



DESS DMI

DESS Droit du Multimédia et de l'Informatique
Université Paris II

La mise en ligne des données de santé : le cas du dossier médical personnel

Mémoire de Raphaël Rault

Sous la direction de Madame le Professeur Agathe Lepage

Année universitaire 2004-2005

Chapitre introductif :	3
§1 : Historique du dossier médical	3
§2 : Les objectifs du Dossier médical personnel	4
§3 : Principaux textes s'appliquant au DMP	8
§4 : Grands principes du DMP	9
<u>1^{ère} PARTIE : UNE PLUS GRANDE IMPLICATION DU PATIENT</u>	11
Chapitre 1 : Le contenu du DMP	11
Section 1 : Des données protégées	11
§1 : Les données à caractère personnel	11
§2 : Les données de santé à caractère personnel : des données sensibles	14
Section 2 : L'exception au principe d'interdiction de la collecte et du traitement des données de santé à caractère personnel	17
§1 : La finalité comme exception au principe d'interdiction du traitement	17
§2 : L'intégration de la CNIL et des Ordres professionnels au processus	19
Chapitre 2 : Droits accordés au patient	23
Section 1 : Préalablement au traitement	23
§1 : Une information spécifique	23
§2 : La portée réduite du consentement du patient	26
Section 2 : Durant toute la durée de conservation	30
§1 : Droit d'accès au DMP	30
§2 : Droit de rectification des données contenues dans le DMP	35
<u>2^{ème} PARTIE : UNE PLUS GRANDE PROTECTION DU PATIENT</u>	37
Chapitre 1 : Quant au traitement de ses données de santé à caractère personnel	37
Section 1 : Les exigences de la loi informatique et libertés	37
§1 : La mise en œuvre du traitement	37
§2 : Nécessité d'un responsable du traitement identifié	41
Section 2 : Les solutions techniques requises	43
§1 : Obligation de sécurité	43
§2 : L'obligation de conservation des données	48
Chapitre 2 : Quant aux acteurs du traitement	51
Section 1 : Les professionnels de santé	51
§1 : Le secret médical au centre du DMP	51
§2 : Nouveaux risques ou dilution des responsabilités ?	54
Section 2 : L'hébergeur de données de santé à caractère personnel agréé	57
§1 : Les obligations de l'hébergeur	57
§2 : Les règles à venir	59
CONCLUSION	62
BIBLIOGRAPHIE	63
REMERCIEMENTS	66

Chapitre introductif :

« Il faudra de l'intelligence, du professionnalisme et beaucoup d'énergie. »¹

La mise en place du Dossier Médical Personnel (DMP) initié par la loi du 13 août 2004 relative à l'assurance maladie est un chantier colossal par la multiplicité d'acteurs qu'il fait intervenir et par les défis juridiques et techniques qu'il soulève.

D'où l'intérêt, ou l'inquiétude (et souvent les deux) de la population française quant à ce projet, la personne la plus concernée étant le patient, donc potentiellement plus de soixante millions de personnes !

Ce constat se retrouve sur l'internet, « miroir de la société », par exemple dans le nombre de réponses proposées par le moteur de recherches « Yahoo » pour une requête sur le « dossier médical personnel » : 3.340.000 !

Ce sont principalement les questions juridiques qui seront développées dans la présente tentative d'analyse du « phénomène DMP », ainsi que les questions pratiques et techniques qui s'y rattachent.

§1 : Historique du dossier médical

Les principes du dossier médical remontent aux livres d'observation médicale établis au IXe siècle par des médecins arabes tels que Rhazès (865-925), Avicenne (930-1037) ou Avenzoar (1073-1162).

Longtemps, le dossier médical a été la simple matérialisation d'un besoin du médecin qui, craignant la trahison de sa mémoire, conservait les notes personnelles qui lui permettaient de ne rien oublier de l'histoire de son patient. La relation entre le médecin et son patient était à cette époque duelle, il s'agissait de la « rencontre d'une conscience et d'une confiance ». La notion de partage dans ce dossier médical en devenir se limitait aux écrits échangés entre médecins ou avec les proches ou la famille du patient².

Les praticiens ayant par la suite découvert la fonction d'outil de communication que pouvait revêtir ce dossier médical, c'est au sein des hôpitaux que celui-ci a été défini. En effet, cela se justifiait par le fait que l'environnement hospitalier a vu naître la médecine plurielle, la création d'équipes soignantes, puis de réseaux de soins.

¹ M. Fieschi, au sujet du projet de mise en place du Dossier médical personnel, *Droit social*, n° 1, janvier 2005, p. 90

² C. Honnorat, « Apprentissage de l'exercice médical - Le Dossier Médical », Faculté de Médecine de Rennes, 25 octobre 2004

Seule la fonction administrative du dossier médical était initialement exploitée pour vérifier la réalité des soins et de l'intervention des soignants. Ainsi se sont développés de multiples dossiers tels que notamment le dossier de soins infirmiers et le dossier de transfusion.

Ces dossiers médicaux sont stockés par les différents intervenants du parcours de soins du patient : les hôpitaux, les médecins libéraux et les cliniques. Cette diversité d'hébergeurs posait le problème du suivi des différentes pathologies du patient et donc l'idée d'un dossier médical unique centralisant toutes les données s'est développée, dans le souci d'une meilleure gestion des prestations des différents professionnels de santé.

§2 : Les objectifs du Dossier médical personnel

L'utilité du développement de l'informatisation dans le domaine médical est évidente pour les pouvoirs publics. Pour preuve, la saisine pour avis par le Premier ministre du Conseil économique et social. Ainsi, parmi les recommandations faites par le Conseil économique et social dans son avis du 9 avril 2002 sur le développement des NTIC appliquées au secteur de la santé, dans le respect des droits de la personne et dans une perspective d'amélioration du système de soins³, figuraient huit axes d'action : mener à bien la diffusion des Nouvelles Technologies de l'Information et de la Communication dans le domaine de la santé, favoriser la coordination des acteurs de la santé, préserver la confidentialité du dossier médical, protéger et former l'utilisateur du système de santé, assurer la plus grande sécurité des outils d'information et de communication, accompagner les professionnels de santé, assurer l'égalité des usagers et des territoires et promouvoir la place et le rôle du secteur public.

La recherche d'économies est une donnée importante pour expliquer les objectifs du projet DMP. En effet, malgré les mesures prises par la loi de financement de la sécurité sociale pour 2004⁴ et en dépit du ralentissement du rythme d'augmentation des dépenses de santé, le déficit de l'assurance maladie s'est élevé à 13 milliards d'euros en 2004, soit plus de 10 % de ses ressources annuelles⁵.

Les objectifs fixés par la loi du 13 août 2004 relative à l'assurance maladie pour remédier à cette situation sont de trois ordres : engager une réforme profonde du système pour corriger des dysfonctionnements qui affectent tant les comptes de l'assurance maladie que la santé des assurés, rénover le pilotage du système dans son ensemble et assainir les finances sociales en clarifiant les flux financiers.

Cette loi propose deux dispositifs afin de fournir un « juste soin de qualité » sans donner le sentiment d'un rationnement purement comptable : le dossier médical personnel en ligne (DMP) et la mise en place du système du médecin traitant.

³ avis du CES « Santé et nouvelles technologies de l'information », *Notes d'Iéna*, n° 98, 9 avril 2002

⁴ Loi n° 2003-1199 du 18 Décembre 2003, *J.O.* n° 293 du 19 décembre 2003

⁵ Voir le dossier législatif consacré à la loi relative à l'assurance maladie, <http://www.senat.fr/dossierleg/pjl03-420.html>

S'agissant du contenu du DMP (sur lequel nous reviendrons), celui-ci prend la forme d'une base de données regroupant les données personnelles du patient afin d'optimiser les soins, dans un souci de respect de la confidentialité, tout le monde ayant à l'esprit les risques en termes d'introductions frauduleuses liés à l'hébergement de données sensibles sur le réseau internet. D'où les conditions strictes posées au choix de l'hébergeur en question.

Selon les sénateurs ayant soutenu le projet de loi, le recours au DMP se justifie principalement par le souci de mettre en place une meilleure efficacité des soins. Le coût présumé du DMP, grand inconnu, varie selon les différentes personnes interrogées sur le sujet (voir infra les estimations du Ministre de la santé) mais pourrait s'élever à un demi milliard d'euros. Cependant la mise en place de cet outil, en ce qu'il améliore le système de soins, permettra de réduire sensiblement les actes et prestations inutiles et de rentabiliser l'investissement initial. Les annonces d'économies attendues se sont arrêtées sur la somme de 3,5 milliards d'euros.

Afin de démontrer l'utilité économique de la mise en œuvre d'un système d'information centré sur le patient, le Professeur Marius Fieschi, auteur du rapport sur « Les données du patient partagées » remis au Ministre de la santé en mai 2003⁶, se réfère, dans une note de janvier 2005⁷, au rapport 2004 de l'Organisation de coopération et de développement économiques⁸ qui démontre que là où ils ont été mis en place, les systèmes de traitement de l'information ont eu un impact positif sur la qualité et le coût des soins.

La communication entre l'hôpital et la médecine de ville étant nécessaire à l'amélioration de la productivité et de la qualité des soins, l'OCDE propose d'améliorer la coordination entre ces deux acteurs par la mise en place de réseaux coordonnés et la création d'un dossier médical informatisé et partagé.

Les études réalisées sur le sujet, principalement américaines, mettent en évidence le fait que l'utilisation d'un système d'information adapté améliore la sécurité, la qualité et la continuité des soins. Ainsi le nombre d'erreurs peut être réduit, notamment dans le cas de la prescription médicamenteuse et de son administration.

Le Professeur Fieschi affirme que l'absence d'un dossier patient électronique représente un frein à la mise en place d'une plus grande implication du malade, souhaitable dans la prise en charge de sa santé.

Mais il faut prendre également en compte la complexité de la mise en œuvre d'un système d'information centré sur le patient, qui passe notamment par une adaptation des habitudes de travail des professionnels de santé à ce nouveau système et un développement de leur gestion informatique des dossiers médicaux. En effet, 85 % des cabinets médicaux disposent d'un ordinateur mais seulement 25 % des

⁶ Rapport Fieschi, « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », mai 2003, consultable sous : <http://www.sante.gouv.fr/html/actu/fieschi/sommaire.htm>

⁷ M. Fieschi, « 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

⁸ « Vers des systèmes de santé plus performants », rapport de l'OCDE 2004 adressé aux ministres de la Santé

médecins utilisent l'informatique pour gérer un dossier. Il ne faut pas imputer ces chiffres à la mauvaise volonté des professionnels de santé qui sont au contraire désireux de simplifier leur gestion des dossiers patients⁹ mais plutôt à l'absence d'un cadre clair et de lignes directrices précises en matière de développement de l'utilisation de l'informatique par ces professionnels. En effet, pour que le DMP soit pleinement utilisé par les professionnels de santé, il faut avant tout qu'il leur soit utile et que ceux-ci puissent y trouver aisément les éléments dont ils ont besoin pour leur pratique professionnelle. Les médecins généralistes évaluent à 5 ou 6 heures par semaine la perte de temps liée à la gestion des informations manquantes afin d'assurer la continuité et la coordination des soins de leurs patients. Le fait de disposer de ces informations manquantes dans le DMP constituera à l'évidence un facteur d'acceptabilité du projet. Celui-ci doit donc permettre un accès rapide et aisé par une ergonomie adaptée et ne pas être trop volumineux.

Les hôpitaux vont jouer un rôle clef car c'est notamment sur eux que repose la réussite de la mise en place du DMP. En effet, les établissements de santé seront amenés à exporter de grandes quantités de données sur le DMP des patients pris en charge. Cela s'explique par le fait que 60 % des actes médicaux et la quasi-totalité des interventions lourdes sont effectués par ces établissements. L'implantation du DMP dans les structures hospitalières va demander une rénovation des systèmes d'information hospitaliers (SIH) qui aujourd'hui se cantonnent trop souvent à des tâches administratives non centrées sur le patient. Cette rénovation risque de poser problème dans le calendrier annoncé pour le DMP car il semble qu'elle prendra plus de deux ans.

Le DMP permettra au médecin de prendre connaissance des éléments diagnostiques et thérapeutiques reportés par les autres professionnels de santé, de suivre le parcours de soins du malade et de prendre connaissance des éléments du compte-rendu de sortie en cas de séjour du patient dans un établissement de santé.

Le but est d'améliorer l'information des différents praticiens qui traitent un même patient, en permettant une meilleure connaissance et un meilleur suivi de l'historique médical de ce dernier, afin d'éviter les soins ou examens redondants.

