des patients que des professionnels de santé à l'égard de leurs données personnels. Pour cela, il part du constat que l'histoire des systèmes de communication informatique démontre, que malgré les précautions prises par les concepteurs de programmes, des possibilités de subtilisation de données confidentielles existent. Le CCNE se base également sur les conséquences de l'utilisation de l'outil informatique qui peut permettre de démultiplier les possibilités de transmission des informations. Ainsi, il en résulte

⁶⁹ Cnil, avis sur le dossier médical personnel, 12 juillet 2004, [http://www.cnil.fr/index.php?id=1613&news\[uid\]=178&cHash=844a59142b](http://www.cnil.fr/index.php?id=1613&news[uid]=178&cHash=844a59142b).

⁷⁰ L'article 8 prévoit que la possibilité de dérogation est subordonnée à l'introduction de garanties appropriées.

⁷¹ CCNE, avis n°104 Le « dossier médical personnel » et l'informatisation des données de santé. <http://www.ccne-ethique.fr/>.

la crainte que données personnelles de santé puissent être récupérées, *via* l'internet, notamment par des assureurs ou des employeurs potentiels.

Enfin, l'utilisation de l'outil informatique en lui-même ou par des personnes non expérimentées peut conduire à des situations anxiogène : peur de l'oubli du mot de passe, changement de clé, panne, pertes ou altérations des données, complexité d'utilisation et du jargon informatique, ...).

B. LE PORTAL UNIQUE D'ACCÈS AU DOSSIER MÉDICAL PERSONNEL : LA « CONFIANCE NUMÉRIQUE »

La mise sur le réseau Internet du DMP, nécessité par l'accès des patients à leur dossier médical de tous endroits, a conduit à la mise en place d'un portail unique d'accès au DMP auquel se connectent les patients ainsi que les professionnels de santé.

L'article 55 de la loi de financement de la sécurité sociale pour 2008⁷² introduit l'article L. 161-36-3-1 dans le Code de la sécurité sociale qui institue « [...] *un service unique d'accueil dématérialisé, dénommé portail du dossier médical personnel* », destiné aux bénéficiaires de l'assurance maladie et aux professionnels de santé.

« Ce portail assure des fonctions d'information générale et un service de gestion permettant aux bénéficiaires de l'assurance maladie de gérer leur dossier médical personnel et les droits d'accès des professionnels de santé. Il assure le contrôle et la traçabilité des accès aux dossiers médicaux personnels. Il produit les données de suivi d'activité nécessaires à l'évaluation de ce service. »

La gestion de ce portail, appelé aussi « tiers de confiance », a été confié à la Caisse des dépôts et consignations (CDC), laquelle est déjà présente au sein du conseil d'administration du GIP-DMP.

Ce « tiers de confiance » a pour objectif de rassurer les titulaires du DMP, inquiets des possibles failles du système sur la sécurité, la confidentialité et l'intégrité des données. C'est par le biais de ce portail que les usagers du DMP s'authentifieront et seules les personnes habilitées pourront accéder à un DMP donné.

Selon la loi, ce portail ne sera pas spécifique du DMP car il devrait également offrir ses services à « *d'autres organismes assurant des missions de partage et d'échange de données personnelles de santé* ». Le DMP ne sera pas le seul dossier dématérialisé à bénéficier du portail unique d'accès. D'autres dossiers médicaux ont vocation à l'utiliser tels que le dossier communiquant de cancérologie (DCC), le dossier pharmaceutique (DP) ou les dossiers de réseaux de santé.

Le portail unique d'accès va établir quatre niveaux de confiance :

- Une confiance dans l'identité des personnes, en permettant de savoir « qui est qui » ;

⁷² Loi n°2007-1786 de financement de la sécurité sociale pour 2008, du 19 décembre 2007, JORF n°0296, 21 déc., page 20603, texte n° 1.

- Une confiance dans la qualification des personnes, en permettant de reconnaître les rôles et les habilitations de chacun ;
- Une confiance quant au contenu et à son utilisation, en assurant l'intégrité et la qualité de l'information.
- Un espace de confiance, en assurant son inviolabilité.

La mise en œuvre de cet espace de confiance nécessite l'existence d'une autorité de certification, capable d'assurer l'identité de tous les acteurs du DMP. La fonction d'autorité de certification spécifique au secteur de la santé est assurée par le GIP-CPS (Groupement d'intérêt public – Carte de Professionnel de Santé) depuis 1993. Afin de mener sa mission de tiers certificateur, le GIP-CPS offre plusieurs services :

- Un service d'enregistrement (SE), afin de garantir l'identité et la profession ;
- Un service de certification (SC) : il fabrique et distribue des certificats électroniques :
 - Des certificats individuels assurant l'authentification, le chiffrement et la signature :
 - Des certificats localisés sur un support sécurisé (la CPS) protégé par code porteur pour s'authentifier et signer ;
 - Des certificats dits de confidentialité pour chiffrer ;
 - Des certificats serveurs applicatifs (CSA) pour sécuriser les flux échangés avec l'extérieur. Ils représentent la « carte d'identité » de la structure juridique sur Internet. Deux catégories de CSA existent : les « SSL » (Secure Socket Layer) et les « SMIME » qui permettent d'authentifier, signer et chiffrer un nom de domaine, une application et une adresse mail.
- Un service de publication (SP) : pour permettre la mise à jour des certificats, il publie les certificats et les listes de révocations dans un annuaire public sur Internet.

Initialement, le dossier médical personnel a été créé pour l'usage des professionnels de santé afin d'assurer une meilleure continuité, coordination des soins et d'améliorer les techniques médicales. Pour autant, d'un dossier médical « partagé », nous sommes passés à un dossier médical « personnalisé », au cœur duquel se trouve le patient.

En raison de son contenu, le dossier médical personnel est soumis à l'ensemble de la réglementation relative à la protection des données à caractère personnel. Ce qui implique l'application de toute une série de mesures de sécurité vis-à-vis des données que contient le DMP. Ainsi, le consentement du patient est la condition *sine qua non* de l'accès des professionnels de santé au DMP.

Par ailleurs, les droits du patient sont quelques peu renforcés à l'égard du dossier médical personnel. En effet, le patient dispose du droit de masquer les informations qu'il souhaite. Dès lors, on peut s'interroger sur l'adéquation de ce droit offert au patient et les objectifs poursuivis par le DMP comme l'amélioration de la prise en charge du patient.

Evidemment, cette évolution tant terminologique que juridique, a eu pour conséquences un changement du régime juridique du DMP mais aussi de sa finalité. Mais aussi, ce changement a un impact en termes de contraintes techniques. En effet, dès lors que le DMP est accessible à partir d'un réseau centralisé sur Internet, les risques de violation de la protection des données se sont accrus. Dès lors, il est nécessaire de faire des choix techniques stricts et d'établir une relation de confiance avec les patients mais les professionnels de santé.

C'est pour toutes ces raisons que le DMP, d'un projet ambitieux est devenu un projet d'une très grande complexité. Celle-ci s'apprécie à travers les difficultés structurelles rencontrées mais aussi des mesures techniques à mettre en place.

PARTE 2

UN PROJET COMPLEXE

CHAPITRE 1 DES CONTRAINTES STRUCTURELLES

Alors que son lancement généralisé était prévu pour le 1^{er} juillet 2007, le service DMP a connu de très gros retards dans sa mise en œuvre. Ces retards sont le résultat de la précipitation des pouvoirs publics dans cette entreprise et du manque d'expérience de conduite d'un tel projet (Section 1).

En outre, le dispositif du DMP bouleverse la relation patient – professionnel de santé en s'immiscant au cœur de ce couple si particulier, dont la confiance repose sur le respect du secret médical (Section 2).

SECTION 1 UNE MISE EN ŒUVRE MALAISEE

La mise en œuvre du DMP a souffert de nombreux retards (§1) mais aussi de l'absence de résolution de questions majeures (§2).

§1 DES RETARDS RECURRENTS

L'instabilité managériale du GIP-DMP n'a pas permis que soit menée une stratégie de développement du DMP efficace (A); d'autant plus, en présence d'un cadre législatif inachevé (B).

A. L'INSTABILITE DE LA GOUVERNANCE

Les retards entrepris lors de la mise en œuvre du DMP résultent principalement de l'impuissance du GIP-DMP à élaborer une stratégie de développement viable. En effet, l'action du GIP-DMP, dès l'origine, a été bridée par un manque de moyens considérables comparativement aux enjeux de la création du DMP.

Ainsi, en France, le coût global du DMP annoncé est de 1,1 milliard d'euros sur cinq ans, quand le Canada y consacre 6,6 milliards d'euros, l'Angleterre 14 milliards et l'Allemagne 4 milliards⁷³.

Outre les moyens du GIP-DMP qui sont à déplorer, celui-ci a également pâti d'une instabilité managériale, voyant se succéder pas moins de trois directeurs durant ses deux premières années d'existence.

Aujourd'hui, le GIP-DMP a fait peau neuve et est désormais composé d'une soixantaine de personnes, organisé autour d'un conseil d'administration de onze membres. Il s'est également

⁷³BioSanté – Eurasanté, Information mensuelle sur les marchés de la bio-santé, n°12, Février 2008.

doté d'un comité d'orientation (COR) associant les représentants des patients et ceux des professionnels de santé, lesquels comptent pour plus de la moitié de ses quatre-vingt membres. Le GIP-DMP s'appuie sur une méthode de concertation en impliquant l'ensemble des acteurs du DMP à la prise de décision.

Pour autant la comparaison fait mal : le « NHS Connecting for Health », considéré comme l'équivalent du GIP-DMP outre Manche, compte près de 600 employés.

L'IGAS (Inspection Générale des Affaires Sociales) a fait un constat implacable dans son rapport sur le Dossier Médical Personnel, remis le 8 novembre dernier à la Ministre de la Santé. Selon l'IGAS, le calendrier et les moyens, dans lesquels était enserré le GIP-DMP, étaient irréalistes. Alors que d'autres pays ont planifié la mise en place du DMP sur une période de dix ans, la France avait prévu d'y parvenir en l'espace de trois ans !

« Notre pays serait ainsi en mesure de mettre en œuvre un projet d'une telle complexité en trois fois moins de temps et avec trois à dix fois moins d'argent qu'il en faut aux autres pays engagés dans une entreprise similaire »⁷⁴.

Afin de faire face à ces difficultés, qui participent de la faiblesse du projet, la Ministre de la Santé a mis en place une nouvelle équipe au sein du GIP-DMP. Cette nouvelle équipe est dotée de l'expérience nécessaire à la relance « ambitieuse et pragmatique » du DMP, selon la Ministre. Laquelle préfère, désormais, avancer sans précipitation, en « se donnant le temps de réussir ». Ainsi, aucune nouvelle date de lancement du DMP n'est prévue à ce jour, même si la Ministre espère pouvoir le généraliser en 2012⁷⁵.

B. UN CADRE LEGISLATIF INCOMPLET

L'instabilité du GIP-DMP n'est pas la seule cause des retards pris pour le lancement du DMP. En effet, le calendrier prévoyant une mise en place du DMP sur une période de trois ans, la phase expérimentale devait être conduite dans les plus brefs délais. Le GIP-DMP a donc lancé un appel d'offres en juillet 2005, dont les réponses sont parvenues au mois de septembre de la même année. Des conventions d'expérimentations ont alors été signées avec les industriels le 22 décembre 2005.

Pour autant, les expérimentations n'ont pas pu débuter dès cette date, en raison de l'absence de publication des décrets d'application de la loi du 4 mars 2002 relative aux droits des malades. La publication de ces décrets étant indispensable pour la mise en œuvre des expérimentations, car ils constituent le socle juridique de l'activité d'hébergeur et fixent les modalités de la protection et de la confidentialité des données médicales personnelles.

Manquaient ainsi les décrets suivants :

- Le décret en Conseil d'Etat, dit « hébergeur », pris après avis de la Cnil et des

⁷⁴ Rapport sur le dossier médical personnalisé (DMP), Mission Interministérielle de revue de projet sur le DMP réunissant l'Inspection Générale des Finances, l'Inspection Générale des Affaires Sociales, le Conseil Général des Technologies de l'Information, déposé en novembre 2007.

⁷⁵ Commission des affaires culturelles, familiales et sociales de l'Assemblée nationale, Compte rendu n°48 du Mardi 17 juin 2008, Séance de 17 heures.

<http://www.assemblee-nationale.fr/13/cr-cafc/07-08/c0708048.asp>

conseils de l'ordre des professions de santé, prévu au troisième alinéa de l'article L. 1111-8 du code de la santé publique, qui devait définir les conditions d'agrément des hébergeurs de données de santé à caractère personnel.

- Le décret en Conseil d'état, dit « confidentialité », pris après avis de la Cnil, prévu par l'alinéa 4 de l'article L. 1110-4 du code de la santé publique relatif à la confidentialité des informations médicales à caractère personnel.

Le décret dit « hébergeur » a été pris le 4 janvier 2006⁷⁶ en tenant compte des avis de la Cnil rendus les 27 mai 2004 et 15 mars 2005. Le décret précise les modalités de l'agrément des hébergeurs d'informations de santé, délivré par le ministre de la santé qui se prononce après les avis de la Cnil et d'un comité d'agrément créé auprès de lui. Les délais nécessaires à la mise en place de ce comité et à l'obtention, même rapide, de l'avis de la Cnil⁷⁷ sur les soumissionnaires retenus par le GIP ont retardé la publication de l'arrêté ministériel d'agrément jusqu'au 29 mai 2006.

Ensuite, le décret relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique, a été pris le 15 mai 2007⁷⁸ et codifié aux articles R. 1110-1 à R. 1110-3 du code de la santé publique.

Non publié à l'époque des expérimentations, la Cnil a admis que des clauses provisoires relatives à la confidentialité soient prévues dans les conventions entre le GIP-DMP et les industriels retenus à l'issue de l'appel d'offres. Lors de son examen des conventions, elle a souhaité en renforcer la rigueur par rapport aux propositions initiales des industriels. Elle a également souhaité que ces modalités provisoires ne s'appliquent pas au-delà du terme fixé aux expérimentations.

Sur ces bases, la Cnil a donné le 30 mai 2006 un avis favorable aux applications informatiques nécessaires aux expérimentations du DMP⁷⁹. Les contrats initiaux signés avec les hébergeurs ont fait l'objet de plusieurs avenants, notamment pour prolonger la durée des expérimentations et introduire des clauses nouvelles conformes au décret « hébergeur » du 4 janvier 2006. Malgré tout, les expérimentations ont eu lieu du 1^{er} juin 2006 au 31 décembre 2006, une durée unanimement jugée trop courte, d'autant que les six mois n'ont pas pu être effectivement utilisés.

⁷⁶ Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JO n°4, 5 janv., p.174, texte n°14.

⁷⁷ Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel, accessible sur www.cnil.fr

⁷⁸ Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), JO n°113, 16 mai, p.9362, texte n°210.

⁷⁹ Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel.

§2 DES QUESTIONS EN SUSPENS

On est toujours en attente de la publication du décret « identifiant de santé » (A) ainsi que des référentiels d'interopérabilité (B).