Toute consultation d'un professionnel de santé et toutes les données médicales utiles pour appréhender le parcours de soins du patient seront consignées dans le DMP.

Il convient de souligner le fait que le niveau de prise en charge des actes et prestations de soins par l'Assurance maladie sera subordonné à l'autorisation donnée par le patient aux professionnels de santé d'accéder à son dossier et de le compléter. Ce point est considéré par certains comme faisant obstacle au libre consentement du patient, requis préalablement à l'établissement du DMP, et sera approfondi dans les développements qui vont suivre.

⁹ 85 % des médecins interrogés par l'IFOP le 27 septembre 2004 approuvent l'instauration d'un dossier médical personnel pour chaque assuré, consultable par le médecin ; <http://www.ifop.com/europe/sondages/opinionf/refassmaladie.asp>

Lors du Conseil des ministres du 12 janvier 2005¹⁰, le ministre des solidarités, de la santé et de la famille, Philippe Douste-Blazy (désormais ministre des affaires étrangères depuis le décret du 2 juin 2005 relatif à la composition du Gouvernement, et remplacé par Xavier Bertrand), a présenté une communication relative au Dossier médical personnel. Celui-ci commence par rappeler que « *Le dossier médical personnel constitue, avec la mise en place du médecin traitant, l'organisation du parcours de soins et le développement de référentiels médicaux, un volet important de la réforme de l'assurance maladie. Il permet une relation entre le médecin et le malade plus riche en informations qui vise à assurer une plus grande qualité, une coordination plus efficace et une meilleure régulation des soins.* »

Les principes directeurs de la mise en place du DMP sont ensuite énoncés : le médecin traitant aura un rôle pivot dans la gestion du dossier médical avec ses patients, le dossier médical sera avant tout un outil de travail pour les professions de santé, ce dossier bénéficiera d'une ergonomie simple pour le professionnel de santé comme pour le patient et sa sécurité, sa confidentialité et l'éthique de son utilisation seront garanties.

La maîtrise d'ouvrage du projet sera assurée par l'Etat et un groupement d'intérêt public a été nommé pour piloter le projet. L'arrêté constitutif de ce GIP nommé « groupement de préfiguration du dossier médical personnel » a été publié le 12 avril 2005¹¹. Selon cet arrêté, le GIP aura pour mission « *la préparation des dispositions permettant à l'organisme gestionnaire du dossier médical personnel (...) d'être opérationnel et d'assurer, de façon temporaire, la mise en oeuvre technique du dossier médical personnel, afin de mettre en oeuvre sans délai la loi du 13 août 2004 dans l'attente de l'installation d'une structure pérenne de gestion du dossier médical personnel* ». Sa mission prendra fin le 31 décembre 2005.

L'objectif du projet consiste à attribuer à chaque patient, à la mi-2007, un dossier ouvert complété progressivement et à en faire bénéficier les patients atteints d'une affection de longue durée (6,5 millions de personnes) dès le début de l'année 2007.

Pour illustrer les moyens mis en œuvre pour atteindre l'objectif annoncé, le ministre met en avant les tests effectués pour vérifier l'interopérabilité du DMP avec les logiciels installés dans les cabinets des praticiens libéraux et le serveur d'accès et de consultation du dossier mis en place dans chaque établissement hospitalier conformément au plan « Hôpital 2007 » dont les six sites pilotes seront choisis à l'issue d'un appel d'offres, ceux-ci devant être opérationnels à partir de septembre 2005.

Enfin, pour répondre aux critiques qui dénoncent le coût du DMP par rapport aux économies annoncées, le ministre tente de les rassurer en affirmant que le coût pesant sur les patients devrait rester inférieur à celui d'autres services d'usage courant comme la carte bancaire, le DMP devant par ailleurs contribuer significativement à la maîtrise médicalisée des dépenses de santé. Les initiatives de gestion dématérialisée de l'information médicale individuelle dans les autres pays

¹⁰

http://www.premier-ministre.gouv.fr/acteurs/gouvernement/conseils_ministres_35/conseil_ministres_12_janvier_441

¹¹ Arrêté du 11 avril 2005 portant approbation de la convention constitutive d'un groupement d'intérêt public, *J.O* n° 85 du 12 avril 2005, p. 6.547

européens sont également mises en avant pour justifier de l'utilité d'un tel projet en termes de qualité et d'efficience du système de santé français.

§3 : Principaux textes s'appliquant au DMP

L'informatisation du système de santé est un projet de longue date¹² dont le « Plan Juppé » de 1996¹³, aboutissant à l'adoption de trois ordonnances, a constitué une étape importante. Ces ordonnances ont été prises conformément à la loi du 30 décembre 1995¹⁴ autorisant le Gouvernement, par application de l'article 38 de la Constitution, à réformer la protection sociale, en vue d'améliorer par des indications et des modalités appropriées de mesure, de contrôle et de responsabilisation, la qualité des soins et la maîtrise des dépenses de santé. L'informatisation des données concernant les assurés sociaux a été la composante essentielle de cette réforme.

La loi du 4 mars 2002 relative aux droits des malades¹⁵ a par la suite consacré un « droit de la santé électronique » protecteur du patient, sous l'impulsion de la démocratisation des connaissances scientifiques et médicales d'une part et de la consécration du capital santé en tant que valeur fondamentale d'autre part¹⁶.

La notion de dossier médical partagé a été consacrée par cette loi du 4 mars 2002 mais la généralisation du dossier électronique partagé était restée au stade expérimental, faute de décret d'application concernant la mise en place d'«hébergeurs agréés» pour les dossiers de santé, et qui devrait être adopté cette année conformément aux dispositions de la loi du 13 août 2004.

C'est en août 2004 qu'a été institué le « Dossier médical personnel ».

En effet, l'article 3 de la loi du 13 août 2004 relative à l'assurance maladie¹⁷ insère une Section 5 intitulée « Dossier médical personnel » dans le Code de la santé publique.

Des décrets en Conseil d'Etat prévus par la loi du 13 août 2004 et indispensables à la mise en place du Dossier médical personnel n'ont cependant pas encore été adoptés¹⁸. Ils concernent : les règles de conservation et de transmission des

¹² Pour exemple : le rapport scientifique dirigé par Isabelle Vacarie intitulé *Le traitement informatique des données de santé – Questions juridiques et éthiques*, publié par l'université Paris I en 1988

¹³ Ordonnances n° 96-344, 96-345 et 96-346 du 24 avril 1996 dites « Plan Juppé », *J.O* n° 98 du 25 avril 1996

¹⁴ Loi n° 95-1348 du 30 décembre 1995, *J.O* n° 304 du 31 décembre 1995

¹⁵ Loi n° 2002-303 du 4 mars 2002 dite « loi Kouchner » relative aux droits des malades et à la qualité du système de santé, *J.O* n° 54 du 5 mars 2002 page 4.118

¹⁶ N. Beslay et J-F Forgeron, « La loi relative aux droits des malades : la consécration du droit de la santé électronique », *Gazette du Palais*, 22-23 janvier 2003, p. 4

¹⁷ Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *J.O* n° 190 du 17 août 2004, p. 14.598

¹⁸ Voir le rapport de l'Assemblée Nationale sur la mise en application de la loi du 13 août 2004, déposé le 23 mars 2005

informations médicales¹⁹, les conditions d'application de la section instituant le Dossier médical personnel²⁰ et enfin les conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et la tenue du Dossier médical personnel²¹.

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés²² modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004²³ apporte un cadre protecteur supplémentaire aux données visées par le DMP. Elle prévoit dans son premier article que l'informatique est au service des citoyens et qu' « *elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Elle est applicable aux données contenues dans le DMP en ce qu'elle s'applique « *aux traitements automatisés de données à caractère personnel* », aux termes de son article 2.

La loi du 6 août 2004 a transposé en droit interne la directive communautaire 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 données²⁴.

Les dispositions relatives à la signature électronique contenues dans la loi du 13 mars 2000²⁵ et le décret du 30 mars 2001²⁶ s'appliquent au DMP, ainsi que les dispositions portant sur l'activité d'hébergement et les moyens de cryptologie figurant dans la loi pour la confiance dans l'économie numérique du 21 juin 2004²⁷.

Des dispositions du Code de déontologie médicale²⁸, du Code pénal, du Code de la santé publique, du Code de la sécurité sociale et du Code civil²⁹ s'appliquent également au DMP.

§4 : Grands principes du DMP

Une Commission nationale permanente a été formée par le Conseil national de l'ordre des médecins afin d'établir un rapport sur les interrogations soulevées par la

¹⁹ Art. 2, I, al. 5

²⁰ Art. 3, I, al. 13

²¹ Art. 5, al. 1^{er}

²² Loi n° 78-17 du 6 janvier 1978, *J.O "Lois et Décrets"* du 7 janvier 1978, p. 227

²³ Loi n° 2004-801 du 6 août 2004, *J.O* n° 182 du 7 août 2004 page 14.063

²⁴ Directive 95/46/CE du Parlement européen et du Conseil, 24 octobre 1995, *JOCE* n° L 281 du 23 novembre 1995, p.31

²⁵ Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *J.O* n° 62 du 14 mars 2000, p. 3.968

²⁶ Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, *J.O* n° 77 du 31 mars 2001, p. 5.070

²⁷ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *J.O* n° 143 du 22 juin 2004, p. 11.168

²⁸ Inséré sous les articles R. 4127-1 à 112 du Code de la santé publique

²⁹ Notamment l'article 9 qui dispose que « Chacun a droit au respect de sa vie privée », principe énoncé par la Déclaration des Droits de l'Homme de 1789 et par l'article 8 de la Convention européenne des Droits de l'Homme de 1950

mise en place du DMP³⁰. Au sein des réflexions menées par ce groupe de travail, les « principes incontournables » du DMP ont été dégagés.

Tout d'abord trois principes essentiels sont énoncés.

La liberté, qui se traduit notamment par le consentement exprès du patient préalablement au traitement et le choix pour le professionnel de santé d'inscrire ou non des données dans le DMP.

La confidentialité, qui soulève le nécessaire encadrement de l'accès aux données du DMP.

La sécurité, qui sera développée plus loin par référence au concept de « coffre-fort électronique ».

Deux données complémentaires semblent importantes pour la Commission.

La traçabilité, qui conduit au choix d'un identifiant spécifique et pérenne pour le patient.

La collégialité et l'accès limité au dossier du patient, qui traduisent le fait que le DMP est également un dossier partagé entre tous les intervenants amenés à l'élaborer.

Une donnée fondamentale est enfin rappelée : l'interopérabilité, qui va justement permettre la communication du DMP entre ces différents intervenants.

Il ne s'agit pas ici d'effectuer une étude exhaustive des problèmes soulevés par le DMP, mais d'adopter une approche « informatique et libertés » en se concentrant sur les nouveaux risques et les solutions apportées ou à définir concernant la mise en ligne des données de santé à caractère personnel initiée par ce nouveau mode de centralisation et de communication des informations médicales qu'est le DMP. De plus il convient d'étudier l'articulation des règles issues de la législation informatique et libertés avec celles issues du droit médical.

³⁰ Projet de rapport, « Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données »

1^{ère} PARTIE : UNE PLUS GRANDE IMPLICATION DU PATIENT

La réforme de l'assurance maladie, et notamment le DMP, a pour but d'impliquer d'avantage le patient dans la prise en charge de sa santé, au besoin en exerçant ses droits (Chapitre 2) sur ses données contenues dans le DMP (Chapitre 1).

Chapitre 1 : Le contenu du DMP

Les données contenues dans le DMP sont protégées (Section 1) mais peuvent par exception faire l'objet d'un traitement (Section 2).

Section 1 : Des données protégées

§1 : Les données à caractère personnel

a) La loi informatique et libertés

À l'article 9 du Code civil, le législateur n'a pas précisé les informations qui relèvent de la vie privée et qui méritent protection. Dans la détermination du contenu de la vie privée, il y a une importance considérable de la doctrine et de la jurisprudence³¹ qui a progressivement précisé les informations relevant de la vie privée.

La loi informatique et libertés rappelle dans son article 1^{er} (non modifié par la loi du 6 août 2004) que 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 et publiques. Elle définit ensuite dans son article 2 les données à caractère personnel en ces termes :
« constitue une donnée à caractère personnel 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

³¹ Pour exemple, Cass. 1^{ère} civ., 9 décembre 2003, *Comm. Com. électr.*, mai 2004, p. 44 : le numéro de sécurité sociale et les références bancaires figurant sur des bulletins de paye reproduits dans un article de presse appartiennent à la vie privée et ne peuvent être révélés sans le consentement de l'intéressé.

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 ».

L'ancien article 4 de la loi de 1978 retenait la notion de « donnée nominative » dont elle donnait une définition fonctionnelle : il s'agissait de toute donnée permettant directement ou non l'identification d'une personne.

La définition apportée par la loi du 6 août 2004 paraît plus large que la définition initiale de 1978 mais en fait la CNIL a toujours eu une interprétation extensive de la notion de « donnée nominative » et même des données ne permettant d'identifier une personne que très indirectement étaient considérées comme nominatives donc dans les faits il n'y a pas eu d'élargissement de la loi³².

La définition de « donnée à caractère personnel » reprend celle de « donnée personnelle » de la directive européenne du 24 octobre 1995³³. Cependant, la directive visait l'ensemble des moyens susceptibles d'être « raisonnablement » mis en œuvre pour identifier une personne mais cet adjectif « raisonnablement » a été supprimé lors des discussions précédant l'adoption de la loi du 6 août 2004 afin de « prévenir des difficultés d'interprétation »³⁴. La loi informatique et libertés exclut donc de son champ d'application les données anonymisées rendant impossible l'identification de la personne visée.

La notion de « donnée à caractère personnel » est large et le rattachement direct ou indirect de cette 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.

La CNIL dispose d'un pouvoir d'appréciation dans la détermination de ce qui peut être qualifié de données à caractère personnel. Se prononçant par exemple sur les puces RFID (Radio Frequency Identification), la CNIL leur a attribuées le caractère de données personnelles car elle a estimé que ces technologies permettaient potentiellement le « profilage » des individus et faisaient peser sur eux un risque particulier comprenant notamment la traçabilité de leurs déplacements.

Dans une délibération visant des statistiques établies sur les interruptions volontaires de grossesse³⁵, la CNIL a retenu que les données transmises étaient indirectement nominatives et ainsi constituaient des données à caractère personnel. En effet, même si le nom de la patiente n'apparaissait pas, ces statistiques comportaient notamment des données médicales relatives aux antécédents de grossesse, à la date de l'intervention, à la durée de l'intervention, à la durée d'hospitalisation, aux complications postopératoires, à l'année et au lieu de naissance, à la nationalité, à la profession,...

³² Enseignement dirigé « Informatique, multimédia et protection des personnes », Gaël Kostic, DESS DMI, 2004-2005

³³ 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

³⁴ Voir le rapport du sénateur Alex Türk, 23 juin 2004, p. 20

³⁵ 10^e rapport de la CNIL, 1989, p. 182 et s., citée par Marie-Laure Laffaire, *Protection des données à caractère personnel*, Editions d'Organisation, 2005

Les données figurant dans le DMP sont-elles donc clairement définies comme des données à caractère personnel auxquelles la loi de 1978 serait applicable ? Pour répondre à cette question, il convient désormais de définir les données réellement contenues dans le DMP.

b) A la recherche d'une définition unitaire du dossier médical :

Faut-il distinguer la notion de « fichier » et de « dossier » ?

Le « fichier » fait l'objet de plusieurs définitions mais regroupe toujours deux éléments : un ensemble d'informations de même nature, cet ensemble étant organisé. La Chambre criminelle de la Cour de cassation dans son arrêt du 3 novembre 1987³⁶ opérait une distinction entre fichier et dossier et affirmait que seul le fichier pouvait faire l'objet d'un traitement visé dans la loi informatique et libertés, le dossier n'étant qu'un regroupement de fichiers qui échapperait à cette loi. Cette distinction artificielle n'était pas acceptable.

La directive du 24 octobre 1995 a apporté une définition légale du « fichier » qui est alors défini comme tout ensemble structuré de données, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. L'alinéa 4 de l'article 2 de la loi informatique et libertés définit le fichier de données à caractère personnel comme « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* ».

Mais quelle est la définition du dossier médical ?

Le dictionnaire Larousse donne deux définitions du « dossier » :

- ensemble de documents se rapportant à un même sujet, une même affaire ;
- chemise en carton léger dans laquelle sont groupés des documents se rapportant à un même sujet.

Le « dossier » est donc défini par son contenant ou son contenu. Néanmoins M. Fieschi, dans son rapport de 2003 précité, souligne que le dossier patient électronique permet de s'affranchir de la forme du contenant et du mode de rangement.

Le « dossier patient » ne serait pas une fin en soi résultant d'une fonctionnalité individualisable du système d'information mais le résultat des traitements de l'information nécessaires dans les différents processus médicaux et de soins.

La difficulté liée à la définition du dossier relève de ce que les différents acteurs du monde médical n'en attendent pas tous le même contenu et le même usage. Des

³⁶ Concernant un traitement effectué par une société de recouvrement de créances, les juges retiennent que « *les renseignements obtenus sur la solvabilité des personnes concernées figuraient dans leur dossier, mais non dans le traitement automatisé d'informations nominatives exploité par [cette société], ni dans aucun fichier* », Cass. crim., 3 novembre 1987, *Bulletin criminel* 1987, n° 382, p. 1.007

termes différents sont donc utilisés : dossier minimum, dossier médical, dossier du patient, dossier du service,...

Ces diverses appellations et définitions laissent aux professionnels de santé la libre appréciation du contenu du dossier médical et amènent à rattacher le dossier à une spécialité médicale plutôt qu'au patient lui-même.

Le caractère variable du contenu du dossier du patient, justement en fonction des patients, pousse certains à le définir non par son contenu mais par son rôle³⁷ (informations utiles et pertinentes dans un processus de diagnostique ou un processus de soins dans la communication entre professionnels) et ses finalités (recherche, analyse médico-économique,...). Il est nécessaire de s'intéresser au contenu de celui-ci.

En effet, le contenu du DMP est une source d'inquiétudes pour les patients mais également pour les professionnels de santé. Un psychiatre a par exemple déclaré qu'« un tel dossier qui suivra les personnes tout au long de leur existence risque de les stigmatiser durablement »³⁸.

Il convient dès lors, dans un souci de sécurité juridique, d'aboutir à une définition unitaire de ce dossier, chantier que met en place la loi du 13 août 2004.

§2 : Les données de santé à caractère personnel : des données sensibles

a) La loi du 13 août 2004

L'alinéa 1^{er} de l'article L. 161-36-1 du Code de la sécurité sociale introduit par l'article 3 de la loi du 13 août 2004 présente le Dossier médical personnel en ces termes :
« *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 [encadrant l'hébergement des données de santé à caractère personnel] 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*³⁹. »

Il convient dès lors de se reporter à l'article L. 1111-8 du Code de la santé publique introduit par la loi du 4 mars 2002 qui dispose que le DMP est constitué « des

³⁷ Voir la note de M. Fieschi, *Droit social*, précité

³⁸ Voir l'article de Catherine Petitnicolas, « L'inquiétude des psychiatres », *Le Figaro*, 22 juillet 2004

³⁹ Ce volet prévention est prévu conformément aux objectifs de prévention et d'éducation à la santé contenus dans la loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique, *J.O* du 11 août 2004, p. 14.277

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

Au surplus, l'alinéa 1^{er} de l'article L. 161-36-2 du Code de la sécurité sociale introduit par l'article 3 de la loi du 13 août 2004 détaille le contenu du Dossier médical personnel :

« Dans le respect des règles déontologiques qui lui sont applicables ainsi que des dispositions des articles L. 1110-4 [respect de la vie privée et du secret des informations des patients] et L. 1111-2 [droit à l'information du malade sur son état de santé] du code de la santé publique, et selon les modalités prévues à l'article L. 1111-8 [hébergement des données de santé] du même code, 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 charge. En outre, à l'occasion du séjour d'un patient, les professionnels de santé habilités des établissements de santé reportent sur le dossier médical personnel les principaux éléments résumés relatifs à ce séjour. »

Dans son intervention du 12 janvier 2005, Philippe Douste Blazy a précisé que le DMP comportait les éléments d'information essentiels du parcours de soins du patient : les comptes-rendus de séjour hospitaliers, les fiches de consultation et les prescriptions de médicaments ou d'examen ainsi que les résultats de ces derniers, les médicaments délivrés par le pharmacien et, le cas échéant, le protocole de soins associé à une affection de longue durée.

Très concrètement, l'Agence nationale d'accréditation et d'évaluation en santé (ANAES), remplacée par la Haute autorité de santé par la loi du 13 août 2004 a détaillé la structuration du dossier médical. Celui-ci se compose de la fiche d'identification, la fiche administrative, la fiche consultation et les fiches d'antécédents. Certaines données sont indispensables dans ces fiches. Dans la fiche d'identification doivent figurer : le nom complet actualisé, le sexe et la date de naissance ; dans la fiche administrative: l'adresse, le numéro de téléphone et la profession ; dans la fiche consultation : le nom du médecin, la date de la rencontre, la synthèse de la rencontre, les décisions prises ; dans les fiches d'antécédents : les antécédents personnels et familiaux, les allergies et intolérances médicamenteuses, les facteurs de risque et les vaccinations et autres actions de prévention.

A terme, il est également envisagé d'incorporer l'imagerie médicale dans le DMP.

A la lecture des dispositions de la loi informatique et libertés et de la loi du 13 août 2004 instituant le DMP, il est indéniable de constater que les données stockées sont des données à caractère personnel permettant l'identification du patient. Ces données entrent donc bien dans le champ d'application de la loi informatique et libertés.

Mais elles sont plus que des données « simplement » protégées car les données qui constituent le DMP sont des données de santé à caractère personnel auxquelles la loi informatique et libertés réserve un statut spécifique.

b) Le principe d'interdiction de leur collecte et de leur traitement

La loi du 6 août 2004 a modifié la loi de 1978 afin d'introduire le principe d'interdiction de la collecte et du traitement des données relatives à la santé et à la vie sexuelle.

Désormais, l'article 8 de la loi informatique et libertés dispose qu'il est interdit d'effectuer la collecte ou le traitement des données à caractère personnel qui font apparaître, directement ou indirectement, « *les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ».

Antérieurement à la loi du 6 août 2004, le consentement exprès de la personne concernée était nécessaire pour effectuer le traitement de ces données, mais à présent la loi prévoit un principe d'interdiction de leur collecte et leur traitement, conformément aux dispositions de la directive européenne du 24 octobre 1995.

Les données contenues dans le DMP sont des données relatives à la santé, l'article L. 1111-8 du Code de la santé publique visant expressément les « *données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* ». Ces données ne doivent donc pas en principe faire l'objet d'une collecte ou d'un traitement.

Ce principe d'interdiction s'explique par le caractère hautement personnel des données médicales.

Cependant, il suffit de continuer la lecture de l'article 8 de la loi informatique et libertés pour observer que des exceptions sont prévues à l'interdiction de la collecte et du traitement des données sensibles dont les données de santé à caractère personnel font partie.

En effet, l'article 8, II, 6° pose comme exception au principe de l'interdiction du traitement des données sensibles « *les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal* ».

Section 2 : L'exception au principe d'interdiction de la collecte et du traitement des données de santé à caractère personnel

§1 : La finalité comme exception au principe d'interdiction du traitement

a) La finalité du traitement de données à caractère personnel

« La pratique enseigne que le danger pour les libertés et la vie privée provient plus de l'objectif poursuivi par le détenteur des données que de leur nature ou contenu ; aussi le contrôle du respect de la finalité est essentiel »⁴⁰.

Reprenant les dispositions de l'article 8 de la directive du 24 octobre 1995, l'article 8, II de la loi informatique et libertés prévoit huit exceptions.

Les trois exceptions applicables à l'interdiction de traitement des données de santé sont les suivantes : la personne concernée (le patient) a donné son accord écrit ; le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée dans le cas où celle-ci se trouverait dans l'incapacité physique de donner son consentement ; le traitement est nécessaire dans le cadre thérapeutique : médecine préventive, diagnostics médicaux, administration de soins ou de traitements, gestion de services de santé agissant dans l'intérêt de la personne concernée (sous la surveillance d'un professionnel de santé).

Aux termes de l'article 8, III la CNIL peut autoriser, compte tenu de leur finalité, certaines catégories de traitements, lorsque les données sensibles visées sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la loi informatique et libertés par la CNIL.

L'article 8, IV dispose lui que ne sont pas soumis au principe de l'interdiction de traitement des données sensibles ceux qui sont justifiés par l'intérêt public et autorisés par la CNIL ou par décret en Conseil d'Etat après avis motivé et publié de la CNIL.