A. LE CHOIX D'UN NUMÉRO D'IDENTIFICATION DE SANTÉ (NIS)

L'ouverture, l'accès et la tenue du dossier médical personnel sont soumis à l'identification du patient. Afin de déterminer cet identifiant de santé, l'article 5 de la loi du 13 août 2004⁸⁰, résultant d'un amendement du gouvernement, prévoit qu'« *un décret en Conseil d'État, pris après avis de la Cnil, détermine les conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et pour la tenue du dossier médical personnel tel que défini à l'article L. 161-36-1 du code de la sécurité sociale, dans l'intérêt de la personne concernée et à des fins exclusives de coordination des soins* ».

Lors de la défense de cet amendement, Monsieur Jean DIONIS du SEJOUR a invoqué devant l'Assemblée nationale que « *Le dossier médical personnel exige une identification personnelle : un DMP pour chaque personne, chaque personne n'ayant qu'un seul dossier. Il faut donc construire un identifiant, c'est-à-dire un ensemble d'informations qui garantisse à la fois l'unicité de ce dossier et son invariabilité dans le temps* »⁸¹.

Le gouvernement a fait le choix du NIR⁸² (numéro d'inscription au répertoire national d'identification des personnes physiques) comme identifiant de santé et a chargé la Cnil d'en autoriser l'usage afin d'identifier un patient à son DMP. Il est également prévu d'étendre cette application à l'ensemble des dossiers de santé informatisés.

Il faut rappeler qu'en cas d'utilisation du NIR, la loi « Informatique et Libertés » exige une autorisation par décret en Conseil d'Etat, pris après avis motivé et publié de la Cnil, laquelle veille à éviter tout risque d'interconnexions de fichiers.

La Cnil s'étant à plusieurs reprises opposée à l'utilisation du NIR, fut évoquée l'idée d'utiliser un numéro d'identification de santé (NIS) dérivé du NIR et construit à partir d'un algorithme, sans possibilité de remonter au NIR. D'aucuns ont relevé que cette solution aurait l'inconvénient de faire perdre beaucoup de temps et d'argent, la création du NIS emportant création d'un répertoire national ; l'échéance du 1er juillet 2007 fixée par la loi pour le lancement du DMP n'étant alors pas tenue.

⁸⁰ L'article 5 de la loi du 13 août 2004 a ensuite été abrogé par l'article 25 de la loi n°2007-127 du 30 janvier 2007.

⁸¹ **DIONIS DU SEJOUR Jean, ETIENNE Jean-claude.** *Nouvelles technologies de l'information et système de santé : la nouvelle révolution médicale*, rapport n°1686 Assemblée nationale- n°370, tome I, office parlementaire d'évaluation des choix scientifiques et technologiques.

⁸² Numéro utilisé par la sécurité sociale et le fisc et communément appelé le numéro INSEE ou « numéro de sécurité sociale ».

Le président de la Cnil, Alex TÜRK, a dès lors décidé la création d'un groupe de travail en vue d'évaluer la doctrine de la Cnil sur l'utilisation du NIR. Les conclusions de ce groupe de travail ont donné lieu à un avis de la Cnil du 20 février 2007⁸³. Dans cet avis, elle constate à nouveau que le NIR « *n'est pas un numéro comme les autres* » puisqu'il est :

- Signifiant : élaboré d'après le sexe, le mois, l'année de naissance et dans la plupart des cas, le département, la commune de naissance en France ou l'indication d'une naissance à l'étranger, il permet de les deviner facilement ;
- Unique et pérenne : à chaque personne est attribué un numéro unique depuis sa naissance ;
- A priori fiable : il est certifié par l'INSEE (Institution national de la statistique et des études économiques) à partir des données d'état civil transmises par les mairies.

Ainsi, toujours consciente des risques liés à l'utilisation du NIR, notamment l'interconnexion généralisée des fichiers⁸⁴, la Cnil a conclu que l'accès à des données nominatives, telles que celles contenues dans le DMP, ne pouvait pas reposer sur le NIR, même associé à un mot de passe, comme ce fut le cas lors des expérimentations.

Elle admet néanmoins la possibilité de construire un numéro de santé identifiant spécifique, généré à partir du NIR, sans possibilité de remonter à celui-ci, « *certifié selon les procédures déjà éprouvées, reconnues et fiables, actuellement utilisées pour les bénéficiaires de l'assurance maladie, mais transcodé selon des techniques établies de l'anonymisation. Ce numéro, non signifiant, constituerait l'identifiant de santé utilisable dans l'ensemble du système de soins. Cette proposition [...] permettrait de bénéficier des avantages du NIR au moment de la création de l'identifiant tout en maintenant un niveau de garantie élevé* ».

La Cnil ajoute que le contrôle de cet identifiant de santé n'est pas suffisant et doit être renforcé par des procédures « d'identité-vigilance », s'assurant par ce biais que le dossier médical se rapporte bien au patient concerné.

Le législateur a réagi sans attendre par la loi du 30 janvier 2007, dont l'article 25 abroge l'article 5⁸⁵ de la loi du 13 août 2004 et crée l'article L.1111-8-1 dans le code de la santé publique, selon lequel : « *Un identifiant de santé des personnes prises en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé défini à l'article L. 6321-1 est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé. Il est également utilisé pour l'ouverture et la tenue du dossier médical personnel institué par l'article L. 161-36-1 du code de la sécurité sociale et du dossier pharmaceutique institué par l'article L. 161-36-4-2 du même code. Un décret, pris après avis de la Commission nationale de l'informatique et des libertés, fixe le choix de cet identifiant ainsi que ses modalités d'utilisation.* »

⁸³Cnil, communiqué du 20 février 2007, www.cnil.fr.

⁸⁴L'utilisation du NIR facilite la recherche et le tri d'informations dans les fichiers.

⁸⁵L. 13 août 2004 relative à l'assurance maladie, article 5 : « *Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et pour la tenue du dossier médical personnel tel que défini à l'article L. 161-36-1 du code de la sécurité sociale, dans l'intérêt de la personne concernée et à des fins exclusives de coordination des soins.* »

Cet identifiant de santé spécifique a donc vocation à être utilisé pour le dossier pharmaceutique (DP) et plus largement pour la conservation, l'hébergement et la transmission de toutes les informations de santé à caractère personnel. Conformément à l'esprit du DMP, cette utilisation est faite « *dans l'intérêt des personnes concernées et à des fins de coordination et de qualité de soins* ».

A l'heure actuelle, nous sommes toujours dans l'attente de la publication de ce décret qui doit être précédée d'un avis de la Cnil.

B. L'INSUFFISANTE INTEROPERABILITE DES SYSTEMES

Jusque-là, la principale préoccupation du GIP-DMP a été d'élaborer les modèles techniques d'hébergement et d'accès du DMP. Aucune étude relative spécifiquement à la problématique d'interopérabilité des systèmes, notamment des logiciels médicaux, n'a été publiée. Mais, désormais, l'incertitude est levée : l'adaptation des postes de travail des professionnels de santé n'est pas assurée à ce jour. L'interopérabilité est seulement prévue dans la loi, mais en pratique aucune action d'envergure pour aboutir à une interopérabilité parfaite n'est engagée.

La loi impose pourtant à tous les détenteurs d'informations de santé à caractère personnel l'utilisation de dispositifs conformes aux prescriptions des règles de confidentialité et répondant à des conditions d'interopérabilité arrêtées par le ministre de la santé⁸⁶. Ainsi, les différents échanges du périmètre DMP doivent être conformes avec le Référentiel Général d'Interopérabilité (RGI) et le Référentiel Général de Sécurité (RGS). En effet, l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, impose que le titulaire d'un marché public prendra comme référence les documents RGI et RGS avec leurs versions respectives en date de parution du Cahier des clauses de travail particulières. En outre, les exigences de l'article L.1111-8 sont indispensables à la mise en place du DMP, dont l'objectif reste d'assurer un meilleur partage des données médicales tout en veillant à garantir le respect de la vie privée.

Le projet DMP étant le fer de lance du développement de l'information médicale, les normes d'interopérabilité qu'il mettra en œuvre auront vocation à servir le bon fonctionnement des systèmes d'informations hospitaliers et de ville.

La mise en place de logiciels interopérables avec les normes techniques requises par le système DMP, dépendra de l'aptitude des éditeurs de logiciels médicaux à s'adapter dans un temps très court à ces évolutions et à commercialiser des logiciels médicaux compatibles. Mais avant tout, il incombe à l'« hébergeur de référence » de développer les spécifications fonctionnelles et techniques qui vont permettre d'assurer la « DMP compatibilité » des logiciels médicaux. Ainsi, selon l'architecture technique élaborée par le GIP-DMP, pour aboutir à une mise en œuvre optimale de cette compatibilité, plusieurs étapes seront nécessaires :

⁸⁶ C. santé publ., article L.1111-8, alinéas 4 et 5.

- Tout d'abord, la publication par le GIP-DMP :
 - Du cadre général d'interopérabilité,
 - Des spécifications détaillées du portail,
 - Des spécifications détaillées des systèmes d'hébergement,
- Ensuite, l'intégration par les éditeurs de l'ensemble des spécifications susmentionnées,
- Puis, la fourniture par le GIP-DMP d'un référentiel et d'un environnement d'homologation des logiciels,
- Enfin, la commercialisation des nouvelles versions par les éditeurs.

Le GIP-DMP prévoit que la commercialisation des logiciels de santé, version « compatible DMP », doit débiter 18 mois après le commencement des travaux de l'« hébergeur de référence », soit à l'été 2009.

Ces référentiels de confidentialité et d'interopérabilité sont soumis à l'avis préalable de la Cnil et du comité d'agrément placé auprès du ministre de la santé. Cet avis s'imposera aux hébergeurs de données. D'ailleurs, la procédure d'agrément des hébergeurs de données a été suspendue pour une période de deux ans à compter de la promulgation de la loi du 30 janvier 2007⁸⁷. Cette suspension doit être applicable le temps nécessaire à la production de ces référentiels mais ne vaut pas pour les dispositifs d'hébergement du DMP.

Compte tenu de la situation passée où les retards se sont accumulés, il serait plus judicieux que le GIP-DMP accompagne les éditeurs de logiciels médicaux dans leurs démarches pour développer des logiciels « compatibles DMP ». En effet, il faut tenir compte du fait que les décrets relatifs à l'identifiant de santé et au DMP ne sont toujours pas parus. Un retard dans leur publication pourrait freiner l'élaboration des spécificités fonctionnelles et techniques concernant, notamment, les procédures de sécurité d'accès et de consultation des DMP.

Il faut également tenir compte de l'état actuel du marché des éditeurs de logiciels de santé. En France, ce marché n'est pas très structuré ; il existe d'innombrables éditeurs de ce genre, on en décompte 130 en France alors qu'il n'y en a qu'une quinzaine en Angleterre. Cette dispersion ne va pas faciliter la mise en place de logiciels compatibles.

N'oublions pas quel coût le changement vers un logiciel compatible va induire chez les professionnels de santé, ce qui peut également freiner légèrement la dynamique mise en place.

Quoiqu'il en soit, il semblerait que le GIP-DMP prenne la mesure de l'ampleur de ces questions de compatibilité. Il envisagerait même un processus d'homologation de la « compatibilité DMP », voire une labellisation « compatible DMP »⁸⁸.

⁸⁷ L. n° 2007-127 du 30 janvier 2007, art. 25.

⁸⁸ Cf. Rapport n°2007-157 sur le Dossier médical personnalisé, de l'IGAS.

SECTION 2 L'IMPACT DE L'OUTIL INFORMATIQUE DANS LA RELATION MEDECIN-PATIENT

L'usage de l'informatique lors du colloque singulier peut avoir des conséquences dommageables (§2). Cet usage a également un impact sur le régime de responsabilité médicale à l'égard des professionnels de santé (§1).

§1 L'IMPACT SUR LE REGIME DE RESPONSABILITE MEDICALE

L'utilisation du DMP par les professionnels de santé peut amplifier les cas d'engagement de la responsabilité médicale (B) comparativement au déroulement classique du régime de responsabilité médicale (A).

A. APERÇU DU REGIME DE RESPONSABILITE MEDICALE

L'usage d'un nouvel outil, aussi particulier quant à son régime juridique, conduit à s'interroger sur la responsabilité du professionnel de santé vis-à-vis du DMP.

Le droit de la responsabilité médicale est d'origine récente. Bien que le code civil de 1804 et le code pénal de 1810 aient posés les principes de la responsabilité médicale, ce ne fût que dans des domaines très particuliers⁸⁹, et ce sont plutôt les tribunaux qui ont introduit le principe général de la responsabilité du médecin :

- *Cass. 18 juin 1835, Affaire THOURET-NOROY contre Monsieur GUIGNE⁹⁰ : Première décision de justice à faire du médecin un justiciable lorsqu'il commet une faute grave et engage sa responsabilité sur le fondement des articles 1382 et 1383 du code civil, autrement dit sa responsabilité civile délictuelle ;*
- *Cass. Civ.1^{ère}, 20 mai 1936, MERCIER⁹¹ : cet arrêt pose le principe de la nature contractuelle de la responsabilité médicale : « Il se forme entre le médecin et son client un véritable contrat comportant pour le praticien, l'engagement sinon, bien évidemment, de guérir le malade, du moins de lui donner des soins, non pas quelconques mais consciencieux et attentifs, et réserve fait de circonstances exceptionnelles, conformes aux données acquises de la science [...] La violation même involontaire de cette obligation contractuelle étant sanctionnée par une responsabilité de même nature,*

⁸⁹ En matière pénale avec l'avortement et en matière civile avec le secret médical.

⁹⁰ Cass. 18 juin 1835, Affaire Thouret-Noroy contre Mr Guigne, Dalloz 1835, I p.300.

⁹¹ Cass. civ. 1^{ère}, 20 mai 1936 Mercier, Sirey 1937 p.321.

également contractuelle ». La Cour de cassation précise également que le médecin est tenu à une obligation de moyens⁹² : il doit mettre en œuvre tous les moyens en sa possession et ne doit pas garantir un résultat.

Pour autant, le médecin sera exonéré de responsabilité, totalement, en cas de survenance d'un cas de force majeure, partiellement en cas de fait d'un tiers. En revanche, la faute de la victime n'exonère pas la responsabilité du praticien.

D'après l'article L.1142-1 du code de la santé publique, « *Hors le cas où leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé mentionnés à la quatrième partie du présent code, ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute* ».

Comme évoqué ci-dessus, le régime de responsabilité applicable aux professionnels de santé est un régime de responsabilité pour faute, la pratique médicale étant une activité à risques exercée au sein d'une profession organisée.

Le médecin peut voir sa responsabilité engagée sur différents fondements : pénal, disciplinaire ou civil. Au pénal, la responsabilité du médecin peut être engagée, quelque soit le mode d'exercice (libéral, salarié, hôpital public), pour des fautes commises constitutives d'une infraction pénale réprimée par le code pénal ou d'une infraction au code de la santé publique. Le médecin engagera sa responsabilité disciplinaire, devant le Conseil de l'Ordre des Médecins, en cas de violation d'une règle déontologique⁹³ ou sur le fondement des principes généraux de morale, de probité, de dévouement pour l'exercice de l'art médical. Enfin, il engagera sa responsabilité devant la juridiction civile, si les conditions de la responsabilité civile (délictuelle ou contractuelle) sont réunies : la faute professionnelle, un préjudice et un lien de causalité entre la faute et le préjudice.