Sous le régime antérieur à la loi du 6 août 2004, les données sensibles ne pouvaient être collectées qu'avec le consentement exprès de la personne visée. Depuis, le principe d'interdiction est posé mais le consentement exprès figure en premier au titre des exceptions. Il convient toutefois de remarquer qu'il peut être fait exception à cette exception⁴¹ lorsque la loi dispose que l'interdiction ne peut être levée par le consentement. Par exemple, l'article L. 1141-1 du Code de la santé publique dispose

⁴⁰ Jean Frayssinet, *Informatique, fichiers et libertés*, Litec, 1992, p. 135

⁴¹ Principes et exceptions ont la vie dure en Droit !

que les entreprises et organismes qui proposent une garantie des risques d'invalidité ou de décès ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier de cette garantie, même si ceux-ci leur sont transmis par la personne concernée ou avec son accord.

L'article 6 de la loi informatique et libertés prévoit les conditions pesant sur le traitement de données à caractère personnel et notamment :

«elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ».

La finalité du traitement fait partie des mentions incluses dans les déclarations ou les demandes d'autorisations effectuées auprès de la CNIL par les responsables de traitements sur lesquels nous reviendrons plus loin.

Une lourde sanction pénale est prévue à l'article 226-21 du Code pénal introduit par la loi du 6 août 2004 en cas de détournement des données à caractère personnel de leur finalité déclarée : cinq ans d'emprisonnement et 300.000 euros d'amende.

b) La finalité du 13 août 2004

La finalité visée par la loi relative à l'assurance maladie est *« de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé ».*

C'est cette finalité qui va « sauver » le DMP et non le consentement exprès du patient, annihilé par l'alinéa 2 de l'article L. 161-36-2 du Code de la sécurité sociale inséré par l'article 3 de la loi du 13 août 2004 qui subordonne le niveau de prise en charge des soins prodigués au patient à l'autorisation d'accès à son DMP que donne celui-ci aux professionnels de santé auquel il a recours.

Dans son avis du 10 juin 2004 adopté après saisine sur le projet de loi relatif à l'assurance maladie et instituant le DMP, la CNIL se réfère à la première exception de la loi informatique et libertés en observant que le texte du projet de loi, par la référence qu'il contient aux dispositions de l'article L.1111-8 du Code de la santé publique, implique que la création du DMP repose sur le consentement exprès de la personne concernée. Néanmoins, dans la mesure où le niveau de prise en charge des actes et prestations est subordonné à l'accès du professionnel de santé au dossier, il apparaît que ce consentement n'est pas totalement libre.

Rappelant les termes de la directive du 24 octobre 1995 selon lesquels les Etats membres peuvent, sous réserve de garanties appropriées, prévoir par leur législation nationale, pour un motif d'intérêt public important, d'autres dérogations que celles prévues dans son article 8, la CNIL estime que les dispositions du projet de loi instituant le DMP 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, aux termes mêmes du projet de loi soumis à son avis, « 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.

La CNIL a par ailleurs rappelé dans son avis du 10 juin 2004 qu'aux termes mêmes des dispositions de l'article 8 de la directive précitée du 24 octobre 1995, la possibilité de dérogation est subordonnée à l'introduction de garanties appropriées.

Saisi d'un recours contre la loi relative à l'assurance maladie par plus de soixante députés, le Conseil constitutionnel a rendu une décision le 12 août 2004⁴². Les auteurs de la saisine soutenaient que la création du DMP portait atteinte au droit au respect de la vie privée et visaient l'article L. 161-36-2 (cité plus haut) pour affirmer que le législateur portait atteinte « au droit à la protection sociale garanti au titre du onzième alinéa du Préambule de la Constitution de 1946 », c'est-à-dire la protection de la santé.

S'appuyant sur les finalités du DMP, qui sont, d'une part, d'améliorer la qualité des soins, d'autre part, de réduire le déséquilibre financier de l'assurance maladie⁴³, et compte tenu de l'ensemble des garanties qui y sont apportées (notamment le secret médical et l'accès au DMP), les juges du Conseil constitutionnel ont considéré que le législateur avait opéré, entre les exigences constitutionnelles en cause, une conciliation qui n'apparaît pas manifestement déséquilibrée et que, dès lors, les griefs invoqués devaient être rejetés.

Les juges ont notamment justifié par la nécessité de favoriser la continuité de la mise à jour du contenu du DMP le fait de subordonner le niveau de prise en charge des soins à l'autorisation donnée par le patient aux professionnels de santé d'accéder à son DMP et de le compléter.

§2 : L'intégration de la CNIL et des Ordres professionnels au processus

a) Les recommandations de la CNIL :

Dès 1997, préoccupée par les questions soulevées par la mise en place de réseaux de transmission d'informations médicales nominatives entre différents intervenants du domaine médical (médecins, caisses de sécurité sociale, organismes de recherche médicale...), la CNIL a adopté une « recommandation de portée générale sur le traitement des données de santé à caractère personnel »⁴⁴ dans laquelle elle

⁴² Cons. Const., 12 août 2004, déc. n° 2004-504 DC, voir le commentaire de Jean-Eric Schoettl, « La réforme de l'assurance maladie devant le Conseil constitutionnel », *Petites affiches*, 15 septembre 2004, n° 185, p.6

⁴³ Une exigence constitutionnelle s'attache à l'équilibre financier de la sécurité sociale depuis la révision constitutionnelle du 22 février 1996, voir Cons. Const., 18 décembre 1997, déc. n° 97-393 DC, cons. 23

⁴⁴ Délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel

exige que des mesures de sécurité renforcées soient prises. Notamment elle souligne l'exigence du recours à des moyens de cryptologie autorisés par le Service central de la sécurité des systèmes d'information (SCSSI) et la mise en œuvre d'un dispositif de filtrage des accès. Par ailleurs, elle interdit formellement l'utilisation des données de prescription à des fins commerciales si ces informations permettent l'identification des personnes. Enfin, elle exige que les professionnels de santé garantissent l'anonymat des patients lors de transmissions de données vers un système d'information médicale.

Dans sa délibération du 8 mars 2001⁴⁵, la CNIL affirmait que les données de santé à caractère personnel, parce qu'elles relèvent de l'intimité de la vie privée, doivent faire l'objet d'une protection particulière, exigée tant par l'article 6 de la Convention n° 108 du Conseil de l'Europe⁴⁶ que par l'article 8 de la directive européenne du 24 octobre 1995. A cet égard la Commission réaffirme la pertinence de sa recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel : les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et à des fins de santé publique, dans les conditions définies par la loi.

Préalablement à l'adoption, le 13 août 2004, de la loi relative à l'assurance maladie, la CNIL avait été saisie pour avis par le Gouvernement du projet de loi et s'est prononcée, dans une délibération du 10 juin 2004, principalement sur les dispositions du texte visant le DMP. Elle s'est également prononcée sur la reconnaissance au bénéfice des professionnels de santé d'un accès en ligne, aux moyens de la carte vitale du patient et de leur carte de professionnel de santé, aux feuilles de soins.⁴⁷

La CNIL rappelle tout d'abord le droit des patients au respect de leur vie privée et au secret des informations les concernant issu de l'article L. 1110-4 du Code de la santé publique modifié par la loi du 4 mars 2002 sur les droits des malades. Elle énonce ensuite la justification de l'atteinte portée au consentement exprès du patient tirée du motif d'intérêt public important (voir supra).

Au titre de ses recommandations, la CNIL estime que la loi devrait être complétée par une mention particulière indiquant que les données susceptibles d'être portées dans le dossier médical personnel sont couvertes par le secret professionnel tel que celui-ci est défini par le code pénal et que quiconque aura obtenu ou tenté d'en obtenir la communication en violation des dispositions du présent article s'exposera à des sanctions pénales, de même que quiconque aura modifié ou tenté de modifier les informations portées sur ce même dossier.

Elle considère également que, l'utilisation du réseau internet pour permettre l'accès à ce dossier médical personnel entraîne des risques de divulgation des données, et ne peut donc être admise que dans la mesure où des normes de sécurité extrêmement strictes sont imposées tant aux professionnels de santé qu'aux organismes appelés

⁴⁵ Délibération n° 01-011 du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au publics

⁴⁶ Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 janvier 1981

⁴⁷ 25ème rapport d'activité de la CNIL, 2004 ; <http://www.ladocumentationfrancaise.fr/brp/notices/054000256.shtml>

à héberger les données, le principe de l'interdiction de toute commercialisation des données de santé directement ou indirectement nominatives devant être posé dans la loi.

b) Les recommandations des Ordres professionnels :

Jean Parrot, président du Conseil national de l'Ordre des pharmaciens, affirme que les pharmaciens sont prêts à être les « moteurs » de la réforme de l'assurance-maladie⁴⁸.

Plus précisément sur « l'ambitieux projet » du DMP, le volet pharmaceutique de ce dossier pourrait devenir opérationnel très vite, affirme-t-il. *« Il suffirait d'héberger, comme le permet la loi, les données présentes dans les ordinateurs de nos officines pour offrir une réelle lisibilité de toutes les dispensations de médicaments, qu'ils soient ou non présentés au remboursement. Cette lisibilité serait précieuse pour les prescripteurs. Elle le serait aussi entre nos confrères, pour leur permettre de jouer pleinement leur rôle de sécurité au moment de la dispensation ».*

Le Conseil national de l'Ordre des médecins est plus réservé sur la question. Selon les termes de la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie conclue le 12 janvier 2005⁴⁹ : *« la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie confie aux partenaires conventionnels l'organisation du suivi médical du patient, sur la base de son dossier médical personnel, tenu et géré par le médecin traitant qu'il a choisi ».*

Dans un communiqué de presse mis en ligne sur le site du Conseil national de l'Ordre des médecins le 28 juin 2004, ce dernier énonce les garanties qui doivent être apportées au DMP :

Le contenu du DMP ne doit pas empiler des données mais enregistrer les seules données médicales pertinentes nécessaires à la coordination, à la qualité, et à la continuité des soins, afin que celui-ci soit opérationnel pour les professionnels de santé.

Le consentement du patient doit être libre et éclairé, ce qui n'est pas le cas dans la loi mais justifié par un motif d'intérêt public important.

Le patient doit avoir la possibilité de s'opposer, pour des raisons légitimes, à l'enregistrement des données, ce qui sera étudié plus loin.

Certains organismes et principalement des organismes payeurs (organismes d'assurance, de capitalisation, de prévoyance,...) ne peuvent assumer le rôle d'hébergeur de données de santé à caractère personnel.

⁴⁸ « Jean Parrot prône le oui », Le quotidien du Pharmacien, 23 mai 2005

⁴⁹ Arrêté du 3 février 2005 portant approbation de la convention nationale des médecins généralistes et des médecins spécialistes

La responsabilité de tous les différents intervenants du DMP (les hébergeurs, les opérateurs de télécommunication, comme les caisses d'assurance maladie qui diffusent les cartes support du DMP) en cas de rupture de la confidentialité pouvant porter atteinte à l'intimité des personnes.

Il convient également de citer la Commission nationale paritaire formée par le Conseil national des médecins et préparant un rapport intitulé « Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données ». Cette commission réfléchit notamment sur les questions pratiques, éthiques et juridiques soulevées par le DMP.

c) Impact de ces recommandations dans la loi du 13 août 2004 :

Le législateur a pris en compte les recommandations émises par la CNIL et les instances ordinales en insérant tout d'abord des dispositions spécifiques, et en soumettant l'adoption des décrets d'application relatifs à la mise en place du DMP à leur accord.

Suite à l'avis de la CNIL sur le projet de loi, l'article 4 de la loi du 13 août 2004 complète l'article L. 1111-8 du code de la santé publique d'un alinéa ainsi rédigé :
« 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. »

De plus, le nouvel article L. 161-36-1 rappelle le respect du secret médical, protection nécessaire à la mise en place du DMP.

L'article 5 de la loi du 13 août 2004 implique la CNIL dans la mise en place de normes de sécurité qui étaient un préalable obligatoire à l'utilisation du réseau internet selon la Commission :

« 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. »

Le nouvel article L. 161-36-4 du Code de la sécurité sociale introduit par l'article 3 de la loi du 13 août 2004 implique la CNIL et les instances ordinales des professionnels de santé dans le processus de mise en place du DMP en disposant que : *« 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 ainsi que du conseil supérieur des professions paramédicales, fixe les conditions d'application de la présente section et notamment les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel. »*

L'article L. 162-1-14 du Code de la sécurité sociale introduit par l'article 23 de la loi du 13 août 2004 rappelle par ailleurs les attributions disciplinaires dont disposent les instances ordinales :

« L'inobservation des règles du présent code par les professionnels de santé, les établissements de santé, les employeurs ou les assurés, ayant abouti à une demande de remboursement ou de prise en charge ou à un remboursement ou à une prise en charge indus ainsi que le refus par les professionnels de santé de reporter dans le dossier médical personnel les éléments issus de chaque acte ou consultation peuvent faire l'objet d'une pénalité prononcée par le directeur de l'organisme local d'assurance maladie, après avis d'une commission composée et constituée au sein du conseil de cet organisme. **Lorsque la pénalité envisagée concerne un professionnel de santé, des représentants de la même profession participent à la commission** ».

Chapitre 2 : Droits accordés au patient

Le patient dispose de droits concernant ses données de santé faisant l'objet d'un traitement. Il peut exercer ces droits préalablement au traitement (Section 1) ou à tout moment durant son parcours de soins (Section 2).

Section 1 : Préalablement au traitement

§1 : Une information spécifique

a) L'information sur le traitement de données

L'article 32 de la loi informatique et libertés prévoit pour la personne concernée par le traitement de données à caractère personnel (dans le cas du DMP : le patient) un droit d'information.

Cette information porte sur l'identité du responsable du traitement, qui dans le cas du DMP n'a pas été encore clairement identifié, ce qui est problématique au regard des conditions de licéité du traitement que nous aborderons dans la deuxième partie de cette étude.

Le patient doit être informé de la finalité poursuivie par le traitement auquel ses données de santé à caractère personnel sont destinées. Cette finalité est aux termes de la loi du 13 août 2004 la « *coordination, la qualité et la continuité des soins* » (voir supra).

Le caractère obligatoire ou facultatif des réponses doit également être mentionné, ainsi que les conséquences éventuelles, à son égard, d'un défaut de réponse. Dans le cas où le patient n'accorderait pas au professionnel de santé l'accès à son DMP, les conséquences seront un remboursement plus faible de ses soins.

Les destinataires des données doivent être précisés. Ces destinataires sont définis à l'article 3 de la loi informatique et libertés : ce sont toutes les personnes habilitées à recevoir communication de ces données autres que le patient, le responsable du traitement, le sous-traitant, les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données, et les autorités légalement habilitées.

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

Il existe certaines hypothèses dans lesquelles le professionnel de santé est autorisé à communiquer les données de santé à caractère personnel du patient, sachant que cette communication doit être exercée avec prudence par le professionnel de santé car le recueil du consentement de son patient ne lui suffira pas à s'exonérer de son obligation de secret médical.

Les destinataires peuvent en être notamment l'équipe soignante, la sécurité sociale ou les autorités sanitaires.

La loi du 4 mars 2002 autorise expressément les professionnels de santé 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. Lorsque le malade est pris en charge par une équipe de soins dans un établissement de santé, les informations sont réputées confiées à l'ensemble de l'équipe.

L'article L. 161-29 du code de la sécurité sociale prévoit que les professionnels de santé communiquent, sous forme nominative, aux organismes d'assurance maladie obligatoire, le code détaillé des actes, prestations et pathologies diagnostiquées.

Enfin, aux termes de l'article L. 3113-1 du code de la santé publique, les professionnels de santé sont tenus de déclarer aux autorités sanitaires certaines maladies infectieuses qui nécessitent une intervention urgente (ex. : légionellose) ou dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique

Néanmoins, l'interdiction de la cession commerciale des données de santé à caractère personnel est posée au dernier alinéa de l'article L. 1111-8 du Code de la santé publique introduit par l'article 4 de la loi du 13 août 2004, et à l'article L. 4113-7 du Code de la santé publique.

La communication à des tiers autorisés des données de santé à caractère personnel du patient par le professionnel de santé est admise concernant les autorités judiciaires, les experts désignés et les agents de l'administration fiscale. Ne sont en revanche pas autorisés les médecins des compagnies d'assurance et les employeurs.

La suite de l'article 32 de la loi informatique et libertés prévoit également au titre de l'information de la personne concernée par le traitement de données à caractère personnel une information sur les droits dont elle dispose : droit d'opposition, droit d'accès et droit de rectification des données traitées.

Le patient devra également être informé du transfert de ses données à destination d'un Etat non membre de la Communauté européenne. Le projet de décret d'application de l'article L. 1111-8 du Code de la santé publique relatif à aux condition d'agrément des hébergeurs de données de santé à caractère personnel modifiant le Code la santé publique, issu de l'article 11, alinéa 34 de la loi du 4 mars 2002 et toujours en attente d'adoption prévoit d'insérer un article R. 1111-14 dans le CSP dont l'alinéa 2 dispose que l'activité d'hébergement devra être nécessairement fournie à partir d'un Etat membre de l'Union européenne, ou à tout le moins à partir d'un Etat offrant des garanties équivalentes à celles existantes en droit français en matière de protection des données sensibles et du secret médical.

Cette information « informatique et libertés » délivrée au patient doit s'articuler avec l'information prévue en droit médical.

La CNIL rappelle dans son avis du 10 juin 2004 l'absolue nécessité d'informer de façon claire le patient sur les modalités de constitution, de mise à jour, d'utilisation et de conservation des données de santé contenues dans le DMP, les conditions dans lesquelles le patient pourra accéder à ses données, ainsi que les modalités retenues pour l'identification et l'authentification (notamment le recours à la carte de professionnel de santé).

b) L'information du patient sur son état et sur les actes médicaux

L'article L. 1111-2 du CSP introduit par la loi du 4 mars 2002 et modifié par la loi du 13 août 2004 prévoit un droit général pour le patient à être informé par les professionnels de santé sur son état de santé et sur les soins qui lui sont proposés, sur leurs conséquences et les risques éventuels qu'ils comportent, ainsi que sur les solutions alternatives et sur les conséquences éventuelles d'un refus de sa part⁵⁰.

L'article 35 du Code de déontologie médicale⁵¹ dispose en outre que :

« le médecin doit à la personne qu'il examine, qu'il soigne ou qu'il conseille, une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il lui propose. Tout au long de la maladie, il tient compte de la personnalité du patient dans ses explications et veille à leur compréhension.

Toutefois, dans l'intérêt du malade et pour des raisons légitimes que le praticien apprécie en conscience, un malade peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic graves, sauf dans les cas où l'affection dont il est atteint expose les tiers à un risque de contamination.

Un pronostic fatal ne doit être révélé qu'avec circonspection, mais les proches doivent en être prévenus, sauf exception ou si le malade a préalablement interdit cette révélation ou désigné les tiers auxquels elle doit être faite ».

⁵⁰ Angelo Castelletta, *Responsabilité médicale – Droit des malades*, Dalloz, 2004, p. 16 et s.

⁵¹ art. R. 4127-35 du CSP

La jurisprudence a rappelé que ce devoir d'information trouve son fondement dans l'exigence de respect du principe constitutionnel de sauvegarde de la dignité de la personne humaine⁵². La Cour de cassation a également affirmé que le médecin qui est légalement ou contractuellement tenu d'une obligation particulière d'information doit rapporter la preuve de l'exécution de cette obligation⁵³.

Ainsi, aux termes de l'article L. 1111-2 du CSP, seules l'urgence ou l'impossibilité d'informer peuvent dispenser le professionnel de santé de cette obligation d'information, la charge de la preuve pesant sur ce dernier.

Néanmoins, la volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respectée, sauf lorsque des tiers sont exposés à un risque de transmission.

Cette information est due par tout établissement de santé et tout professionnel de santé.

Cette obligation cumulée d'information sur le traitement et sur l'état du patient et les actes médicaux pesant sur le professionnel de santé permet au patient d'exercer, en connaissance de cause, son droit d'opposition.

§2 : La portée réduite du consentement du patient

a) Le droit d'opposition du patient

Ce droit d'opposition préserve le droit à la vie privée, répondant ainsi notamment aux vœux de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 qui vise à « *garantir, sur le territoire de chaque partie, à toute personne physique, (...) le respect de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel le concernant* »⁵⁴.

L'article 38 de la loi informatique et libertés dispose que :

« *toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

⁵² Dans une espèce où la responsabilité du médecin a été retenue concernant le défaut d'information des risques d'un accouchement par voie basse en cas de présentation par le siège, Cass. 1^{ère} civ., 9 octobre 2001, *Bull. civ. I*, n° 249

⁵³ Défaut d'information sur les risques liés à une coloscopie, Cass. 1^{ère} civ., 25 février 1997, *Bull. civ. I*, n° 75

⁵⁴ Voir I. Vacarie, *Le traitement informatique des données de santé – Questions juridiques et éthiques*, Université Paris I, 1988

Ce droit d'opposition doit s'exercer sans frais à l'utilisation aux fins de prospection de ces données.

Les patients ont donc un droit de maîtrise et de contrôle sur la collecte et l'utilisation d'informations qui leur sont personnelles. Cette notion d'intérêt légitime n'étant cependant pas définie, elle reste soumise à l'appréciation du juge, qui ne sera pas aisée dans le domaine médical. Ainsi, cette absence de définition de l'intérêt légitime limite la mise en œuvre de son droit d'opposition par le patient.

Cependant, si la légitimité du motif est établie, passer outre à l'opposition de la personne expose aux peines définies à l'article 226-18-1 du Code pénal introduit par la loi du 6 août 2004, à savoir cinq ans d'emprisonnement et 300.000 euros d'amende.

L'ancien article 26 de la loi informatique et libertés prévoyait que le droit d'opposition n'était pas applicable aux traitements opérés « *pour le compte de l'Etat, d'un établissement public, ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public* ». Les patients admis dans les hôpitaux publics ne pouvaient donc s'opposer à l'enregistrement des données personnelles les concernant, puisque les traitements d'informations mis en œuvre dans ces établissements étaient soumis à la procédure de création par acte réglementaire pris après avis motivé de la CNIL. Cette dernière a cependant indiqué en 1992 dans son 13^e rapport que « *le droit d'opposition s'applique dans tous les cas, sauf mention contraire expressément portée dans l'acte réglementaire créant le traitement* ».

Cependant cette prise de position de la CNIL semblait à la fois aller à l'encontre de la loi de 1978 et à l'encontre de sa propre autorité en matière d'appréciation des risques pour les libertés individuelles, le traitement auquel elle reconnaît au patient le droit de s'opposer ayant reçu son aval⁵⁵.

L'article 38 de la loi informatique et libertés modifiée par la loi du 6 août 2004 ne fait donc plus référence à cette exception au droit d'opposition mais permet uniquement de l'écarter lorsque le traitement répond à une obligation légale ou qu'une disposition expresse de l'acte autorisant le traitement l'écartere.

Le refus d'inscription par le patient de données dans son DMP laisse uniquement la possibilité au professionnel de santé d'insérer une note personnelle dans son dossier professionnel (distinct du DMP).

b) Le consentement exprès du patient, corollaire du droit d'opposition

L'obligation d'obtenir le consentement de l'intéressé préalablement au traitement de ses données résulte non seulement de la législation en vigueur⁵⁶, mais également du

⁵⁵ Voir L. Dusserre, *L'information médicale – L'ordinateur et la loi*, Editions Médicales Internationales, 1996, p. 41

⁵⁶ Art. 226-19 du Code pénal : « *le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les*

fait que ces données revêtent le caractère d'attributs de la personnalité. Il a été écrit au sujet de l'information publique que : « *bien que la personne concernée ne soit pas « auteur » de l'information, au sens de la mise en forme, elle est le titulaire légitime de ses éléments. Leur lien avec l'individu est trop étroit pour qu'il puisse en être autrement. Quand l'objet des données est un sujet de droit, l'information est un attribut de la personnalité* »⁵⁷.

L'analyse selon laquelle les personnes seraient titulaires d'un droit de propriété sur leurs données doit donc être rejetée⁵⁸. Celle-ci avait trouvé un terrain propice avec les premiers modèles économiques issus de l'internet qui voulaient que l'on puisse céder ou « vendre » ses données personnelles en échange notamment de service gratuits. Cette théorie porterait exception au principe selon lequel l'information appartient à celui qui en réalise la collecte ou qui en assure la formulation car le droit de propriété serait attribué à la personne concernée par les données et non au détenteur de la base de données. Afin de rejeter cette théorie du droit de propriété sur les données personnelles, il convient d'analyser l'exercice des droits conférés à la personne par la législation : dans certains cas les données ne peuvent pas être modifiées par la personne concernée donc il n'a pas de libre disposition de ces données, élément nécessaire du droit de propriété. De plus, « *un droit de propriété peut être vendu mais les droits de l'homme ne peuvent jamais faire l'objet de transactions* »⁵⁹.