Depuis l'arrêt Mercier, la doctrine de la Haute Juridiction n'a pas varié⁹⁴. Mais sous cette apparente continuité jurisprudentielle, la Cour de cassation a profondément modifié la situation du malade-victime en lui reconnaissant deux droits :

- *Le droit à l'information du malade-victime* : dans un arrêt du 25 février 1997, la Cour de cassation a imposé au médecin d'apporter la preuve qu'il a bien fourni à son malade les informations lui permettant de donner « un consentement éclairé » avant tout acte médical c'est-à-dire « des informations simples (compréhensibles), accessibles et loyales ». La preuve de cette information peut être apportée par tous moyens⁹⁵, « l'information doit porter non seulement sur les risques graves de l'intervention mais aussi sur tous les

⁹² De nos jours, le médecin est tenu d'une obligation de résultat en matière de chirurgie esthétique, de prothèses et d'analyses biologiques standards. La charge de la preuve est différente selon que l'obligation est de moyen ou de résultat : le médecin est présumé coupable/fautif en matière d'obligation de résultat, alors qu'en cas d'obligation de moyen le patient doit apporter la preuve de la faute du médecin.

⁹³ Selon l'article L.382 CSP : « l'ordre des médecins veille d'une part au maintien des principes de moralité, de probité, de dévouement indispensables à l'exercice de la médecine ; et d'autre part, à l'observation par tous ses membres des devoirs professionnels ainsi que des règles édictées par le code de déontologie médicale ».

⁹⁴ Encore, par un arrêt du 8 novembre 2000 (Cass.1^{ère} civ. 08 nov. 2000, n°99-11.735, n°1815 FP-P+B+R), elle a jugé qu'en l'absence de faute, le médecin ne pouvait être tenu responsable du dommage subi par le malade au cours d'une intervention chirurgicale.

⁹⁵ Cass. Civ.1^{ère}, 14 octobre 1997, Civ. I, *Bull.* n° 278, rap. Sargos publié au *JCP* 1997, 11, 22942.

inconvenients pouvant en résulter »⁹⁶ ; « *le médecin est tenu de donner une information sur les risques graves afférents aux investigations et soins proposés et il n'est pas dispensé de cette obligation par le seul fait que ces risques ne se réalisent qu'exceptionnellement* »⁹⁷.

- Le droit à la sécurité : le 29 juin 1999⁹⁸, la Cour de cassation a rendu trois arrêts en matière d'infection nosocomiale faisant mention pour le médecin ou l'établissement de santé d'une obligation de sécurité. Il sera ainsi retenu une responsabilité alors qu'aucune faute d'asepsie n'aura été mise en évidence. La faute sera présumée puisque le malade était indemne de toute affection avant l'intervention.

Contrairement au devoir d'information, qui entre dans le cadre de la déontologie médicale⁹⁹ et dont l'absence est assimilée à une faute, on se trouve en présence d'une brèche énorme au sein de la doctrine de l'obligation de moyens. En effet, le groupe des affections nosocomiales est loin d'être homogène puisqu'environ 30% d'entre elles sont totalement inévitables. A l'entrée d'un hôpital, il y a 30% de risques d'en contracter une.

A noter que pour la responsabilité des hôpitaux, le Conseil d'Etat, le 9 avril 1993, dans un arrêt BIANCHI¹⁰⁰, a reconnu la responsabilité de l'établissement hospitalier en l'absence de faute, lorsque et seulement si des conditions strictes sont présentes : un acte nécessaire, un risque connu mais exceptionnel, une absence de risque chez ce patient, un lien de causalité entre l'acte et le dommage et la gravité exceptionnelle des séquelles.

Cela démontre que le patient bénéficie d'une protection non négligeable dans le régime de responsabilité médicale.

B. LA RESPONSABILITE MEDICALE A L'AUNE DU DOSSIER MEDICAL PERSONNEL

Dans le cas du DMP, les règles de la responsabilité ne sont pas modifiées : la responsabilité du médecin pourra être engagée en cas de faute professionnelle reconnue par le juge dans l'usage du DMP. Malgré tout, dans un contexte de juridiciarisation des questions médicales, le Groupement d'intérêt public du DMP (GIP-DMP) a sollicité une étude exhaustive sur les questions juridiques, notamment en matière de responsabilité médicale, susceptibles d'être soulevées par l'usage du DMP. En matière de responsabilité des professionnels de santé, l'étude a conclu que le DMP « *ne constitue qu'un outil de stockage de l'information accessible à tous [et] n'entraîne pas de modification du régime de responsabilité des professionnels* »¹⁰¹. Le cabinet d'avocats chargé de l'étude relève, toutefois, que deux éléments résultant de l'application du régime juridique du DMP, peuvent

⁹⁶ Cass. Civ.1^{ère}, 17 février 1998, D. Halliez, Petites affiches n° 90 - 6 mai 1999.

⁹⁷ Cass. Civ.1^{ère}, 23 février 1999.

⁹⁸ Cass. Civ. 1^{ère}, 29 juin 1999, pourvoi n°97-14254 ; Bulletin 1999 I N° 220 p. 141, Le Dalloz, 1999-10-28, n° 38, p. 559, note D. THOUVENIN. Gazette du Palais, 1999-10-30, n° 303, p. 3, note Y. LACHAUD. Revue trimestrielle de droit civil, 1999-12, n° 4, p. 840, note P. JOURDAIN. Gazette du Palais, 2000-04-06, n° 97, p. 13, note S. HOCQUET-BERG.

⁹⁹ C. déont. méd., article 35.

¹⁰⁰ Accessible sur http://www.lexinter.net/JPTXT2/arret_bianchi.htm au 13 mai 2008.

¹⁰¹ <http://www.d-m-p.org/docs/DMPetudeResponsabilite2005.pdf>

conduire à une acception plus large d'un cas de faute professionnelle de la part des juges :

- L'obligation faite aux professionnels par la loi de tenir à jour le DMP : « chaque professionnel de santé, exerçant en ville ou en établissement de santé, quel que soit son mode d'exercice, reporte dans le dossier médical personnel, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge¹⁰² ». Il semblerait que les hypothèses de violation de cette obligation soient limitées compte tenu des engagements auxquels le médecin est tenu, en premier chef le secret médical et le recueil du consentement du patient qui tiennent lieu de garde-fou. Ainsi, lors de la mise à jour du DMP, le médecin sera à même d'apprécier la nature et la forme des informations à inscrire dans le DMP.
- L'hypothèse d'une erreur de diagnostic faite en méconnaissance d'une information inscrite dans le DMP. Jusqu'à l'arrêt Mercier, la responsabilité médicale ne pouvait être que délictuelle. Mais cet arrêt a mis en évidence l'obligation de soins résultant de la relation contractuelle liant le patient à son médecin. L'article 33 du code de déontologie médicale¹⁰³ précise les modalités de cette obligation de soins : « Le médecin doit toujours élaborer son diagnostic avec le plus grand soin, en y consacrant le temps nécessaire, en s'aidant dans toute la mesure du possible des méthodes scientifiques les mieux adaptées et, s'il y a lieu, de concours appropriés. ». Comme rappeler ci-dessus, il s'agit d'une obligation de moyens et non pas d'une obligation de résultat.

En qualité de « serveur de résultats »¹⁰⁴, puisque destiné à rassembler l'ensemble des informations médicales du patient et à les mettre à disposition des médecins, le DMP peut faciliter la mise en cause du diagnostic d'un médecin. En effet, toujours selon l'étude commandée par le GIP-DMP, la méconnaissance d'une information, inscrite dans le DMP, lors de la formulation d'un diagnostic erroné pourrait engager la responsabilité du médecin pour faute : « Depuis 1986 déjà, les juges ont tendance à estimer que l'erreur de diagnostic constitue une faute à part entière. Cette assimilation sera renforcée, lorsque le professionnel disposera de tous les éléments permettant de connaître le « passé médical » du malade, puisqu'il deviendra susceptible d'éviter une confusion dans le diagnostic. Or, avec le DMP, le médecin bénéficiera de la totalité des informations lui permettant de réaliser les meilleurs diagnostics et/ou acte thérapeutique. Le DMP risque donc de faciliter l'assimilation de l'erreur et de la faute ».

Pour parer à ce type de faute éventuelle, le DMP doit assurer l'accessibilité et la lisibilité dans les conditions normale de l'exercice médical, grâce à une organisation structurée des informations.

¹⁰² Article L. 161-36-2 du Code de la sécurité sociale.

¹⁰³ Figure aussi à l'article R.4127-33 du code de la santé publique.

¹⁰⁴ Rapport sur le dossier médical personnalisé (DMP), Mission Interministérielle de revue de projet sur le DMP réunissant l'Inspection Générale des Finances, l'Inspection Générale des Affaires Sociales, le Conseil Général des Technologies de l'Information, déposé en novembre 2007.

Il faut souligner que ces considérations ne valent pas dans l'hypothèse où le patient a exercé son droit de masquage, notamment à l'endroit d'une information utile au diagnostic : la responsabilité du médecin ne peut pas être engagée. Le décret dit « DMP » doit prévoir un journal retraçant les décisions de masquage auquel on pourrait se référer en cas de contentieux.

§2 LA RELATION MEDECIN – PATIENT EN CAUSE

L'outil informatique, comme acteur dans la protection de la santé du patient, peut perturber la relation médecin-patient (A) ; mais il peut également servir de médiateur (B) en impliquant davantage le patient dans la protection de sa santé.

A. L'INFORMATIQUE COMME OBSTACLE AU « COLLOQUE SINGULIER »¹⁰⁵

Suite à l'apparition du réseau Internet, les sites relatifs à la santé ont pullulé révolutionnant ainsi l'accès à l'information médicale par les patients. Alors qu'auparavant, le patient ne se référait qu'au discours abrupt de son médecin traitant à propos de sa santé, désormais il peut échanger en ligne avec d'autres patients, recevoir des conseils d'autres praticiens, dont les propos sont adaptés à sa compréhension de profane.

Cette évolution de la technique permet d'ouvrir une fenêtre sur le monde obscur de la médecine, les patients se sentant moins isolés et sensiblement plus avertis. Les médecins eux-mêmes, y voient quelques avantages, par exemple un patient informé. Ils y voient aussi quelques obstacles car un patient informé ne correspond pas forcément à un patient bien informé. En effet, si la plupart des sites Internet traitant de la santé sont prudents quant à la qualité de l'information délivrée, d'autres peuvent être dangereux. L'accès par les malades une quantité monstrueuse d'informations « brutes », peut entraîner les pratiques d'automédication, qui, comme chacun le sait, peut causer des effets indésirables chez le malade.

L'usage du dossier médical personnel peut pareillement léser la relation patient-médecin. Prenons par exemple l'hypothèse où le professionnel de santé, autorisé par le patient à accéder à son DMP, y dépose un compte-rendu de résultats en l'absence du patient, autrement dit en dehors de toute consultation médicale. En effet, comme on l'a vu, le praticien autorisé peut accéder seul au DMP et l'alimenter, seul. Dans ce cas, faut-il penser que le patient aura la possibilité d'avoir accès à ces résultats *via* son DMP sans l'accompagnement d'un professionnel de santé ? Il semblerait que non. Le CCNE, dans son avis sur le dossier médical personnel¹⁰⁶ a en effet relevé que les informations transmises au patient concernant un diagnostic ou un pronostic défavorable ne devraient être versées au DMP qu'après la consultation d'annonce. Il a jugé cela comme étant une limite au DMP. Nous partageons son

¹⁰⁵ Le colloque singulier désigne la rencontre indispensable entre un professionnel et un patient, rencontre qui permet au premier de trouver une réponse au besoin du second.

¹⁰⁶ CCNE, avis n°104 Le « dossier médical personnel » et l'informatisation des données de santé.
<http://www.ccne-ethique.fr/>.

avis. L'objectif du DMP d'améliorer la coordination des soins ne peut être entièrement rempli si une consultation d'annonce doit sans cesse précéder le dépôt de données importantes sur le patient par le professionnel de santé.

Dans la logique d'un dossier médical partagé, on aurait pu prévoir que certaines informations de santé soient partagées entre médecins directement *via* le DMP sans pour autant être précédées d'une consultation. Cela aurait permis un gain de temps donc d'argent, compte tenu des délais d'attente pour obtenir un rendez-vous d'un professionnel de santé.

On se trouve ici en face d'une contradiction entre les objectifs affichés du DMP et l'obligation de recueillir le consentement du patient pour accéder à son DMP.

B. L'INFORMATIQUE: ENTREMETTEUR DE LA RELATION MEDECIN/PATIENT

Suivant le même raisonnement qu'évoqué ci-dessus, le fait que le médecin puisse obtenir des informations médicales pour former son diagnostic ailleurs que dans les confidences directes du patient sur ses symptômes et ses antécédents est un élément également un élément perturbateur du colloque singulier et de sa qualité. Cette perturbation peut trouver sa cause autant dans l'entremise d'un ordinateur que dans le contenu du DMP.

Le CCNE a évoqué ce risque et sa cause matérielle dans un avis sur l'informatisation de la prescription : « *Le constat n'est pas rare : parce qu'il « triangularise » la relation, la présence d'un ordinateur dans un espace d'interlocution tend à empêcher une forme directe de discussion. Le regard du sujet assis derrière son écran est capté, comme si la lumière artificielle l'attirait à lui. En consultation, il arrive que le médecin soit comme « happé » par son écran, en sorte qu'il regarde davantage en direction de l'ordinateur que du côté de son patient. Ce glissement pernicieux dans l'usage de l'outil informatique est révélateur d'une possible altération de la qualité relationnelle du dialogue.* »¹⁰⁷

Comme on l'a vu, un droit au masquage des informations souhaitées par le patient, a été mis en place par le législateur. Ce droit ne va pas permettre d'améliorer le colloque singulier du patient et du professionnel de santé, déjà perturbé. Ce masquage peut s'avérer arbitraire et pouvant entraîner des risques d'erreurs non négligeables. Or, il ne faut pas oublier que la qualité du colloque singulier est le fondement de la relation thérapeutique entre le médecin et le professionnel de santé.

¹⁰⁷ Avis sur les problèmes éthiques posés par l'informatisation de la prescription hospitalière et du dossier du patient, Comité consultatif national d'éthique pour les sciences de la vie et de la santé, 16 février 2006.

CHAPITRE 2 DES CONTRAINTES TECHNIQUES

Le fait que le dossier électronique puisse désormais « sortir » du cabinet médical et figurer sur la toile, impose le recours à des normes de sécurité suffisante pour éviter toute menace interne ou externe. A cette fin, il faut d'abord étudier les standards existant en informatique (Section 1), pour ensuite en faire une application spécifique au système DMP (Section 2).