De façon très claire, et sous l'impulsion de la CNIL, les rédacteurs de la loi du 13 août 2004 ont complété l'article L. 1111-8 du Code de la santé publique d'un alinéa ainsi rédigé :

« *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* » qui dispose que « *le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende.* »

Les exceptions au droit d'opposition dans le cadre des données détenues par l'administration et encadrées par la loi informatique et libertés sont également là pour mettre à mal la reconnaissance d'un droit de propriété sur les données personnelles, la cession de celles-ci à l'administration n'étant pas purement discrétionnaire.

La communication de ces données doit donc résulter soit du consentement de l'intéressé, soit d'obligations législatives ou réglementaires, la théorie de

opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende »

⁵⁷ J-M Bruguière, *La diffusion de l'information publique : le service public face au marché de l'information*, thèse de doctorat soutenue le 23 juin 1995, université de Montpellier I

⁵⁸ Voir le Livre Blanc « Administration électronique et protection des données personnelles », *La Documentation Française*, 2002, p. 75

⁵⁹ M-J Radin, citée par Arnaud Belleil, *e-Privacy*, Dunod, 2001

l'autodétermination informationnelle assurant à l'individu le droit de décider de la communication et de l'emploi des informations relatives à sa personne.

La CNIL, dans son avis du 10 juin 2004, rappelle que dans le cadre de la consultation par le médecin de l'historique des remboursements détenus par l'organisme dont relève le patient, l'accord préalable de ce dernier sera obligatoire. En pratique cet accord se traduira par la mise à disposition au médecin par le patient de sa carte Vitale. La loi du 13 août 2004 prévoit qu'un identifiant peut être utilisé pour l'ouverture et la tenue du DMP dans l'intérêt du patient et à des fins de coordination des soins exclusivement.

L'alinéa 2 de l'article L. 161-36-2 du Code de la sécurité sociale jette un pavé dans la mare :

« Le niveau de prise en charge des actes et prestations de soins par l'assurance maladie prévu à l'article L. 322-2 est subordonné à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter. Le professionnel de santé est tenu d'indiquer, lors de l'établissement des documents nécessaires au remboursement ou à la prise en charge, s'il a été en mesure d'accéder au dossier. »

L'élément problématique dans l'obligation de recueil du consentement exprès du patient par le médecin préalablement à l'utilisation du DMP, réside donc dans le fait que le patient devra accepter que le médecin accède à son dossier personnel afin d'être complètement remboursé des soins qu'il sollicite. En effet, le professionnel de santé se doit d'attester, lors de l'établissement de la feuille de soins, qu'il a bien été en mesure de consulter le dossier. Ainsi, comme le retient la CNIL dans son avis, le consentement du patient est déterminé par un enjeu financier...

Interrogé sur la position de la CNIL concernant le projet de loi relatif à l'assurance maladie, François Bernard⁶⁰ a répondu que les dispositions conditionnant le niveau de remboursement des soins à l'accès au DMP par le professionnel de santé étaient justifiées par un motif d'intérêt public important : « 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 ayant pour but la sauvegarde de l'assurance maladie. Par ailleurs la CNIL rappelle que l'article 8 de la directive communautaire du 24 octobre 1995 subordonne la dérogation au principe selon lequel des données de santé ne peuvent être traitées sans le consentement du patient à l'introduction de garanties appropriées (voir supra).

Les professionnels de santé estiment qu'il est inconcevable du point de vue déontologique mais aussi juridique, compte tenu des engagements internationaux de la France en matière de respect à la vie privée, qu'un médecin puisse consulter ou compléter le dossier médical personnel sans le consentement du patient.

La modulation de la prise en charge par l'assurance maladie des actes et prestations de soins selon que le patient a, ou non, autorisé le professionnel de santé à accéder à ce dossier et à le compléter doit être assortie de garanties.

⁶⁰ Conseiller d'Etat honoraire, Commissaire en charge du secteur « santé »

Mais ces garanties resteront insuffisantes si le taux de modulation de la prise en charge retenue par l'Union nationale des caisses d'assurance maladie (UNCAM) entrave par son importance la liberté du patient et son accès aux soins.

Le Conseil national de l'Ordre des médecins, préalablement au vote du projet de loi sur l'assurance maladie, avait estimé qu'il relevait de la responsabilité du Parlement de fixer les limites de la réduction du niveau de prise en charge des soins, s'il décidait de maintenir cette disposition et qu'en aucun cas il ne pouvait déléguer cette responsabilité à un décret ou à une décision de l'UNCAM, mais cette recommandation n'a pas été suivie.

Les professionnels de santé sont « choqués » de la limitation du consentement du patient à l'accès du praticien au DMP car ils semblent raisonner par analogie avec le consentement du patient aux soins médicaux tiré de l'article L. 1111-4 CSP issu de la loi du 4 mars 2002 et qui dispose que :

« aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment ». Le consentement du patient revêt une grande importance dans la relation de confiance qui existe entre le patient et son médecin. Il est également important quant aux conséquences qu'il peut avoir sur la responsabilité du médecin à la suite d'actes médicaux.

Section 2 : Durant toute la durée de conservation

§1 : Droit d'accès au DMP

a) Le droit d'accès par le patient

Le droit d'accès par le patient aux données de santé à caractère personnel le concernant est reconnu aussi bien par la loi Kouchner du 4 mars 2002 que par la loi informatique et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004.

Aux termes de l'article 39, I de la loi informatique et libertés, un droit d'accès est réservé à toute personne physique justifiant de son identité et concernée par les données à caractère personnel collectées. Pour ce faire, celle-ci peut s'adresser directement au responsable du traitement ou au prestataire auquel la mise en œuvre du traitement automatisée a été confiée. A la réception de cette demande, le responsable du traitement est tenu de délivrer une copie des données mais peut subordonner cette délivrance au paiement d'une somme qui ne peut cependant excéder le coût de la reproduction.

L'article 43 de la loi informatique et libertés dispose que :

« lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique ».

L'article L. 1111-7 du Code de la santé publique introduit par l'article 11 de la loi du 4 mars 2002 et modifié par la loi du 22 avril 2005⁶¹ dispose que *« toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels et établissements de santé, qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé »*

Ces informations visent notamment les résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en oeuvre, 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.

L'article prévoit ensuite la demande d'accès direct ou par un intermédiaire, qui doit dans le cadre des données de santé à caractère personnel nécessairement être un médecin désigné à cet effet⁶². Un délai minimum de réflexion de quarante-huit heures pour la communication doit également être respecté.

Le droit d'accès a été complété par un décret du 29 avril 2002⁶³ et un arrêté du 5 mars 2004 qui homologue *« les recommandation de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès »*⁶⁴. Ce dernier constitue un guide pratique à l'usage de l'ensemble des professionnels de santé et des personnels des établissements de santé⁶⁵. Il rappelle que la demande d'accès ne répond à aucun formalisme particulier et qu'elle peut dès lors être orale. Cependant des précautions doivent être prises : il faut tout d'abord s'assurer de l'identité du demandeur, et de sa qualité à recevoir l'information. Il est recommandé ensuite d'accuser réception de la demande par tout moyen. Il faut préciser les frais d'accès au dossier et d'envoi du dossier. Enfin, l'accompagnement de l'accès au dossier doit être décrit.

La loi du 13 août 2004 fixant les conditions d'accès aux différentes catégories de données figurant au DMP devait compléter le droit à l'information médicale du patient sans s'y substituer.

⁶¹ Loi n°2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie, J.O n° 95 du 23 avril 2005, p. 7.089

⁶² Art. 43 de la loi informatique et libertés

⁶³ Décret n° 2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique, J.O n° 101 du 30 avril 2002, p. 7.790

⁶⁴ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, J.O n° 65 du 17 mars 2004, p. 5.206

⁶⁵ C. Féral-Schuhl, « Les conditions d'accès au dossier médical : guide pratique », *Le Quotidien du médecin*, 10 mars 2005, p. 44

b) Un droit d'accès limité au DMP

L'article L. 161-36-2 du Code de la sécurité sociale introduit par l'article 3 de la loi du 13 août 2004 dispose que sous réserve de respecter la vie privée et le secret des informations concernant le patient, et son droit à être informé sur son état de santé, « *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 charge. En outre, à l'occasion du séjour d'un patient, les professionnels de santé habilités des établissements de santé reportent sur le dossier médical personnel les principaux éléments résumés relatifs à ce séjour* ».

Selon le Conseil national de l'Ordre des médecins, cet article, par un renvoi au Code de la Santé publique, a réservé l'accès au dossier médical personnel aux seuls professionnels de santé et uniquement à l'occasion des actes de diagnostic, de soins ou de prévention et des consultations qu'ils prodiguent

Le partage du DMP entre les différentes spécialités médicales suppose qu'il permette un accès différent et personnalisé aux données selon le professionnel de santé concerné. L'accès différencié selon les spécialités médicales à cette information unique mais ubiquitaire est rendu possible par les techniques informatiques⁶⁶.

Dans son avis du 10 juin 2004 sur la loi relative à l'assurance maladie, la CNIL a abordé la question de l'accès au DMP. Elle a insisté sur le fait que ce droit d'accès s'exerce, concernant le professionnel de santé, dans le respect des règles déontologiques applicables et des dispositions du Code de la santé publique.

L'article L. 161-36-3 du Code de la sécurité sociale également introduit par l'article 3 de la loi du 13 août 2004 qu'il convient ici de reproduire entièrement malgré sa relative longueur pose des limites au droit d'accès par le professionnel de santé :

« *L'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus à l'article L. 161-36-2, même avec l'accord de la personne concernée.*

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

⁶⁶ M. Fieschi, « Vers le dossier médical personnel », *Droit social*, janvier 2005, p.80 et s.

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

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

Et l'article L. 161-36-4 du Code de la sécurité sociale de disposer :

« 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 ainsi que du conseil supérieur des professions paramédicales, fixe les conditions d'application de la présente section et notamment les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel. »

L'accès au DMP est donc interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. Ceci vise à éviter une potentielle technique de « scoring médical » des personnes par les assurances complémentaires de santé. Ainsi, l'accès du médecin conseil au dossier médical personnel est délicat. Investi de pouvoirs de contrôle, il ne fait pas partie des professionnels de santé qui ont accès au dossier médical personnel. Or un amendement déposé en ce sens par un parlementaire avait été rejeté par le Gouvernement et le ministre de la santé qui a évoqué la possibilité pour le contrôle médical d'avoir accès au dossier médical personnel, avec le consentement du patient.

L'accès au DMP est également proscrit dans le cadre de la médecine du travail. Pour les professionnels de santé, cette disposition démontre que l'indépendance du médecin du travail, vis-à-vis de l'employeur, n'est pas acquise dans notre société.

Tout manquement à ces dispositions est passible des sanctions pénales prévues à l'article 226-13 du Code pénal (voir supra).

La CNIL sera amenée à se prononcer sur les modalités d'accès aux différentes catégories d'informations contenues dans le DMP et sur les conditions dans lesquelles un identifiant pourra être utilisé pour l'ouverture et la tenue du DMP dans l'intérêt du patient et à des fins exclusives de coordination des soins.

c) De l'anonymisation des données :

Les procédés d'anonymisation des données ont depuis plusieurs années été conseillés par la CNIL dans le cadre des applications comportant des informations sensibles. Les données de santé faisant partie de cette catégorie, l'anonymisation des données est préconisée par la CNIL en cas de transmission de données à l'assurance maladie complémentaire. En effet, le détail des codes des médicaments inclus dans les feuilles de soins électroniques est nécessaire à l'assurance maladie obligatoire pour rembourser l'assuré. Mais ces codes sont susceptibles de renseigner

les caisses d'assurance maladie sur les pathologies des assurés. La loi n'autorise donc pas les organismes d'assurance maladie complémentaire à avoir accès à ces données. Mais cet accès pourrait permettre à ces organismes de mieux identifier les soins remboursés pour améliorer leur politique de tarification à l'égard de leurs assurés, personnaliser leurs garanties contractuelles et donc faire preuve de plus d'efficacité dans les dépenses de santé.

Afin de permettre cet accès par les organismes d'assurance maladie complémentaire, le rapport « Babusiaux » a été remis au ministre de la Santé en mai 2003⁶⁷ et préconise entre autres l'expérimentation d'un procédé de transmission anonyme des données de santé. Faisant application de ce rapport, la CNIL a autorisé, le 9 novembre 2004, pour une durée d'un an et pour des fins statistiques, la Fédération nationale de la mutualité française (FNMF) à effectuer le traitement sous forme anonymisée des codes des médicaments et des produits et prestations figurant sur les feuilles de soins électroniques pour le compte de ses mutuelles adhérentes volontaires. Ce traitement s'est effectué sur le fondement de l'article 8-III de la loi informatique et libertés. Concrètement le transfert de ces données est protégé par des moyens de cryptologie : les données sont chiffrées sur le poste du professionnel de santé par une clef fournie par le GIE SESAM Vitale et sont anonymisées de façon irréversible dès réception par la FNMF. La Direction centrale de la sécurité des systèmes d'information (DCSSI) est par ailleurs chargée par la CNIL d'évaluer cette procédure et de lui fournir un bilan de l'expérimentation.

d) Le statut des notes internes

Au sujet des notes gérées par le professionnel pour son propre usage, dont le statut semble devoir être précisé par le législateur, un rapport publié par l'Agence nationale d'accréditation et d'évaluation en santé (ANAES)⁶⁸ en février 2004 précise que : *« C'est dans la mesure où certaines des notes des professionnels de santé ne sont pas destinées à être conservées, réutilisées ou le cas échéant échangées, parce qu'elles ne peuvent contribuer à l'élaboration et au suivi du diagnostic et du traitement ou à une action de prévention, qu'elles peuvent être considérées comme « personnelles » et ne pas être communiquées : elles sont alors intransmissibles et inaccessibles à la personne concernée comme aux tiers, professionnels ou non ».*

Dans un rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques de juin 2004⁶⁹ est souligné au sujet de ces notes à usage interne la contradiction existant entre les différents textes encadrant l'accès du patient à son dossier et est rappelée en ces termes la priorité dont bénéficie la législation informatique et libertés : *« Si les notes, informations personnelles des médecins figurent sur un support informatique, la loi informatique et libertés de 1978 permet au*

⁶⁷ Rapport Babusiaux, « L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques », mai 2003, consultable sous : <http://www.sante.gouv.fr/html/actu/babusiaux/sommaire.htm>

⁶⁸ Remplacée par la « Haute autorité de santé » instituée par la loi du 13 août 2004

⁶⁹ Rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques sur les télécommunications de haut débit au service du système de santé du 22 juin 2004, disponible sous <http://www.assemblee-nationale.fr/12/rap-off/i1686-t1.asp>

malade d'en vérifier le contenu et, éventuellement d'en exiger des modifications, voire la destruction et de s'opposer à leur utilisation à des fins de recherche ».

La continuité du droit d'accès est le droit de rectification des données.

§2 : Droit de rectification des données contenues dans le DMP

a) Un droit de rectification limité

Ce droit est reconnu par l'article 40 de la loi informatique et libertés et permet à toute personne physique identifiée d'exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Postérieurement à cette demande, le responsable du traitement devra pouvoir justifier, sans frais pour le demandeur, qu'il a procédé auxdites opérations.

En cas de litige, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

L'article 40 poursuit en disposant que « *si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa* ». Il résulte des termes de cet article que pèse sur le responsable du traitement une obligation de moyen. En effet, celui-ci « *doit accomplir les diligences utiles* ». Cette obligation de moyen provient de l'article 12 de la directive du 24 octobre 1995, l'ancien article 38 de la loi informatique et libertés prévoyant une obligation de résultat.

De nombreuses interrogations subsistent sur la réalisation concrète de ce droit de rectification appliqué au DMP, quant à son étendue et à ses modalités.

b) La technique du masquage des données

L'article 10.3 de la recommandation n° R (97) 5 du 13 février 1997 relative à la protection des données médicales⁷⁰ souligne que si le patient le demande, ses données de santé doivent être effacées. Cependant il peut être dérogé à ce principe

⁷⁰ Recommandation n° R (97) 5 relatives à la protection des données médicales, adoptée par le comité des ministres du Conseil de l'Europe le 13 février 1997

si les données du patient sont rendues anonymes ou si des intérêts supérieurs et légitimes ou des obligations d'archivage s'opposent à l'effacement de ces données.

Les intérêts de la santé publique et de la science médicale sont notamment visés par la recommandation en tant qu'intérêts supérieurs ou légitimes.

Par conséquent, le masquage d'informations contenues dans le DMP est possible à la demande du patient. Cette donnée reste néanmoins dans le DMP mais sous un masque visible. Postérieurement, le patient pourrait prendre la décision de « baisser les masques ».

En effet, il paraît impensable selon les professionnels de santé de laisser la possibilité au patient d'effacer des données de son DMP.

Toujours selon les professionnels de santé, ce droit de rectification doit être considéré comme une décision grave qui nécessite une explication claire et précise du médecin avec le patient et effectuée par le médecin, en présence du patient.

De plus, il convient d'exclure la possibilité pour les différents professionnels de santé amenés à intervenir successivement sur le DMP dans le cadre du parcours de soins du patient, de se corriger entre eux.

Jean Dionis du Séjour⁷¹ considère pour sa part que le droit de rectification accordé au patient dans le cadre du DMP serait « redoutable ».

Dans la pratique, la mise en œuvre du droit de rectification risque donc d'être une source de conflits dans une relation de confiance entre le médecin et le patient⁷².

Après avoir observé l'orchestration de la législation « informatique et libertés » et de celle relative au droit médical, ainsi que la volonté du législateur, dans le cadre de la loi relative à l'assurance maladie, d'instaurer une plus grande implication du patient dans la prise en charge de sa santé, par l'exercice de ses droits « informatique et libertés », il convient désormais d'étudier les obligations pesant sur les acteurs du traitement.

⁷¹ Cité dans le projet de rapport de la Commission nationale paritaire DMP de l'Ordre des médecins

⁷² Voir T. Verbiest, « Le dossier médical informatisé : la délicate protection des données personnelles », 16 mars 2005, www.droit-technologie.org

2^{ème} PARTIE : UNE PLUS GRANDE PROTECTION DU PATIENT

Cette protection accrue du patient à l'égard du traitement de ses données de santé (Chapitre 1) passe par la responsabilisation des acteurs du traitement (Chapitre 2)

Chapitre 1 : Quant au traitement de ses données de santé à caractère personnel

La loi informatique et libertés pose des conditions à la licéité des traitements (Section 1), ces traitements étant effectués principalement par les professionnels de santé et les hébergeurs de données de santé à caractère personnel dans le cas du DMP (Section 2).

Section 1 : Les exigences de la loi informatique et libertés

§1 : La mise en œuvre du traitement

a) Conditions de licéité du traitement

La loi informatique et libertés définit de façon large le traitement de données à caractère personnel dans le but avoué d'accorder un champ d'application étendu à ses dispositions, les risques d'atteintes liées à ces traitement s'étant développés en parallèle avec le développement des technologies de l'information et de la communication.

L'article 2 prévoit donc que la loi est applicable aux traitements automatisés ou non de données à caractère personnel contenues ou appelées à figurer dans des fichiers. Par exception, la loi ne s'applique pas aux traitements mis en œuvre pour

l'exercice d'activités exclusivement personnelles, ce qui n'est pas le cas du traitement de données de santé prévu dans le cadre du DMP.

La loi du 6 août 2004 a ainsi mis fin à la distinction existant antérieurement entre les traitements automatisés ou non. De plus la référence à la notion de « fichier » met fin à la distinction (critiquée) opérée par la Cour de cassation⁷³ qui estimait qu'un ensemble de dossiers papier ne constituait pas un fichier. Ainsi l'alinéa 4 de l'article 2 dispose que « *constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* ».

L'article 2 définit en son alinéa 3 le traitement de données à caractère personnel comme « *toute opération ou tout ensemble d'opérations portant sur de telles données* » et énumère ensuite les principaux procédés qui peuvent être utilisés pour ce traitement : « *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* ».

Les conditions de licéité au traitement des données à caractère personnel, introduites par la loi du 6 août 2004, figurent aux articles 6 à 10.

L'article 6 énonce les conditions nécessaires au traitement des données à caractère personnel. Ces données doivent être collectées et traitées de manière loyale et licite, pour des finalités déterminées, explicites et légitimes, sans modification ultérieure incompatible avec ces finalités.

Les données doivent être exactes, complètes, et si nécessaire mises à jour. A défaut, le droit de rectification de la personne concernée par le traitement peut être exercé.

Enfin, ces données doivent être conservées sous une forme qui permet l'identification des personnes concernées par le traitement, la durée de conservation ne devant pas excéder la durée nécessaire à l'accomplissement des finalités pour lesquelles elles sont collectées et traitées.

L'article 7 rappelle par la suite la nécessité de recevoir le consentement exprès de la personne concernée, préalablement au traitement.

Les données de santé contenues dans le DMP étant considérées comme des données sensibles par la loi informatique et libertés, il est en principe interdit de les collecter ou de les traiter⁷⁴.

Il est fait exception à ce principe d'interdiction notamment lorsque la personne concernée a donné son consentement exprès (ce consentement n'étant pas libre et éclairé dans le cadre du DMP) et pour la sauvegarde de la vie de la personne concernée (cette exception trouvera à s'appliquer en cas d'urgence médicale,

⁷³ Cass. crim., 3 novembre 1987, *Bull. crim.*, 1987, n° 382, p. 1.007 (précité)

⁷⁴ art. 8, loi informatique et libertés (voir supra)

lorsque le consentement du patient ne pourra être recueilli par le professionnel de santé du fait par exemple de sa perte de conscience successive à un accident).

La CNIL et le Conseil constitutionnel, concernant le traitement prévu dans le cadre du DMP, ont retenu la finalité légitime directement issue de l'article 8, II, 6° qui vise « *les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal* ».

En effet, nous avons pu constater à plusieurs reprises dans notre étude que les dispositions de la loi du 13 août 2004 subordonnaient le niveau de prise en charge des soins au consentement que pouvait donner le patient au professionnel de santé d'accéder à son DMP⁷⁵ et que cela portait atteinte à un consentement libre et éclairé du patient mais était justifié 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 de la loi visant à sauvegarder l'assurance maladie⁷⁶.

Ainsi le traitement des données de santé à caractère personnel des patients prévu dans le cadre du DMP semble répondre également à l'article 8, IV de la loi informatique et libertés qui dispose que ne sont pas soumis au principe de l'interdiction de traitement des données sensibles ceux qui sont justifiés par l'intérêt public et autorisés par la CNIL ou autorisés par décret en Conseil d'Etat après avis motivé et publié de la CNIL.

b) La procédure de mise en œuvre du traitement

Antérieurement à la réforme de la loi informatique et libertés en 2004, tout traitement automatisé d'informations directement ou indirectement nominatives devait être déclaré à la CNIL. Mais ces traitements étaient différenciés et faisaient l'objet de formalités distinctes selon qu'ils relevaient du secteur public ou du secteur privé.

Ainsi, concernant la recherche médicale, les fichiers médicaux ayant pour fin le « suivi médical individuel des patients » réalisés « par les personnels assurant ce suivi et destinés à leur usage exclusif », restaient soumis à la procédure de principe de la loi de 1978, c'est-à-dire la déclaration à la CNIL.

⁷⁵ Art. L. 161-36-2, al. 2 du Code de la sécurité sociale, introduit par l'article 3 de la loi du 13 août 2004 et qui dispose : « *le niveau de prise en charge des actes et prestations de soins par l'assurance maladie prévu à l'article L. 322-2 est subordonné à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter. Le professionnel de santé est tenu d'indiquer, lors de l'établissement des documents nécessaires au remboursement ou à la prise en charge, s'il a été en mesure d'accéder au dossier* ».

⁷⁶ Voir l'avis de la CNIL du 10 juin 2004 et la décision du Conseil constitutionnel n° 2004-504 du 12 août 2004, précités

S'agissant des fichiers médicaux spécialement constitués et ayant « pour fin la recherche dans le domaine de la santé », ils devaient satisfaire aux dispositions de la loi du 1^{er} juillet 1994⁷⁷ et du décret d'application du 9 mai 1995⁷⁸.

Les traitements automatisés de données directement ou indirectement nominatives mis en œuvre dans les établissements de santé publics ou privés participant au service public entraient dans la catégorie des traitements relevant du secteur public, conformément à l'ancien article 15 de la loi informatique et libertés. Par conséquent, la charge de la demande d'avis auprès de la CNIL incombait à l'administration de l'établissement. Ces traitements devaient faire individuellement l'objet de cette procédure de demande d'avis si leurs finalités n'étaient pas identiques à celles de traitement qui avait été autorisé (contrairement à ce que pensaient certains médecins).

Les traitements automatisés de données nominatives dans le secteur public faisaient d'une manière générale l'objet d'un acte réglementaire élaboré par le responsable de l'établissement après avis motivé de la CNIL et ne devaient faire qu'exceptionnellement l'objet d'une autorisation législative prévue à l'ancien article 15 de la loi informatique et libertés⁷⁹.