SECTION 1. LES STANDARDS DE LA SECURITE INFORMATIQUE

Les premières mesures de sécurité d'un système informatique concernent l'accès des utilisateurs à ce système (A) mais aussi la plateforme d'hébergement de ce système (B).

§1 UN ACCES SOUS CONTROLE

Seuls le titulaire (A) et les professionnels de santé autorisés (B) ont accès au contenu du DMP, en lecture et en écriture. L'article L.1111-8 du code de la santé publique précise ainsi, que « *tout acte de cession à titre onéreux de données de santé identifiantes, directement ou indirectement, y compris avec l'accord de la personne concernée est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal* ».

A. ACCES ET IDENTIFICATION DES PATIENTS

Le patient titulaire de son DMP, peut accéder en mode lecture à tous les éléments du dossier médical personnel. Mais il ne pourra accéder en mode écriture que dans une partie de l'espace « Identification » et dans la totalité de l'espace « Expression personnelle ».

L'espace « Expression personnelle » peut comporter tous les documents souhaités par le patient, dans la limite de l'espace de stockage prévu, et sous sa propre responsabilité. Toutes les données contenues dans cet espace peuvent être modifiées ou effacées par le patient. En revanche, il ne pourra ni modifier ni effacer les données de santé toujours alimentées en écriture par les professionnels de santé, il n'y aura accès qu'en mode lecture. Le patient aura néanmoins la possibilité de télécharger ces données sur son poste de travail.

Pour accéder à son DMP, le titulaire n'aura pas d'autre choix que d'utiliser un

navigateur web¹⁰⁸, que ce soit pour le mode lecture seule, le mode lecture et écriture ou le mode copie/édition/enregistrement sur un poste de travail.

En outre, il incombera à l'« hébergeur de référence » de mettre à la disposition du titulaire toute une gamme d'outils (recherche, tri, etc.) et de développer des interfaces visant à proposer l'accès au DMP *via* d'autres terminaux (téléphones portables, télévisions, assistant personnel).

En application de la Loi « Informatique et libertés », l'hébergeur, en tant que responsable du traitement, devra permettre au titulaire de demander une correction d'anomalie d'ordre technique et non médical (par exemple une corruption de document, une erreur d'exploitation, suite à un virus,...). Cette demande se fera par le biais d'un formulaire électronique mis à disposition du patient sur son DMP par l'hébergeur qui devra alors procéder à la correction, sous la responsabilité du médecin de l'hébergeur dans un délai maximum de 48 heures.

En outre, le patient dispose du droit de masquer certaines informations contenues sur son DMP : cela s'applique aux données de santé et aux données d'expression personnelle. Les données peuvent être masquées à une ou plusieurs catégories de professionnels de santé. Sauf opposition du patient, les données masquées sont visibles pour le médecin traitant et pour les professionnels de santé accédant au dossier en cas d'urgence ou de risque immédiat pour la santé (procédure de « bris de glace »). Il existe la possibilité de « masquer le masquage » vis-à-vis des professionnels de santé et de l'auteur du document. Néanmoins, une trace doit permettre d'identifier les données masquées et l'auteur du masquage, ainsi que le fait que les données étaient masquées lors de la consultation d'un professionnel de santé.

Dans la même logique, l'hébergeur doit tracer l'ensemble des actions réalisées par tous les utilisateurs. Ainsi, à la demande du titulaire, il doit pouvoir l'informer des actions réalisées sur son DMP, en lui communiquant les éléments d'identification des documents concernés, leurs auteurs, la date de dépose, les masquages réalisés.

L'article L.1111-8-1 du Code de la santé publique prévoit le mode d'identification personnelle du patient, nécessaire à la collecte des données de santé et à l'accès au DMP. Le texte précise qu'il s'agira d'un « identifiant de santé » et renvoie à un décret en Conseil d'État, pris après avis de la Cnil, le soin de fixer les conditions d'utilisation de cet identifiant de santé. Les conditions d'application de l'ensemble du dispositif, et notamment les conditions d'accès aux différentes catégories d'informations qui figurent au DMP, doivent être fixées par le décret « DMP » (article L. 161-36-4 du code de la sécurité sociale). Il doit également préciser le contenu du DMP ainsi que les modalités de gestion et d'utilisation du DMP tant par le patient que par les professionnels de santé, en particulier les outils d'identification (la future carte Vitale 2 contenant le numéro d'identification de santé pour le patient, la carte de professionnel de santé (CPS) pour les professionnels de santé) et d'authentification.

¹⁰⁸ Définition de « navigateur web » : « Un navigateur web est un logiciel conçu pour consulter le World Wide Web. Techniquement, c'est au minimum un client HTTP. Le terme navigateur web (ou navigateur Internet) est inspiré de Netscape Navigator. [...] La fonction principale d'un navigateur web est de permettre la consultation d'informations disponibles (« ressource » dans la terminologie du Web) sur le World Wide Web » ; accessible sur http://fr.wikipedia.org/wiki/Navigateur_web, au 10 août 2008.

Enfin, l'article 55 de la loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008¹⁰⁹, précise la durée de conservation du DMP qui est fixée à dix ans à compter de sa clôture. Il précise également certaines conditions particulières d'accès au DMP : en cas de décès du titulaire d'un DMP, les ayants droit peuvent y accéder conformément aux dispositions de l'article L.1110-4 du code de la santé publique ; l'accès à ce dossier est également possible dans le cadre d'une expertise médicale.

B. ACCES ET IDENTIFICATION DES MEDECINS

L'accès du DMP est limité aux seuls professionnels de santé et, parmi eux, à ceux désignés par le patient. Même avec le consentement du patient, le DMP ne peut être accessible à d'autres personnes. Ainsi, l'article L. 161-36-3 du Code de la sécurité sociale interdit l'accès au DMP lors de la conclusion de contrats exigeant l'évaluation de l'état de santé de l'une des parties comme le contrat de travail, ou de contrats de protection complémentaire en matière de santé. Le DMP n'est pas non plus accessible au médecin du travail. Le non-respect de ces dispositions est pénalement sanctionné.

En effet, la loi prévoit que l'accès des professionnels de santé à un dossier médical personnel est subordonné au consentement exprès du titulaire de celui-ci. Pour autant, il est prévu des cas exceptionnels pour lesquels une autorisation de consultation et/ou d'écriture peut être donnée au professionnel de santé, alors même que des droits n'ont pas été enregistrés au préalable dans le portail. Ainsi, il est prévu :

- L'accès par déclaration du professionnel de santé ;
- L'accès « bris de glace » pour les situations d'urgence et alors que le patient est dans l'impossibilité d'exprimer sa volonté) ;
- L'accès médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente (le 15), mais ils ne peuvent que consulter le DMP et non l'alimenter.

Compte tenu des résultats des expérimentations, le cadre législatif mis en place par la loi du 13 août 2004 relative à l'assurance maladie concernant l'accès des médecins au DMP et aux modalités d'expression du consentement du patient a été complété. L'article 88-IV de la loi de financement de la sécurité sociale pour 2007 a introduit l'article L. 161-36-2-1 dans le code de la sécurité sociale. Cet article élargit expressément l'accès au dossier médical personnel aux médecins coordonnateurs des établissements assurant l'hébergement des personnes âgées, avec l'accord du titulaire ou de son représentant légal.

En outre, l'article 25 de la loi n° 2007-127 du 30 janvier 2007¹¹⁰ introduit un nouvel article L. 161-36-2-2 dans le code de la sécurité sociale qui autorise les professionnels de santé à accéder au DMP d'une personne qui est hors d'état d'exprimer son consentement et dont la situation comporte un risque immédiat pour sa santé, sauf opposition expressément et préalablement exprimée (procédure dite de « bris de glace »). Il est également prévu que le médecin puisse solliciter du patient son consentement à ce qu'un confrère à qui il confie une partie de la prestation de soins accède au DMP de l'intéressé et l'alimente.

¹⁰⁹ L. n°2007-1786 de financement de la sécurité sociale pour 2008, du 19 décembre 2007, JORF n°0296, 21 déc., page 20603, texte n° 1, article 55 codifié à l'article L.161-36-3 du Code de la sécurité sociale.

¹¹⁰ Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique

Cette modification du cadre législatif quant à l'accès des médecins au DMP, confirme que le DMP reste un dossier médical professionnel, à l'usage des professionnels de santé dans l'intérêt du patient.

Le professionnel de santé peut déposer dans le DMP les informations utiles à la coordination, la qualité, la continuité des soins et la prévention ; les informations déposées sont datées et signées. Les documents de santé supprimés sont rendus inaccessibles au professionnel de santé et au titulaire, et conservées pendant dix ans par l'hébergeur. Au-delà de ce délai réglementaire, l'hébergeur procède à l'effacement total des données.

Enfin, le professionnel de santé libéral peut accéder à un DMP *via* son logiciel professionnel depuis son lieu d'exercice ou depuis le domicile du patient. L'accès des professionnels de santé au DMP *via* un navigateur web n'est pas nécessaire pour le démarrage du DMP. Quant à l'authentification, outre ce que doit prévoir le décret « DMP », la présence de la carte CPS (Carte de Professionnel de Santé) est obligatoire.

§2 UN MODELE D'HEBERGEMENT COMPLEXE

La mise en place du DMP s'est appuyée sur un cadre législatif préexistant en matière d'hébergement de données de santé à caractère personnel (A) ; le GIP-DMP a néanmoins cru nécessaire d'adapter un nouveau modèle d'hébergement dans le cadre du DMP (B).

A. LES HEBERGEURS DE DONNEES DE SANTE A CARACTERE PERSONNEL

La loi du 13 août 2004 qui institue le dossier médical personnel prévoit que « *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 code de la santé publique* ».

C'est la loi du 4 mars 2002 (Article L1111-8, du code de la santé publique) qui définit la fonction d'hébergement de données de santé, précisant que celle-ci est assurée par un « hébergeur » à qui ces données ont été confiées : « *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.* »

Ainsi, l'hébergeur est chargé de la conservation et de l'intégrité des DMP. Il contrôle la sécurité et la confidentialité des données et des documents hébergés, et donne accès, en écriture ou en lecture, au dossier conformément aux droits d'accès que lui a précisés le patient.

La loi du 4 mars 2002 a été complétée par le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique¹¹¹.

Les conditions d'agrément de ces hébergeurs de données, prévues par le décret, sont codifiées aux articles R.1111-9 et suivants du code de la santé publique¹¹². Les candidats à l'agrément doivent offrir un certain nombre de garanties parmi lesquelles figure la mise en œuvre de règles de confidentialité et de sécurité. Ce dispositif législatif vise à rendre applicable les critères posés par les articles L.1111-7 et suivants du code de la santé publique relatifs au droit d'accès du patient à l'ensemble des informations concernant sa santé détenues par les professionnels de santé.

L'agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel est délivré par le ministre chargé de la santé, qui se prononce après avis de la Commission nationale de l'informatique et des libertés et d'un comité d'agrément placé auprès de lui, comprenant des personnalités qualifiées et des représentants des usagers du système de santé. Ce comité d'agrément a vocation à agréer les hébergeurs de données, et à trancher des demandes d'agrément qui lui seraient adressées. Il doit rendre sa décision dans le mois qui suit l'avis de la Cnil. Celle-ci a un rôle important car elle doit se prononcer sur les garanties proposées par le candidat à l'agrément. Le candidat à l'agrément doit présenter les solutions techniques qu'il envisage, pour garantir le respect de la loi, et s'engager :

- à ce que le service rendu soit réalisé sur le territoire de l'Union Européenne ;
- à ce que ces données soient individualisées au regard d'autres données ;
- il doit également nommer une personne responsable de cette activité.

Ainsi, pour être agréé, l'hébergeur de données devra mettre en place une politique de confidentialité, identifiée, contractualisée, et même garantie, envers ses éventuelles sous-traitants, et décrire notamment les modalités d'exercice du droit d'accès prévu par la loi.

L'agrément est délivré aux hébergeurs de données de santé à caractère personnel pour une durée de trois ans. Il peut être renouvelé par l'hébergeur, sous réserve qu'il présente une nouvelle demande.

La politique de confidentialité de l'hébergeur devra notamment être explicite sur les points suivants¹¹³ :

- sur les aspects de respect des droits des personnes concernées par les données déposées ;

¹¹¹ Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique, J.O. du 5 janvier, texte n°14.

¹¹² C. santé publ., article R.1111-9 : « Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficiaire d'un agrément à ce titre doit remplir les conditions suivantes :

1° Offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi ;[...] ».

¹¹³ C. santé publ., article R.1111-15.

- en matière de sécurité de l'accès aux informations ;
- en matière d'organisation et de procédure de contrôle interne, mises en place pour garantir la sécurité des traitements et des données ;
- en matière de garanties de disponibilité et de continuité des services, de politique de sécurité liée à la sauvegarde, la restauration et l'archivage des données.

Tout manquement du sous-traitant aux obligations ou à la politique présentées par l'hébergeur peut mettre fin à l'agrément. Il faudra également déterminer les responsabilités encourues et par qui, prestataire technique (hébergeur) ou service médical.

B. L'HÉBERGEUR « DE RÉFÉRENCE » ET LES HÉBERGEURS « AGRÉÉS »

La fin de la phase d'expérimentation a débouché sur la modification du dispositif d'hébergement des données du DMP. Jusque-là, des opérateurs privés étaient mis en concurrence sur le territoire national. Sélectionnés sur appel d'offres, ils se répartissaient le territoire en six monopoles géographiques, et devaient par la suite entrer en service parallèlement et de manière compétitive. Leurs rémunérations devaient être déterminées administrativement et assurées, directement ou indirectement, par l'Etat.

Face à la complexité d'un tel dispositif, notamment en cas de changement d'un opérateur à un autre décidé par le patient et dans le but d'agir sur une diminution des prix, le GIP-DMP a décidé de changer de modèle. Désormais, le dispositif d'hébergement des données du DMP s'opère à un double niveau : celui d'un hébergeur dit « de référence » et celui d'hébergeurs « agréés ».

L'« hébergeur de référence » est sélectionné à l'issue d'un appel d'offres et a compétence nationale. Il aura vocation à garantir la continuité du service, la reprise et la transférabilité inter-opérateurs des dossiers. Ainsi, cet opérateur n'aura pas d'activité commerciale liée à cette mission et sera rémunéré proportionnellement au nombre de dossiers gérés sur la base d'un prix administré, avec un minimum garanti de cinq millions de dossiers.

Alors que les hébergeurs « agréés », hébergeurs de données de santé à caractère personnel au sens de la loi du 4 mars 2002, seront en compétition nationale pour s'attacher la clientèle des patients. Ils devront opérer selon les normes d'interopérabilité de l'« hébergeur de référence » et seront rémunérés proportionnellement au nombre de dossiers hébergés par la collectivité, sur la base d'un tarif public unique établi à partir du prix proposé par l'« hébergeur de référence ».

Ils pourront offrir l'accès gratuit au DMP dans le cadre d'une offre de bouquets de services payants ou rétribués. Autrement dit, ils pourront proposer aux patients d'autres services à valeur ajoutée, sans lien direct avec le contenu du DMP, auquel ils n'auront pas accès. L'assuré pourra choisir l'hébergeur de son choix et pourra en changer à tout moment.

Ainsi, le rôle et les fonctions diffèrent entre « hébergeur de référence » et hébergeurs « agréés ». L' « hébergeur de référence » est LE décideur de la conception, du développement et de la maintenance des DMP, de leur exploitation dans des conditions d'hébergement sécurisé avec une disponibilité de 99,9%. Il a doit, en outre assurer la fonction de préserver, sécuriser et administrer les données du DMP. Tous les quatre ans sera désigné un nouvel « hébergeur de référence ».

Le rôle d' « hébergeur de référence » est réservé aux sociétés qui ont l'envergure pour assurer la conception de l'ensemble du système, de l'applicatif, des services et de l'hébergement : "un grand intégrateur".

Dans un communiqué de presse du 30 mars 2007, le GIP-DMP a fait savoir que l'appel d'offres pour sélectionner l' « hébergeur de référence » des DMP était lancé. Cet appel d'offres a été publié au Journal Officiel de l'Union Européenne (JOUE) le 3 avril 2007¹¹⁴ ainsi qu'au Bulletin Officiel des Annonces de Marchés Publics (BOAMP), publié le 4 avril 2007¹¹⁵. Cette procédure avait déjà été annulée deux fois.

Six hébergeurs ont déjà été agréés, le 18 mai 2006, afin de participer à la phase d'expérimentation. Les données produites lors de celle-ci ne pourront être conservées par les hébergeurs seulement en cas de consentement « libre, éclairé et certain » du patient. Sous la même condition, elles pourront être réutilisées dans le cadre de la phase de généralisation, sous la condition que le patient ouvre son DMP au démarrage de la généralisation.

Le choix de ce modèle d'hébergement peut poser problème au fil du temps. En effet, l' « hébergeur de référence » peut se retrouver en situation hégémonique face aux hébergeurs « agréés » ; il aura l'avantage d'avoir élaboré les spécifications qui s'imposeront aux autres hébergeurs. De plus, il bénéficiera d'une garantie de rémunération correspondant à cinq millions de DMP s'il assure son rôle de garant de la continuité du service. Le plus important : il pourra concurrencer les hébergeurs « agréés », puisqu'il sera autorisé à assurer l'hébergement de dossiers sans pour autant pouvoir faire la promotion de son service d'hébergement auprès des usagers. Mais, une promotion lui sera-t-elle vraiment nécessaire compte tenu de sa position hégémonique d' « hébergeur de référence ». La promotion autour du DMP suffira à le faire connaître.

Le GIP-DMP a malgré tout tenu à rappeler que *"l'hébergeur de référence n'aura pas l'exclusivité de l'hébergement des DMP, mais à la différence des autres hébergeurs agréés, sera chargé d'une mission de service public : être en capacité d'hébergement de l'ensemble des 60 millions d'assurés. Il ne pourra fournir d'autres fonctionnalités ou services à destination des titulaires des DMP"*.

Enfin, tant le rapport de l'IGAS de novembre 2007¹¹⁶ que celui de la Commission des affaires culturelles, familiales et sociales du 29 janvier dernier¹¹⁷, ont recommandé

¹¹⁴ JOUE n°2007/S65-079617.

¹¹⁵ Annonce n°337 publiée le 04/04/2007 dans le BOAMP n°066 B, Dépt.75.

¹¹⁶ Rapport sur le dossier médical personnalisé (DMP), Mission Interministérielle de revue de projet sur le DMP réunissant l'Inspection Générale des Finances, l'Inspection Générale des Affaires Sociales, le Conseil Général des Technologies de l'Information, déposé en novembre 2007.

¹¹⁷ Rapport d'information sur le dossier médical personnel déposé le 29 janvier 2008, Assemblée nationale-

l'annulation de l'appel d'offres visant à désigner l' « hébergeur de référence ». L'IGAS considère qu'il s'agit d'un modèle de concurrence susceptible d'entraîner des dérives et que ce marché « est un piège juridique et financier pour l'Etat ».

SECTION 2. LES CHOIX TECHNIQUES DU DOSSIER MEDICAL PERSONNEL

La principale crainte du public vis-à-vis du DMP est la récupération de données identifiantes par des tiers malintentionnés. C'est pourquoi les mesures de sécurité adoptées pour le système DMP sont l'objet de tous les regards (§1) ; d'autant que les vulnérabilités à l'égard d'un système informatique, tel que le DMP, doivent être dans tous les cas supprimées (§2).

§1 LA SECURITE DES DONNEES DU DOSSIER MEDICAL PERSONNEL

Il s'agit ici d'analyser les normes de sécurité mises en place au sein du système DMP (B), au regard des modèles préexistants pour le secteur de la santé (A).

A. LES MODELES DE SECURITE POUR LE SECTEUR DE LA SANTÉ

Le dossier médical personnel entre dans la catégorie générale des systèmes d'information et de communication de santé (SICS). Ces derniers permettent de stocker et de gérer des informations médicales, administratives ou sociales relatives à des personnes. Ils exploitent les technologies de l'informatique pour permettre aux utilisateurs un accès rapide, et ainsi faciliter les actes médicaux, les remboursements, etc.

Toutefois, les menaces qui guettent de tels systèmes peuvent engendrer une réticence de la part des patients et des usagers. En effet, l'exploitation abusive par un utilisateur malhonnête d'un SICS insuffisamment protégé peut rendre possible la divulgation de données personnelles à différents intéressés : employeurs, concurrents, etc. Les erreurs de saisie ou de conception peuvent entraîner des erreurs de diagnostic ou de soins. Les défaillances peuvent empêcher le personnel soignant d'accéder à des informations indispensables.

Pour atteindre un niveau de protection satisfaisant, il faut définir une politique de sécurité correspondant aux besoins. C'est une étape primordiale qui consiste à élaborer un ensemble de règles en fonction d'une analyse des risques. Ceci afin de minimiser le risque de dommages indésirables ou de pallier leurs effets. Aussi, protégera-t-on les informations et les

ressources identifiées comme sensibles. Une politique de sécurité se développe selon trois axes : physique, administratif et logique. Le premier précise l'environnement physique du système à protéger (les éléments critiques, les mesures prises vis-à-vis du vol et des catastrophes) ; le deuxième décrit les procédures organisationnelles (répartition des tâches, séparation des pouvoirs) ; le troisième décrit les contrôles d'accès logiques (qui, quoi, quand, pourquoi, comment) et s'intéresse aux fonctions d'identification, d'authentification et d'autorisation de mettre en œuvre par le système informatique.

Un SICS relie des organisations multiples et des utilisateurs ayant des profils différents (professionnels de santé, patients, organismes sociaux), met en jeu des technologies complexes (communications, traitement, télémédecine, paiement, archivage), manipule des informations sensibles et hétérogènes (médicales, paramédicales, médico-administratives et médico-financières), etc. Indispensable pour gérer la dynamique et maîtriser les dépenses, le système informatique ne doit pas engendrer de dégradation de la sécurité. Au contraire, il doit empêcher l'exécution de toute opération non autorisée et protéger les informations sensibles.

L'analyse des risques permet la mise en œuvre d'une politique de sécurité en identifiant les vulnérabilités résiduelles et en évaluant leurs impacts sur la sécurité du système.

Les couples menaces/vulnérabilité permettent d'identifier les risques auxquels peuvent être soumis les SICS. Par exemple : l'attribution des données d'un patient à un autre, l'utilisation non autorisée des données et des programmes (introduction de virus, destruction illégitime de données), les erreurs de saisie, etc. Le code de déontologie médicale et le code de santé publique sensibilisent les professionnels de santé aux risques liés au secret professionnel.

Les intrusions dans les SICS revêtent une importance primordiale. En effet, si les propriétés de sécurité sont violées :

- Le médecin risque de prendre des décisions portant préjudice aux patients,
- La valeur de l'information comme base de diagnostic est amoindrie,
- Un professionnel de santé appelé à justifier ses actions pourrait être dans l'incapacité d'utiliser les dossiers informatiques comme preuve.

Les risques identifiés ci-dessus justifient directement un besoin de confidentialité, d'intégrité, de disponibilité et d'auditabilité (DICA).

La confidentialité est à la fois liée au respect du secret professionnel des organismes de santé et à la vie privée des patients. En effet, il n'y a pas de traitement médical sans confiance, de confiance sans confidences et de confidences sans secret. Un médecin, par exemple, ne devrait diffuser que des données anonymes lorsqu'il utilise son expérience à des fins de publication scientifique.

L'intégrité peut être mise en cause par des manipulations erronées mais également par la perte de données, accidentelle ou délictueuse. Elle touche également à la validité des données saisies, en particulier, à l'éviction des collisions¹¹⁸ et des doublons¹¹⁹ lors de la création de pseudonymes.

¹¹⁸ Il y a collision lorsqu'à partir de données nominatives différentes, on génère un même pseudonyme (qui risque ainsi d'être alloué à deux personnes différentes).

¹¹⁹ Il y a doublon lorsque deux pseudonymes différents sont générés pour une même personne.

La disponibilité concerne à la fois le caractère d'urgence et la pérennité des données. Les ressources critiques (y compris les données et les services) doivent être disponibles aux utilisateurs autorisés, après un temps d'attente raisonnable, par exemple pour le médecin en cas d'urgence ou dans le cadre de la télémédecine. Par ailleurs, le règlement des archives hospitalières impose des délais de conservation très longs : 70 ans pour les dossiers de pédiatrie, de neurologie, de stomatologie et de maladies chroniques, durée illimitée lorsqu'il s'agit de maladies héréditaires.

De nombreuses propriétés de sécurité peuvent être définies en termes de confidentialité, d'intégrité et de disponibilité de l'information ou du service lui-même, ou encore de métadonnées¹²⁰ comme le moment de réalisation d'une action ou l'identité de la personne qui a réalisé une tâche.

L'auditabilité correspond ainsi à la disponibilité et à l'intégrité de métadonnées relatives à l'existence d'une action, à l'identité de la personne qui l'a réalisée, à l'instant de l'action. L'authenticité d'un message est équivalente à l'intégrité du contenu du message et de son origine. La non-répudiation correspond à la disponibilité et à l'intégrité de l'identité de l'émetteur, l'instant de l'émission/réception.

B. LES NORMES DE SECURITE DU DOSSIER MEDICAL PERSONNEL

Le cahier des clauses techniques particulières (CCTP) du 30 mars 2007, élaboré par le GIP-DMP à l'occasion du lancement de la consultation portant sur l'« hébergeur de référence » des dossiers médicaux personnels, décrit toutes les normes techniques requises et qui s'imposent à l'« hébergeur de référence »¹²¹.

En matière de confidentialité, le CCTP exige qu'aucun accès aux données ne puisse être réalisé en dehors des cas prévus par la loi. Cela impose :

- des règles d'identification des acteurs, patients et professionnels de santé ;
- le respect de la liste des professionnels de santé habilités par le patient, alimentée et gérée sur le portail d'accès unique ;
- le respect de la liste des masquages éventuels et de la liste des documents cachés ou détruits. Ainsi, il est requis que toute opération de destruction d'information ou de données sensibles soit assurée de façon sûre : les documents doivent être détruits avec les moyens appropriés (par exemple un déchiqueteur) ; les supports (disques, bandes...) doivent être effacés de manière sûre avant leur mise au rebut ou leur réutilisation.

Ces règles correspondent à des exigences strictes de maîtrise des accès du système et aux flux. L'objectif étant que seules les personnes habilitées puissent avoir accès aux données

¹²⁰ Métadonnée : mot composé du préfixe grec *meta*, indiquant l'auto-référence ; le mot signifie donc proprement « donnée de/à propos de donnée ». La métadonnée est une donnée servant à définir ou décrire une autre donnée quel que soit son support (papier ou électronique) ; <http://fr.wikipedia.org/wiki/M%C3%A9tadonn%C3%A9e>.

¹²¹ CCTP n°2007-303, du 27 mars 2007, élaboré par le GIP-DMP, accessible sur www.d-m-p.org au 15/07/2008.

médicales personnelles ou données techniques sensibles telles que les fichiers journaux ou le paramétrage de sécurité.

Il faut souligner que l'« hébergeur de référence » n'est pas responsable du système d'identification et d'authentification des patients et professionnels de santé. Cette responsabilité relève du portail unique d'accès. Mais l'« hébergeur de référence » reste responsable de la stricte application des privilèges (authentification et droits) transmises par le portail.

Le CCTP requiert, en outre, une totale intégrité des données et des traitements pour l'ensemble du DMP. Quelque soit le sinistre, résultant soit d'une action malveillante, d'une modification accidentelle ou non légitime, toute situation antérieure doit pouvoir être restaurée sans perte de données intègres. Aucune perte de donnée n'est tolérée à l'exception des sessions en cours lors d'un incident majeur. Ainsi, en cas d'incident majeur ayant pu donner lieu à une perte de session en cours, les utilisateurs doivent être informés de l'existence de l'incident.

L'intégrité d'une donnée suppose son imputabilité et le CCTP impose que toute action sur le DMP puisse être imputable à son auteur. A ce titre, doivent être conservés de manière intègre, les traces et preuves assurant la valeur probante de cette imputabilité. L'intégrité et l'imputabilité au sein du DMP sont assurées par l'usage de la signature électronique des données déposées, permettant ainsi leur contrôle et leur archivage, ainsi que la gestion de la preuve. La signature électronique (*digital signature*) est un procédé d'authentification de l'auteur d'un document. Elle doit d'une part être liée informatiquement au document qu'elle signe, et doit d'autre part identifier le signataire sans que celui-ci puisse répudier cette signature. Elle repose sur un système de chiffrement qui assure authentification, intégrité et durabilité¹²².

¹²² Exemple de procédé basé sur la méthode de chiffrement à clé publique RSA, la plus utilisée :

Bob souhaite signer un message adressé à Alice.

Bob calcule, par application d'une fonction de hachage, une empreinte $e(m)$ numérique du message m ; cette empreinte numérique est conçue de telle manière qu'il est très peu probable que deux messages différents puissent avoir la même empreinte numérique. Cette empreinte est usuellement de 160 bits.

Bob joint l'empreinte au message pour former un nouveau message $m1$.

Bob chiffre le message $m1$ avec sa clé privée qu'il est le seul à connaître, et obtient un message chiffré $M1$.

Bob chiffre ce message $M1$ avec la clé publique d'Alice et obtient un message chiffré $M2$ qu'il adresse à Alice.

Alice déchiffre le message $M2$ avec sa clé privée, qu'elle est la seule à connaître, et obtient ainsi le message $M1$. Alice déchiffre le message $M1$ avec la clé publique de Bob ; si elle obtient alors un message compréhensible, ce ne peut être que le message m signé de façon certaine par Bob, qui ne pourra pas renier sa signature.

L'existence d'algorithmes de signature électronique sûrs a permis de promulguer la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Cette loi stipule que l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Cas d'usage de la signature électronique par le système DMP

	PS¹²³ en version 1 du DMP	PS en version ultérieure du DMP	Patient en cas de dépose de données en version 1	Patient en cas de dépose de données en version 2
Signature des données électroniques par l'auteur	Non obligatoire	Obligatoire	Non obligatoire	Optionnel
Signature technique des données émises par le système émetteur	Non obligatoire	Non obligatoire	Sans objet	Sans objet
Signature des données reçues par l'hébergeur	Obligatoire	Obligatoire	Obligatoire	Obligatoire

Les échanges sur le réseau Internet entre les différents acteurs du DMP font l'objet d'un chiffrement¹²⁴. Sera également mis en œuvre la maîtrise des accès des acteurs métier (patients et professionnels de santé) afin de parer à toute modification non légitime. Cela passera notamment par l'utilisation d'authentification forte, de la gestion des privilèges.

Le CCTP impose que le service DMP et ses données associées soit disponibles 24 heures sur 24, 7 jours sur 7 pendant 365 jours par an. Le taux de disponibilité doit être de 99,9%, soit seulement 8 heures d'arrêts cumulés autorisés par an. En cas d'indisponibilité totale, celle-ci ne doit pas dépasser 4 heures consécutives.

Notons que, bien que le service DMP doive couvrir la métropole et les départements d'outre-mer (DOM), les mesures de disponibilité exigées par le CCTP ne sont mesurées que pour la métropole.

¹²³ PS : Professionnel de santé.

Les mesures de sécurité ne doivent en aucun cas être perturbées ou arrêtées, tant que les données n'ont pas été « sanctuarisées », c'est-à-dire protégées strictement en intégrité et confidentialité.

Le système sera considéré comme indisponible dans les cas suivants :

- L'usage du service est impossible du fait du défaut de fonctionnement d'une fourniture ou d'un service sous la responsabilité de l'hébergeur ;
- Les temps de réponse dépassent les temps de réponse acceptables ;

Selon le CCTP, « *dans le cas où des dispositions de bascule vers un site de secours seraient proposées, les mêmes exigences de disponibilité s'appliquent sur le site de secours* ». Il est assez étonnant que la formule choisie soit « dans le cas où », cela voudrait-il dire que le choix d'utiliser un système de bascule vers un site de secours soit laissé à l'appréciation de l'hébergeur ?

En effet, il serait étonnant que ne soient pas imposés les principes de la « haute disponibilité » (ou *high availability*, HA). La haute disponibilité permet à un site internet/à une application d'être disponible à 99,99% sur l'année. A cette fin, il faut jouer sur la performance :

- Eviter que la saturation du serveur (nombre maximum d'utilisateurs atteints, bande passante maximum atteinte, mémoire des serveurs saturées) ;
- Eviter qu'une panne n'entraîne une indisponibilité trop longue du service (remplacement des pièces, recouvrement des données).

Une mise en place idéale de la haute disponibilité consisterait :

- Tout d'abord, pour éviter la panne, à mettre en place cumulativement, ou tout au moins au choix :
 - Une redondance géographique (deux adresses physiques différentes) ;
 - Une redondance des réseaux pour accéder au serveur (routeur, réseau) ;
 - Une redondance des disques durs à l'intérieur de chaque serveur (en effet, le disque dur est la pièce la plus fragile). Le système le plus approprié dans ce cas est le RAID 5 ;
 - Sauvegarder des données en temps réel (système dit de « réplication » mis en place au niveau de la base de données) et en différé ;
 - Faire un historique des sauvegardes.

Ainsi, en cas de panne, on devrait pouvoir basculer sur le système de secours rapidement et, mieux, automatiquement.

- Ensuite, afin d'éviter la saturation du serveur :
 - Faire une répartition des applications (tâches) au sein du système (dit

« CLUSTER » ou « système de grappes ») : un serveur pour les e-mails, un serveur pour les pages web, un serveur pour la base de données ;

- Mettre en place des serveurs performants.

Le CCTP met en place un système de traçabilité de toutes les personnes agissant sur le DMP, notamment à travers des exigences d'auditabilité : toute action technique ou fonctionnelle doit être imputable à son auteur. En raison de la nature particulière des données du DMP, l'exactitude des données gérées pour le compte des patients et des professionnels de santé doit être assurée afin d'éviter toute erreur de diagnostic. L'hébergeur doit se ménager les moyens nécessaires à la lutte contre les actions malveillantes (fraude, intégration de code malicieux,...) et à la recherche de l'imputabilité de chaque opération réalisée sur le système à toutes les étapes du cycle de vie du projet.

Les exigences de disponibilité peuvent d'autant plus être remplies que le CCTP instaure un système de traçabilité non seulement des traces fonctionnelles mais aussi des traces techniques. Par traces fonctionnelles, il faut entendre les traces d'actions et de consultation du DMP réalisées par les patients et les professionnels de santé. Elles doivent être consultables en ligne par les patients et les professionnels qui en sont les auteurs.

Les traces techniques sont toutes les traces des actions assurées automatiquement par le système ou par les opérateurs techniques de celui-ci. Imputabilité et traçabilité conjointement permettent d'identifier et de localiser toute défaillance du système (volontaire ou non) et ainsi d'agir dans les plus brefs délais pour assurer la disponibilité requise.

La gestion de la preuve implique que les traces soient produites et conservées dans le temps dans des conditions garantissant leur intégrité donc leur valeur probante. Le portail comme l'hébergeur devront obéir à cette règle, car en effet, leur domaine de responsabilité est disjoint l'un de l'autre donc les traces qu'ils génèrent doivent être « autosuffisantes », autrement dit qu'il ne soit pas nécessaire de croiser les traces de l'hébergeur avec celles du portail pour reconstituer une opération.

En cas d'incident DICA (Disponibilité, Intégrité, Confidentialité, Auditabilité), le CCTP prévoit des pénalités.

§2 LES VULNERABILITES DU SYSTEME

D'aucuns disent que la plus grande vulnérabilité du système se trouve placée devant l'écran de l'ordinateur, en d'autres termes il s'agit de l'utilisateur. Ce type de risque est dénommé le « risque informatique » (A). Malgré les précautions prises lors des expérimentations, les failles de sécurité n'ont pas manqué (B).

A. LE « RISQUE INFORMATIQUE » OU GESTION DES RISQUES HUMAINS

« On qualifie généralement de risques informatiques, toutes les causes externes qui peuvent compromettre l'efficacité d'un système, à l'exclusion de toute anomalie fonctionnelle (panne machine, bug, erreur de programmation...).

On peut les répartir en deux catégories :

- les **risques logiques** : d'origine humaine. On peut citer les différents types de malveillances, venant du personnel, d'un voleur ou d'un hacker.
- les **risques physiques** : ils sont liés à l'environnement du système informatique (accès, bâtiments, fourniture électrique, climatisation...) »¹²⁵.

Il faut entendre ici tous les risques d'agressions des systèmes d'informations : notamment, l'intrusion dans le système par un tiers, l'introduction d'un virus. Ces risques peuvent provenir autant de l'extérieur que de l'intérieur, autrement dit d'un membre du personnel de l'entreprise.

Pour la suite du raisonnement, un travail de définition est nécessaire :

- Une attaque est une action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité ;
- Une intrusion est une faute opérationnelle résultant de l'exploitation d'une vulnérabilité dans le système ;
- Une menace est une violation potentielle d'une propriété de sécurité ;
- Une vulnérabilité est une faute accidentelle ou intentionnelle (avec ou sans volonté de nuire), introduite dans la spécification, la conception, la configuration ou dans l'opération du système.

Dans le cas du dossier médical personnel, les professionnels de santé, notamment les médecins libéraux, sont susceptibles d'être mal protégés contre ce type de risques. Alors que, la sécurité est au cœur du métier des hébergeurs de données de santé à caractère personnel qui, du fait de la gestion de données intimes et protégées par la loi « Informatique et Liberté », doivent pare à tout risque de perte de données.

Ainsi, les professionnels de santé, et surtout ceux exerçant au sein d'une petite structure, devront tenter de s'armer contre toute attaque de leur poste de travail, en premier lieu. Les postes de travail du personnel, devront impérativement être équipés d'un anti-virus, différent du logiciel de pare-feu, et à jour. En outre, ils devront être équipés d'un logiciel de détection et d'éradication des logiciels espions (appelés aussi « *spywares* ») également tenu à jour.

Parmi les *spywares*, le « *keylogger* » peut être fortement utile en matière

¹²⁵ Définition selon le dictionnaire [guideinformatique.com](http://www.guideinformatique.com/definition-risques_informatiques-1220.htm) : http://www.guideinformatique.com/definition-risques_informatiques-1220.htm au 13 août 2008.

d'authentification. Littéralement « *enregistreur de touches* », il s'agit d'un dispositif d'espionnage, chargé d'enregistrer, à l'insu de l'utilisateur les frappes de touches du clavier. Certains « *keyloggers* » sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

Dans la mesure où les « *keyloggers* » enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail. Les spywares s'installent généralement en même temps que d'autres logiciels et donc la principale difficulté est de les détecter. La meilleure façon de se protéger est encore de ne pas installer de logiciels dont on n'est pas certain de la provenance et de la fiabilité (notamment les freewares, les sharewares et plus particulièrement les logiciels d'échange de fichiers en Peer-to-Peer). Qui plus est, la désinstallation de ce type de logiciels ne supprime que rarement les spywares qui l'accompagnent.

Comme dans la pratique il est quasiment impossible de ne pas installer de logiciels, il est alors recommandé d'installer des logiciels, nommés **anti-spywares** permettant de détecter et de supprimer les fichiers, processus et entrées de la base de registres créés par des spywares. De plus, l'installation d'un pare-feu personnel peut permettre d'une part de détecter la présence d'espioniciels, d'autre part de les empêcher d'accéder à Internet (donc de transmettre les informations collectées).

L'autre pendant de ce système de protection concerne le contrôle d'accès physique aux postes de travail du personnel. Cet accès doit être protégé, au minimum par un mot de passe. Aussi élaborées que soient les protections logiques d'un ordinateur, elles peuvent être défaits si l'attaquant a accès physiquement à la machine. Si les contrôles d'accès logiques ont déjà été faits (machine déjà démarrée, déjà connectée au réseau par son utilisateur légitime), et que l'ordinateur est laissé sans surveillance, l'intrus n'a même plus besoin de les contourner ces protections logiques.

Il est également recommandé que le personnel utilise des mots de passe forts et les change régulièrement. Un mot de passe de cinq caractères peut être deviné en quelques secondes, un mot de passe qui figure dans un dictionnaire, même long, est également vulnérable (attaques « dictionnaire »). Le mot de passe doit comporter au moins huit caractères, lettres, chiffres et caractères spéciaux (ponctuation, parenthèses etc.). Ce mot de passe doit être facile à mémoriser et si on l'écrit, parce qu'on craint de l'oublier, il doit être conservé en lieu sûr : il est imprudent de l'écrire sur un « post-it » collé sous le clavier. Enfin, il est prudent d'en confier une copie à une personne de confiance, dans une enveloppe scellée, pour qu'en l'absence du titulaire du poste les personnes autorisées puissent néanmoins y accéder en cas de besoin légitime.

Enfin supprimer les comptes utilisateur périmés : nettoyer complètement les disques des ordinateurs réformés ou, mieux, les détruire : ces disques contiennent souvent des informations sensibles que l'on peut récupérer, même si les fichiers ont été supprimés des répertoires par logiciel ou si l'ordinateur est apparemment inutilisable. Synthétiquement, on peut émettre d'autres règles communes d'utilisation de l'informatique par le personnel de la collectivité :

- déconnexion ou au minimum verrouillage de l'économiseur d'écran avant de laisser l'ordinateur sans surveillance, même pour un bref instant ;

- rendre les employés responsables des ordinateurs portables qui leur sont confiés ;
- interdire l'utilisation personnelle et familiale de ces machines ;
- interdire l'utilisation d'ordinateurs personnels sur le réseau de l'entreprise ;
- règles d'utilisation d'internet (par exemple restrictions sur les sites accessibles, interdiction de participer aux forums depuis le poste professionnel...);
- responsabilité des employés en cas d'infraction aux règles.

En l'absence de ces règles élémentaires de protection des postes utilisateurs, les risques possibles sont notamment les suivants :

- Cheval de Troie: récupération d'adresse IP et de mots de passe ;
- Risque d'attaques par force brute car code secret choisi par le patient trop simple (4 chiffres) : « attaque dictionnaire » ;
- Attaque du serveur web: (vol de fichier, corruption de données, déni de service) ;
- Envoie du mdp par SMS: non sécurisé ;
- Ingénierie sociale: exploitation des vulnérabilités humaines (se faire passer pour le support au téléphone / intrusion physique) ;
- Traçage par les hébergeurs grâce à un outil de traçabilité (sous-programme du « contrôle Active-X » que le patient doit télécharger lors de l'accès au site de l'hébergeur) ;

Un des risques identifié par le rapport de novembre 2007, en conséquence du modèle d'hébergement, est de donner lieu à des pratiques contestables :

- La reconstitution par un hébergeur du profil de ses clients par le traçage de leur accès au DMP;
- Des stratégies de captation de clientèle entre hébergeurs, voire entre professionnels de santé, ou, à l'inverse, d'actions commerciales ou d'influence en direction des acteurs censées pouvoir orienter le choix du patient, parmi lesquels les médecins et les pharmaciens seront les plus exposés.

En effet, l'accès au site de l'hébergeur est subordonné au téléchargement d'un programme « contrôle Active-X » sur le poste du patient. Ce programme peut contenir, à l'insu du patient, un sous-programme qui va garder en mémoire la séquence des touches utilisées par l'internaute et, à la fin de la consultation, la renvoyer au serveur hébergeur. Sans

aller jusqu'à pirater les codes d'accès du patient, ce programme peut ensuite établir les statistiques de séquences, qui vont indiquer les « préférences » du patient et en déduire les zones du dossier les plus souvent consultées (donc ses sujets de préoccupations majeurs, sans avoir accès au contenu même du dossier).

S'ouvre alors la possibilité pour l'hébergeur d'adresser au patient des publicités ou incitations correspondant à ses préoccupations. Ces pratiques sont courantes mais pas qualifiées juridiquement : l'internaute a accepté le téléchargement du logiciel, avec un message d'avertissement, rédigé de manière à ce qu'il n'en comprenne pas le vrai sens.

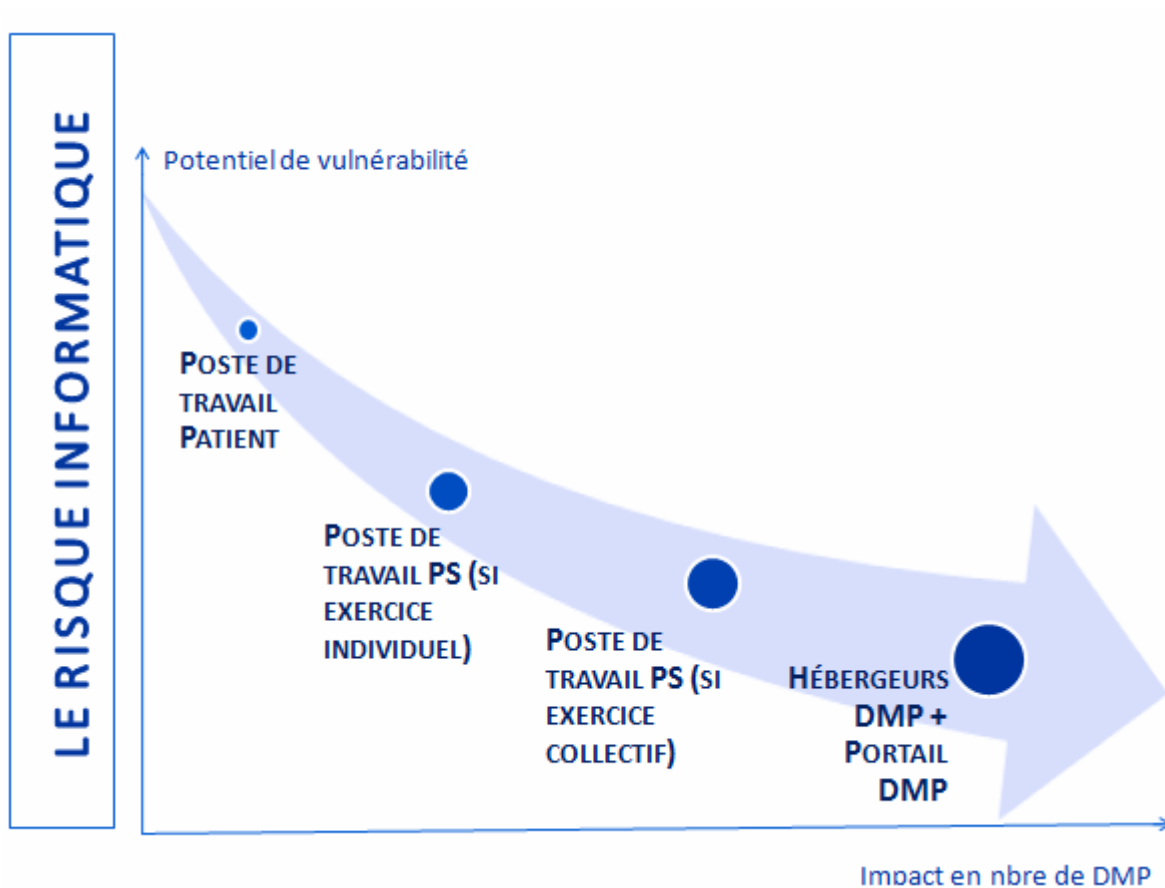
Le cahier des clauses techniques particulières (CCTP) élaboré par le GIP-DMP, évoque assez peu les risques humains de divulgation d'information et ne propose comme solution que des mesures de sensibilisation des personnels aux enjeux de la confidentialité et des sanctions y associées (violation du secret professionnel ou du principe de discrétion).

Quelques solutions, outre les règles élémentaires de protection, peuvent être conseillées :

- La protection des accès externes par des « passerelles d'accès sécurisés » ;
- La mutualisation des mécanismes d'authentification et éventuellement de gestion de session ;
- Des autorités d'enregistrement et de certification et opérateurs indépendants des parties ;
- Fonder la confiance réciproque en assurant l'imputabilité, la non-répudiation et l'auditabilité.

Face à ces différents risques, il existe un projet de mise à disposition en accès libre de bonnes pratiques aux patients. L'enregistrement non crypté des informations pour en faciliter la lecture par les ordinateurs personnels des patients ne peut que poser un problème de fond qui n'a pas encore été réellement abordé.

Enfin, il faut noter que, dans le cadre du DMP, plus le niveau potentiel de vulnérabilités augmente plus l'impact potentiel en nombre de DMP diminue, et inversement (cf schéma ci-dessous). Le niveau potentiel de vulnérabilités est élevé lorsqu'il ne concerne que le poste de travail d'un patient, qui n'a peut être pas mis en œuvre les précautions de sécurité de base ; ainsi, l'impact potentiel en nombre de DMP sera moindre, il ne concernera que le DMP du patient en cause.



B. LES ECHECS DE LA PHASE D'EXPERIMENTATION DU DOSSIER MEDICAL PERSONNEL

Pour mettre en place le dossier médical personnel sur l'ensemble du territoire français, le GIP-DMP a prévu deux phases successives : une phase d'expérimentation et une phase de généralisation.

La première phase a pour objectif de valider en grandeur réelle des éléments techniques, fonctionnels, organisationnels et médicaux du DMP, et notamment de :

- mesurer la qualité de service assurée par les hébergeurs,
- identifier les conditions d'appropriation de l'outil DMP par les acteurs,
- mettre en évidence l'impact du DMP sur les pratiques médicales,
- obtenir une évaluation de la satisfaction des acteurs,
- permettre la rédaction du cahier des charges de généralisation.

Initialement prévue sur la période d'avril à décembre 2006, cette première n'a pu vraiment débuter qu'à l'été 2006 faute d'hébergeurs agréés, notamment en raison de la publication tardive du décret « hébergeur » paru en janvier 2006. Trente mille dossiers de

patients devaient être traités pendant cette phase d'expérimentation et permettre, par son évaluation, d'éclairer les choix définitifs nécessaires à la seconde phase, la généralisation du DMP.

Suite à un appel d'offres, six consortiums d'industriels ont été retenus pour la phase d'expérimentation du DMP, qui s'est déroulé dans 13 régions de France sur 17 sites pilotes :

1. CEGEDIM-THALES avec 2 sites pilotes : Alsace et Aquitaine Nord ;
2. SANTEOS (à savoir Atos, Unimédecine, HP, Strateos et Cerner) avec 3 sites pilotes : Aquitaine Sud, Champagne et Picardie ;
3. SANTENERGIE (à savoir Siemens, Bull, EDS) avec 4 sites pilotes : Basse Normandie, Limousin, Midi-Pyrénées, Pays de Loire ;
4. INVITA – ACCENTURE - LA POSTE-NEUF CEGETEL - INTRA-CALL CENTER -JET MULTIMEDIA - SUN MICROSYSTEMS avec 3 sites pilotes : Haute Normandie, Ile de France (Paris Ouest) et Nord Pas De Calais ;
5. FRANCE TELECOM – IBM – CAP GEMENI – SNR avec 3 sites pilotes : Ile de France (Est), Languedoc Roussillon et Nord ;
6. D3P (à savoir RSS – Microsoft – Medcost) avec 2 sites pilotes : Rhône-Alpes (Annecy et Lyon)

La Cnil s'est prononcée le 21 mars 2006, conformément au code de la santé publique, sur les dossiers de demande d'agrément présentés par chaque hébergeur afin d'examiner « *les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité des données* ». Elle a ensuite autorisé les expérimentations sur zones géographiques¹²⁶, qui devaient s'achever fin août.

Chaque consortium devait développer cinq mille dossiers patients. Mille-cinq-cents professionnels de santé libéraux et une centaine d'établissements de santé y ont participé.

Pour le suivi opérationnel des expérimentations, le GIP-DMP a bénéficié d'une part, sur le plan technique, d'un *reporting* quantitatif hebdomadaire assuré par les hébergeurs, et d'autre part, par les correspondants du GIP-DMP dans les régions comportant des sites pilotes.

Des résultats de ces expérimentations, le GIP-DMP en a tiré des enseignements qualitatifs sur le plan fonctionnel, organisationnel et médical afin de guider ses actions d'optimisation du projet lors de la phase de généralisation du DMP :

- Fonctionnel : évaluation du fonctionnement du DMP et des services mis à disposition des professionnels de santé et des patients par les hébergeurs, notamment les modalités d'alimentation et de consultation du DMP ; les

¹²⁶ Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel.

conditions d'acceptabilité fonctionnelle du DMP ;

- Organisationnel : évaluation de l'efficacité de l'entité régionale du pilotage de l'expérimentation ; des moyens et outils ; de la mobilisation des acteurs en dehors des instances de pilotage ;
- Médical : évaluation de l'impact médical du DMP sur les pratiques des professionnels de santé et les relations entre eux ; sur la relation entre le patient et les professionnels de santé.

Les chiffres de la phase d'expérimentation¹²⁷ :

- 17 sites pilotes, dans 13 régions, ont participé à l'expérimentation ;
- 100 établissements de santé et 2 500 professionnels de santé ont été impliqués ;
- 38 200 DMP ont été ouverts, dont 67% par des établissements de soins,
- 5 000 dossiers étaient actifs à la fin de l'expérimentation, soit seulement 14% des dossiers ouverts, ils contenaient 4 à 6 documents, partagés par 1,16 professionnel de santé en moyenne.
- Parmi les participants aux expérimentations, le CHU Nord de Nantes a créé 349 dossiers, les Nouvelles Cliniques Nantaises 57 dossiers et la Clinique Jules Verne 7 dossiers, au 10 octobre 2006.

Côté patients :

- 84% d'entre eux sont satisfaits du DMP et 80% sont prêts à recommander à des proches d'ouvrir leur dossier ;
- 72% pensent bénéficier d'une meilleure coordination des soins grâce au DMP.

Côté professionnels :

- 66 % déclarent qu'ils ouvriront un DMP pour eux-mêmes ;
- 75 % des hospitaliers et 68 % des libéraux ont tout à fait ou assez confiance dans la sécurité et la confidentialité du DMP.

Les industriels ayant participé aux expérimentations :

- Cegedim et Thalès ;
- Réseau Santé Social, Microsoft et Medcost/Doctissimo, réunis au sein du consortium D3P ;
- France Télécom, IBM, Cap Gemini et SNR ;

¹²⁷Les chiffres clés du DMP, accessible sur http://www.d-m-p.org/index.php?option=com_content&task=view&id=49&Itemid=167, le 13 août 2008.

- In Vita, Aventure, la Poste, Neuf Cegetel, Intra Cell Center, Jet Multimedia et Sun Microsystems ;
- Siemens, Bull et EDS, réunis au sein du consortium Santé Énergie ;
- Atos, Unimédecine, HP, Strateos et Cerner, réunis au sein du consortium Santeos.

La phase d'expérimentation a révélé un certain nombre d'insuffisances relatives à la sécurité des données des dossiers médicaux personnels. Ce qui a fait vivement réagir la Cnil qui, suite à ses contrôles, a conclu que « *la courte durée d'expérimentation du DMP ne permet pas de mesurer son fonctionnement effectif et que les mesures de sécurité doivent être renforcées* »¹²⁸.

La Cnil a notamment constaté des carences dans la façon dont les identifiants et les mots de passe sont transmis par les hébergeurs ou les centres d'appel aux centres de soins et aux patients. Dans certains cas, ces échanges se font par voie électronique ne bénéficiant pas de « protection particulière ». Pire, des patients ayant oublié leur mot de passe se les ont faits communiquer par téléphone. Dans le même esprit, des centres d'appel n'ont pas mis en place des mesures d'identification-authentification des patients, en ne prévoyant notamment pas d'interrogation de ces derniers à partir de « questions défis » renseignées lors de leur inscription.

La Cnil relève également qu'une de ses recommandations n'a pas été suivie. Elle concerne l'obligation de chiffrement complet des bases de données, et pas seulement des canaux de communication.

Enfin, la Commission a relevé une faille de sécurité sur le site Internet de l'hébergeur Santénergie. Bien que résolue, cette faille permettait l'accès au DMP par le patient *via* un couple identifiant/mot de passe « identiques et facilement déductibles ». L'identifiant **et** le mot de passe étaient constitués des cinq premières lettres du nom + les deux premières lettres du prénom + le chiffre 1 ou 2 en cas d'homonyme.

Ex. : François DUPONT : identifiant = DUPONFR1 et mdp = DUPONFR1

¹²⁸ Cnil, Conclusions des missions de contrôles relatives à l'expérimentation du DMP, www.cnil.fr, consulté le

CONCLUSION

Le dossier médical personnel est sans conteste un dossier médical « personnel » et « professionnel », car en effet les deux adjectifs ne sont pas incompatibles ; et comme tout dossier médical, le DMP concilie ces deux critères.

Sa création et sa mise en œuvre ont suscité de nombreux débats au sein des associations de patients, mais aussi des représentants des professionnels de santé. Les échecs successifs, notamment le déploiement du DMP à la date du 1^{er} juillet 2007, y ont contribué.

Le cadre législatif reste encore incomplet, puisque le décret d'application du DMP et celui relatif à l'identifiant de santé ne sont toujours pas parus.

Enfin, dans sa dernière décision sur le dossier médical personnel, le CCNE est très réservé quant à un déploiement du DMP pour l'ensemble de la population française. Il recommande que le DMP ne s'applique qu'aux patients volontaires, « *atteints de maladies dont l'état nécessite l'intervention de nombreux professionnels sur le long cours* ». Il souhaite également que la généralisation éventuelle à l'échelle nationale, tout en concernant que les personnes volontaires, s'effectue seulement au bout d'une période de trois à cinq ans d'évaluation des résultats.

Le CCNE propose ici un DMP transfiguré ; un outil parmi d'autres pour une population de patients spécifiques et non l'outil devant révolutionner les systèmes d'information et de communication de santé.

Actuellement, la question qui se pose à propos du DMP est de savoir si une nouvelle version du DMP va prendre forme ou si les pouvoirs publics vont s'en tenir à la version initiale, déjà modifiée, du DMP conformément aux objectifs et ambitions affichés dès le commencement de cette vaste entreprise.

TABLE DES MATIÈRES

<i>Remerciements</i>	3
<i>Sommaire</i>	5
Chapitre introductif	6
§1 L'origine du dossier médical personnel	6
§2 Les objectifs du dossier médical personnel	7
§3 Le cadre légal du dossier médical personnel	8
Partie 1 Un projet ambitieux : l'amélioration de la prise en charge des patients	10
Chapitre 1 Un dossier médical partagé	11
Section 1 Une information partagée	11
§1 La nécessité d'une répartition efficace de l'information médicale	11
A. La prise en considération de nouveaux besoins	11
B. Continuité, coordination des soins et amélioration des techniques médicales	12
§2 Le contenu du dossier médical personnel	13
A. Des données à caractère personnel	13
B. Des données dites « sensibles »	15
Section 2 Une information protégée	17
§1 En tant qu'information d'un traitement automatisé	17
A. Le corpus juridique européen	17
B. La loi française « Informatique et Libertés »	20
§2 En tant qu'information de santé	21
A. Les lois relatives à la protection des malades et à l'assurance maladie	21
B. La règle du secret médical	23
Chapitre 2 Un dossier médical personnalisé	25
Section 1 Un patient au cœur de son dossier médical	25
§1 Le recueil du consentement du patient sur la collecte et le partage de ses données médicales	25
A. Un préalable à l'accès au dossier médical personnel	25
B. Le droit au « masquage » des informations médicales	27
§2 Les droits du patient à l'égard du dossier médical électronique	28
A. Des droits équivalents à ceux existant pour le dossier médical version papier	28
B. Les droits du patient spécifiques au DMP	29
Section 2 Le passage d'un dossier « partagé » à un dossier « personnalisé »	30
§1 Des conséquences juridiques	30
A. Quant au régime juridique du dossier médical personnel	31
B. Quant à la finalité du dossier médical personnel	32
§2 Des conséquences techniques	33
A. Un nécessaire renforcement de la sécurité	33
B. Le portail unique d'accès au dossier médical personnel : la « confiance numérique »	34

Partie 2 Un projet complexe	37
Chapitre 1 Des contraintes structurelles	38
Section 1 Une mise en œuvre malaisée	38
§1 Des retards récurrents	38
A. L'instabilité de la gouvernance	38
B. Un cadre législatif incomplet	39
§2 Des questions en suspens	41
A. Le choix du numéro d'identification de santé (NIS)	41
B. L'insuffisante interopérabilité des systèmes	43
Section 2 L'impact de l'outil informatique dans la relation médecin-patient	45
§1 L'impact sur le régime de responsabilité médicale	45
A. Aperçu du régime de responsabilité médicale	45
B. La responsabilité médicale à l'aune du dossier médical personnel	47
§2 La relation médecin – patient en cause	49
A. L'informatique comme obstacle au « colloque singulier »	49
B. L'informatique : entre maître de la relation médecin/patient	50
Chapitre 2 Des contraintes techniques	51
Section 1 Les standards de la sécurité informatique	51
§1 Un accès sous contrôle	51
A. Accès et identification des patients	51
B. Accès et identification des médecins	53
§2 Un modèle d'hébergement complexe	54
A. Les hébergeurs de données de santé à caractère personnel	54
B. L'hébergeur « de référence » et les hébergeurs « agréés »	55
Section 2 Les choix techniques du dossier médical personnel	58
§1 La sécurité des données du dossier médical personnel	58
A. Les modèles de sécurité pour le secteur de la santé	58
B. Les normes de sécurité du dossier médical personnel	60
§2 Les vulnérabilités du système	64
A. Le « risque informatique » ou gestion des risques humains	65
B. Les échecs de la phase d'expérimentation du dossier médical personnel	69
Conclusion	73
Table des matières	74
Bibliographie	76
Liste des abréviations	82
Annexes	83

BIBLIOGRAPHIE

Monographies

- ALLAERT François-André, DUCROT Henry, DUSSERE Liliane.** *L'information médicale, l'ordinateur et la loi*, 2^e édition, Cachan, Ed. médicales internationales, 1999, 256 p.
- BRAIBANT Guy.** *Données personnelles et société de l'information : transposition en droit de la directive n°95- 46 / Rapport au Premier Ministre*, Paris, la Documentation Française, 1998, 291 p.
- CADEAU Emmanuel, LE COZ Pierre, PEDROT Philippe.** *Dictionnaire de droit de la santé et de la biomédecine*, Paris, Ellipses, 2006, 476 p.
- CONTIS Maïalen.** *Secret médical et évolutions du système de santé*, Bordeaux, Les études Hospitalières, 2006, 853 p.
- KAYSER Pierre,** *La protection de la vie privée par le droit : protection du secret de la vie privée*, Paris, éd. Economica-PUAM, 3e éd, 1995, 605 p.
- LAUDE Anne, MATHIEU Bertrand, TABUTEAU Didier.** *Droit de la santé*, 1ère édition, Paris, PUF, 2007, 686 p.
- VACARIE Isabelle.** « *Le traitement informatique des données de santé, questions juridique et éthiques* », France, Université Paris I Panthéon-Sorbonne, Centre d'études et de recherches en santé et sécurité sociale (CEDRESS), 266 p.

Périmètres

- BESLAY Nathalie, FORGERON Jean-François.** « *La loi relative aux droits des malades : la consécration du droit de la santé électronique* », Gaz. Pal., 22-23 janvier 2003, p.4.
- CHABERT Catherine.** *Le dossier médical on line et le secret médical*, Gaz. Pal., 15-17 juillet 2001, p.25.
- DELPRAT Laurent.** « *Du secret médical au secret d'État... ou la justification d'une violation du secret médical par la protection de la liberté d'expression* », Médecine & Droit n°76, janvier-février 2006, pp. 1-10.
- FERAL-SCHUHL Christiane.** « *L'hébergement des données médicales numériques: un dispositif légal spécifique* », Le Quotidien du médecin, 6 mars 2003, p.37.
- FERAL-SCHUHL Christiane.** « *Les conditions d'accès au dossier médical: guide pratique* », Le quotidien du médecin, 10 mars 2005, p.44.
- FIESCHI Marius.** « *Vers le dossier médical personnel. Les données du patient partagées: un atout à ne pas gâcher pour faire évoluer le système de santé* », Droit social, n°1, janvier 2005, p.80-90.
- de LAMBERTERIE Isabelle.** « *Qu'est-ce qu'une donnée de santé ?* », RGDM, n° spécial 2004, p.11, spéc. p.13.
- « *Information mensuelle sur les marchés de la bio-santé* », BioSanté – Eurasanté, n°12, Février 2008.

Internet

Articles:

POIDEVIN Blandine. « *L'hébergement de données médicales* », www.village-justice.com, 8 décembre 2005, consulté le 3 juin 2008.

VADROT Dominique. « *Le Dossier médical personnel. Etat des lieux fin octobre 2004. Proposition d'une solution pour une installation rapide* », www.institutmontaigne.org, 25 octobre 2004, consulté le 17 juin 2008.

VERBIEST Thibault, WERY Etienne. « *Le dossier médical informatisé: la délicate protection des données personnelles* », www.droit-technologie.org, 16 mars 2005, consulté le 12 juin 2008.

VITENBERG Jacques. « *Le feuilleton de l'accès au dossier médical, commentaire de l'Arrêt du Conseil d'Etat du 26 septembre 2005* », www.village-justice.com, 15 juin 2007, consulté le 3 juin 2008.

Avis:

Cnil, délib. n°97-008, 4 févr. 1997, portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel, www.cnil.fr, consulté le 7 août 2008.

Cnil, délib., n°04-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie, www.cnil.fr, consulté 7 août 2008.

Cnil, Avis sur le dossier médical personnel, 12 juillet 2004, www.cnil.fr, consulté le 18 juin 2008.

Cnil, délib., n°2004-081, 9 nov. 2004, prise sur le fondement de l'article 8-III de la loi du 6 janvier 1978 portant autorisation d'une expérimentation présentée par la Fédération nationale de la Mutualité française ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques, www.cnil.fr, consulté le 15 juillet 2008.

Cnil, délib., n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel, www.cnil.fr, consulté le 15 juillet 2008.

Cnil, communiqué « *Quel identifiant pour le secteur de la santé ? La Cnil propose la création d'un numéro spécifique généré à partir du NIR mais anonymisé* », 20 février 2007, www.cnil.fr, consulté le 15 juillet 2008.

Cnil, Conclusions des missions de contrôles relatives à l'expérimentation du DMP, www.cnil.fr, consulté le 15 août 2008.

CCNE, avis sur les problèmes éthiques posés par l'informatisation de la prescription hospitalière et

du dossier du patient, Comité consultatif national d'éthique pour les sciences de la vie et de la santé, 16 février 2006, www.ccne-ethique.fr, consulté le 22 juillet 2008.

CCNE, avis n°104, Le « dossier médical personnel » et l'informatisation des données de santé, <http://www.ccne-ethique.fr>, consulté le 17 août 2008.

- *Rapports:*

DIONIS DU SEJOUR Jean, ETIENNE Jean-claude. *Nouvelles technologies de l'information et système de santé : la nouvelle révolution médicale*, rapport n°1686 Assemblée nationale- n°370, tome I, office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 21 juin 2004, www.assemblee-nationale.fr, consulté le 22 juillet 2008.

M. FIESCHI. *Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, Rapport au ministre de la Santé, de la Famille et des Personnes handicapées, janvier 2003, www.sante.gouv.fr, consulté le 22 juillet 2008.

TÜRK, Alex. *Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, n°367, Sénat, déposé le 19 mars 2003, www.senat.fr, le 22 juillet 2008 .

Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, <http://conventions.coe.int>, consulté le 18 juillet 2008.

Rapport d'activité 2006/2007 du GIP-DMP, accessible depuis www.d-m-p.org au 12 juin 2008.

Rapport sur le dossier médical personnalisé (DMP), Mission Interministérielle de revue de projet sur le DMP réunissant l'Inspection Générale des Finances, l'Inspection Générale des Affaires Sociales, le Conseil Général des Technologies de l'Information, déposé en novembre 2007.

Rapport d'information sur le dossier médical personnel déposé le 29 janvier 2008, Assemblée nationale-n°659, Commission des affaires culturelles, familiales et sociales, www.assemblee-nationale.fr

Commission des affaires culturelles, familiales et sociales de l'Assemblée nationale, Compte rendu n°48 du Mardi 17 juin 2008, Séance de 17 heures, accessible depuis <http://www.assemblee-nationale.fr/13/cr-cafc/07-08/c0708048.asp> au 17 août 2008.

Etude de la responsabilité liée à l'introduction du dossier médical personnel, <http://www.d-m-p.org/docs/DMPetudeResponsabilite2005.pdf>

- *Autres:*

Code de déontologie médicale, 2008, accessible depuis www.legifrance.gouv.fr au 19 juillet 2008.

CCTP n°2007-303, du 27 mars 2007, élaboré par le GIP-DMP, accessible sur www.d-m-p.org au 15/07/2008.

Les chiffres clés du DMP, www.d-m-p.org, le 18 juin 2007, consulté le 13 août 2008.

Dictionnaire, www.guideinformatique.com, consulté le 13 août 2008.

Législation

- *Lois:*

Loi n°78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°152, 2 juill., p.9559, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Loi n°94-548, 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°152, 2 juill., p.9559.

Loi n°2002-303, 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JO, 5 mars, p. 4118, texte n°1.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n°182, 7 août, p. 14063, texte n°2.

Loi n° 2004-810, 13 août 2004 relative à l'assurance maladie, JO n°190, 17 août, p.14598.

Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique (Titre résultant de la décision du Conseil constitutionnel n° 2007-546 DC du 25 janvier 2007), JO n°27, 1^{er} février, p.1937, texte n°1.

Loi n°2007-1786 de financement de la sécurité sociale pour 2008, du 19 décembre 2007, JORF n°0296, 21 déc., page 20603, texte n° 1.

- *Décrets et ordonnances*

Décret n°2005-1309, 20 octobre 2005, pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004, JO n°247, 22 oct. 2005, p. 16769, texte n°31, art. 38

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, JO n°286, 9 déc., page 18986 , texte n° 9.

Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JO n°4, 5 janv., p.174, texte n°14.

Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), JO n°113, 16 mai, p.9362, texte n°210.

- *Directives*

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, J.O.C.E n° L.281 du 23 novembre 1995, p. 31 à 50.

- *Codes*

Code de la santé publique, Edition Dalloz, 2008.

Code de sécurité sociale, Edition Dalloz, 2008.

Code pénal, Edition Dalloz, 2008.

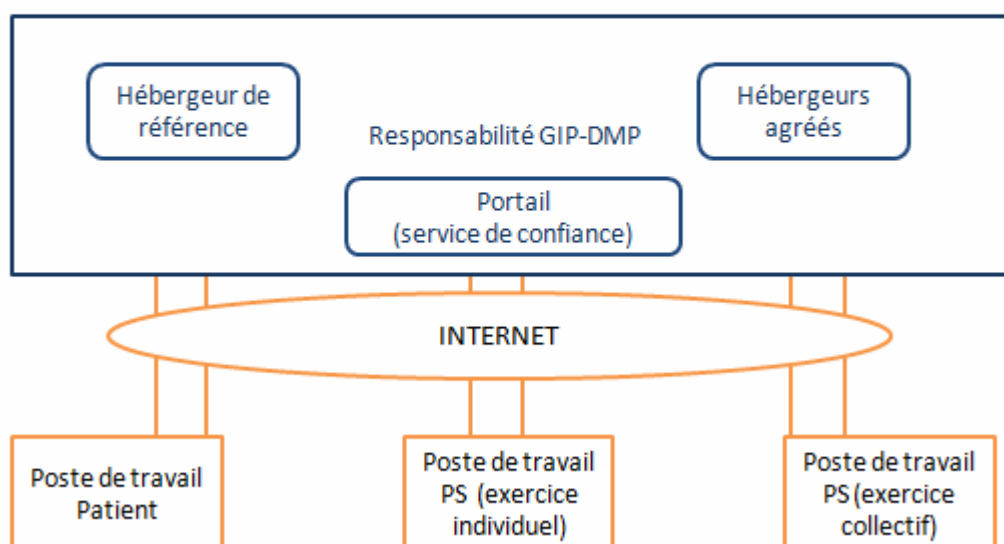
LISTE DES ABRÉVIATIONS

bull.	<i>bulletin</i>
bull.civ.	<i>Bulletin des arrêts de la Cour de cassation (chambres civiles)</i>
C.déont.	<i>Code de déontologie</i>
C.pén.	<i>Code pénal</i>
C. santé publ.	<i>Code de la santé publique</i>
Cass.1 ^{ère} civ.	<i>Cour de cassation, première chambre civile</i>
CCTP	<i>Cahier des clauses techniques particulières</i>
CE	<i>Conseil d'Etat</i>
CEDH	<i>Cour européenne des droits de l'homme</i>
CPS	<i>Carte de professionnel de santé</i>
CESDH	<i>Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales</i>
Cnil	<i>Commission nationale de l'informatique et des libertés</i>
Cnrs	<i>Centre national de la recherche scientifique</i>
comm.	<i>commentaire(s)</i>
Cons. const.	<i>Conseil constitutionnel</i>
CSS	<i>Code de la sécurité sociale</i>
D.	<i>décret</i>
D.	<i>Dalloz (Recueil)</i>
DCC	<i>Dossier communiquant de cancérologie</i>
DP	<i>Dossier pharmaceutique</i>
DMP	<i>dossier médical personnel</i>
décis.	<i>décision</i>
délib.	<i>délibération</i>
Dir.	<i>directive</i>
Dr. soc.	<i>Droit social</i>
éd.	<i>édition</i>
ex.	<i>exemple</i>
Gaz. Pal.	<i>Gazette du Palais</i>
GIP	<i>Groupement d'intérêt public</i>
JCP	<i>Juris-classeur périodique(La semaine juridique)</i>
JO	<i>Journal officiel</i>
JOUE	<i>Journal Officiel de l'Union Européenne</i>
L.	<i>loi</i>
NIR	<i>Numéro d'inscription au répertoire national d'identification des personnes physiques</i>
p.	<i>pages</i>
PIDCP	<i>Pacte international sur les droits civils et politiques</i>
PS	<i>professionnel de santé</i>
préc.	<i>Précité</i>
RGI	<i>Référentiel général d'interopérabilité</i>
RGS	<i>Référentiel général de sécurité</i>
rapp.	<i>Rapport</i>
s.	<i>suivants (et)</i>
SICS	<i>Systèmes d'information et de communication de santé</i>

ANNEXES

Annexe n° 1 : Le système DMP

Schéma organisationnel



Annexe n°2 :

L'échange d'informations entre PS et le Portail