Depuis la réforme de la loi du 6 janvier 1978 par la loi du 6 août 2004, la distinction entre les fichiers publics et privés est abandonnée. Désormais il faudra une autorisation de la CNIL pour tous les fichiers réputés les plus dangereux (c'est-à-dire portant sur des données sensibles).

Il existe désormais quatre types différents d'autorisations : une autorisation simple de la CNIL, un arrêté ministériel pris après avis motivé de la CNIL, un décret en Conseil d'Etat pris après avis de la CNIL ou une décision de l'organe délibérant d'une personne morale de droit public ou privé gérant un service public, prise après avis de la CNIL.

Le régime de déclaration prévu dans l'actuelle loi informatique et libertés doit être écarté pour le DMP car les données de santé qu'il contient sont des données sensibles, telles que les définit l'article 8 de la loi.

C'est donc le régime d'autorisation par acte réglementaire qui va désormais s'appliquer au traitement des données de santé visées dans le DMP.

L'article 26 de la loi prévoit que les traitements qui portent sur des données sensibles (les données de santé), sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié (avec le décret autorisant le traitement) de la CNIL.

⁷⁷ Loi n°94-548 du 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, *J.O* n° 152 du 2 juillet 1994, p. 9.559

⁷⁸ Décret n° 95-682 du 9 mai 1995 pris pour l'application du chapitre V bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifiant le décret n° 78-774 du 17 juillet 1978, *J.O* n° 110 du 11 mai 1995, p. 7.799

⁷⁹ Voir L. Dusserre, *L'information médicale, l'ordinateur et la loi*, Editions Médicales Internationales, 1996, p. 30

Cette obligation d'autorisation subordonnée à un décret en Conseil d'Etat est justifiée par la protection importante dont doivent bénéficier les données sensibles traitées de façon non anonymisées.

L'article L. 161-36-1, A, I, alinéa 4 prévoit ce régime d'autorisation renforcé : « *afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 est obligatoire* ».

Selon la CNIL, la méthode qu'elle adopte en matière d'autorisations est identique à celle qu'elle utilisait pour délivrer ses avis sur les traitements du secteur public sous l'ancien régime : un examen attentif des garanties mises en œuvre par le déclarant, au besoin renforcées, ne débouchant qu'exceptionnellement sur un avis défavorable. La CNIL n'estime pas qu'elle aura à recourir largement aux refus d'autorisation, de même que les avis défavorables sous le régime de l'ancienne loi de 1978 étaient l'exception. Par contre, l'autorisation peut n'être accordée que sous certaines conditions, définies par la CNIL. Ainsi, par exemple, l'autorisation peut être délivrée pour un temps déterminé et limité, ou encore sous la forme d'une expérimentation, avec nécessité de présentation d'un bilan au terme de ce délai.

De plus, il sera toujours possible à la CNIL de retirer son autorisation en cas de dysfonctionnement grave du traitement.

Ce dysfonctionnement peut résulter d'un manquement à ses obligations par le responsable du traitement.

§2 : Nécessité d'un responsable du traitement identifié

a) Difficulté d'identification du responsable du traitement pour le DMP

La loi informatique et libertés impose la désignation d'un responsable du traitement.

Ce responsable du traitement est défini à l'article 3 de la loi informatique et libertés comme « la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ». Il est fait exception à cette définition en cas de dispositions législatives ou réglementaires expresses, ce qui n'est pas le cas dans la loi du 13 août 2004.

Mais qui est le responsable du traitement des données de santé des patients incorporées dans le DMP ? « Y a-t'il un pilote dans l'avion de la réforme de l'assurance maladie ? »

Antérieurement au projet de mise en place du DMP, cela ne posait guère de problème : il s'agissait du médecin traitant⁸⁰. Dans le cadre de la gestion centralisée des données d'un patient, cela devient plus problématique, particulièrement en cas d'hospitalisation. Faut-il considérer que le responsable de la détermination des finalités du traitement est le médecin chef de l'hôpital, le directeur de celui-ci, le chef de service, les intervenants techniques, le médecin traitant, le responsable du système d'information hospitalier (SIH) ?

Les finalités du traitement de données de santé dans le cadre du DMP étant précisés dans la loi du 13 août 2004, le responsable du traitement semblerait devoir être l'organisme public gestionnaire du DMP visé dans l'arrêté du 12 avril 2005⁸¹.

Cette question de l'identification claire et précise du responsable du traitement est un pré requis à la mise en place du DMP, il convient donc qu'elle trouve rapidement une réponse formelle.

b) Obligations incombant au responsable du traitement

Au titre de ses obligations, celui-ci doit accomplir les formalités préalables au traitement des données (voir supra).

Il doit également informer la personne concernée par le traitement, notamment sur son identité, la finalité poursuivie par le traitement, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires du traitement, les droits de la personne concernée par le traitement et les transferts de données envisagés à destination d'un Etat non membre de la Communauté européenne⁸².

Le responsable du traitement doit également respecter la finalité déclarée du traitement.

Concernant la finalité thérapeutique du traitement dans le cadre du DMP, le responsable du traitement doit assurer un certain niveau de qualité des données. Celles-ci doivent être adéquates, pertinentes et non excessives. Elles doivent être exactes et mises à jour à l'occasion de chaque consultation médicale. De manière générale, le praticien a une responsabilité particulière par rapport à l'encodage des données. En effet, dans la mesure où le DMP est amené à être consulté par

⁸⁰ Art. R. 4.127-73 CSP : « *Le médecin doit protéger contre toute indiscretion les documents médicaux, concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents. Il en va de même des informations médicales dont il peut être le détenteur. Le médecin doit faire en sorte, lorsqu'il utilise son expérience ou ses documents à des fins de publication scientifique ou d'enseignement, que l'identification des personnes ne soit pas possible. A défaut, leur accord doit être obtenu* » et art. R. 4127-96 CSP : « *Sous réserve des dispositions applicables aux établissements de santé, les dossiers médicaux sont conservés sous la responsabilité du médecin qui les a établis* ».

⁸¹ Arrêté du 11 avril 2005 portant approbation de la convention constitutive d'un groupement d'intérêt public, J.O n° 85 du 12 avril 2005, p. 6.547

⁸² Art. 32, I de la loi informatique et libertés

différents professionnels de santé, il est crucial que les données soient correctes. Il doit à cet égard prendre les mesures organisationnelles qui s'imposent pour que chaque intervenant « encodeur » respecte des consignes préalablement établies⁸³.

Une obligation de respecter la durée de conservation des données pèse sur le responsable du traitement. Ce point sera développé dans la problématique de l'archivage des données, ainsi que l'obligation de sécurité et de confidentialité pesant également sur lui (voir infra).

Le responsable du traitement doit enfin informer sans délai la CNIL de tout changement sur les informations fournies au titre de ces formalités et de toute suppression de traitement⁸⁴.

Section 2 : Les solutions techniques requises

§1 : L'obligation de sécurité

a) La sécurisation des données

L'article 34 de la loi informatique et libertés dispose que le responsable du traitement « *est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

En étudiant les termes de l'article, il convient de constater que cette obligation de sécurité est une obligation de moyens. En effet, le responsable du traitement doit prendre « *toutes précautions utiles* », la charge de la preuve du manquement à cette obligation de sécurité pèsera donc en cas de litige sur la personne concernée par le traitement. Ceci peut s'expliquer par la très grande difficulté aujourd'hui d'obtenir une sécurité absolue dans les réseaux informatiques. L'internet est un portail sur le monde mais c'est donc également un portail sur les éventuelles attaques virales et intrusions en tous genre⁸⁵ provenant du monde entier.

L'alinéa 2 de l'article 34 prévoit que des décrets, pris après avis de la CNIL, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements

⁸³ T. Verbiest, « Le dossier médical informatisé : la délicate protection des données personnelles », 16 mars 2005, www.droit-technologie.org

⁸⁴ Art. 30 de la loi informatique et libertés

⁸⁵ Les sites internet américains étant réputés comme les plus protégés ont déjà plusieurs fois été victimes d'intrusions frauduleuses et dernièrement une pratique s'est développée consistant à bloquer des dossiers sur les postes des utilisateurs par l'utilisation de moyens de cryptologie puis à demander une « rançon » par courrier électronique afin de transmettre la clé de chiffrement permettant de le débloquent...

nécessaires à la sauvegarde de la vie humaine avec impossibilité de recueillir le consentement et les traitements nécessaires à la médecine et à l'administration des soins.

Ces dispositions de la loi informatique et libertés ont été prises en compte par la loi du 13 août 2004 qui prévoit à son article 5 que « *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* ».

Dans son avis du 10 juin 2004, la CNIL insiste sur la spécificité de l'internet en considérant que dès lors qu'est envisagé l'utilisation de ce réseau pour permettre l'accès effectif au DMP, celle-ci ne devait être acceptée que dans la mesure où des normes de sécurité extrêmement strictes sont imposées tant aux professionnels de santé qu'aux hébergeurs agréés, compte tenu des risques de divulgation des données.

Ainsi la CNIL considérait que le principe d'interdiction de toute commercialisation des données de santé visées devait être posé par la loi du 13 août 2004, ce qui a été fait et posé à son article 4 insérant un nouvel alinéa à l'article L. 1111-8 du CSP et qui dispose 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* » (cinq ans d'emprisonnement et de 300.000 euros d'amende).

Le responsable du traitement doit prendre les mesures techniques et organisationnelles requises pour protéger les données contre leur destruction accidentelle ou non autorisée, contre leur perte accidentelle ou leur modification. Il se doit, par ailleurs, de sécuriser l'accès aux données et de garantir leur intégrité par rapport à d'autres éventuels traitements non autorisés.

Les mesures techniques et organisationnelles doivent assurer un niveau de protection adéquat compte tenu de l'état de la technique en la matière, des frais qu'entraîne l'application de ces mesures, de la nature des données à protéger et des risques potentiels. Cela suppose l'interopérabilité des systèmes⁸⁶, des protocoles et des architectures relatifs à ces nouveaux services. Il faut également mettre en œuvre des systèmes efficaces d'identification des utilisateurs et intervenants. Il faut en effet définir, au préalable, les personnes et les institutions qui peuvent avoir accès aux données⁸⁷.

En raison des risques inhérents au réseau internet, le DMP doit être particulièrement protégé car il contient des données sensibles : l'historique médical de plus de soixante millions de personnes, rien que ça ! D'où la volonté des responsables politiques et de tous ceux qui défendent le projet (ainsi que ceux qui y seront, bon

⁸⁶ Cf. « Les grands principes du DMP », p.8

⁸⁷ T. Verbiest, « Le dossier médical informatisé : la délicate protection des données personnelles », 16 mars 2005, www.droit-technologie.org

gré mal gré, confrontés...c'est-à-dire potentiellement toute la population française) de sécuriser le DMP avec ce qui se fait de mieux en matière de sécurité informatique afin d'aboutir à l'eldorado convoité par tous les possesseurs d'ordinateurs : la sécurité informatique ultime, la citadelle imprenable mais accessible à tous ceux dont on aura préalablement accordé l'accès, bref, le « coffre-fort électronique ».

Cette métaphore caractérise donc les solutions techniques existantes qui permettent de placer les données personnelles sous le contrôle effectif de leurs titulaires⁸⁸.

Elle suggère la mise sous clef des données personnelles (en l'espèce les données de santé à caractère personnel), leur titulaire étant le seul capable d'y accéder. Dans le cas du DMP il faut non seulement assurer l'accès sécurisé au patient mais également à tous les professionnels de santé amenés à compléter le DMP (avec l'accord du patient).

L'obligation de sécurité passe également par l'authentification des personnes y accédant.

b) Authentification : le projet de carte Vitale 2

Il faut assurer l'authentification du patient et du professionnel de santé lors de l'accès au DMP. Cette authentification se distingue particulièrement sur l'internet de l'identification en ce que l'identification est une démarche volontaire de la personne voulant avoir accès aux données et ne prouve pas son identité, alors que l'authentification consiste, pour un système informatique, à effectuer la vérification de l'identité d'une entité (personne, machine...)⁸⁹.

L'authentification peut passer par des moyens de preuve revêtant différentes formes : mot de passe, carte à puce, certificat électronique, biométrie, signature...

Afin de vérifier effectivement l'identité de la personne, un protocole d'authentification est utilisé⁹⁰.

Ce coffre-fort peut être hébergé soit sur l'ordinateur de la personne, sous son contrôle direct, soit chez un intermédiaire public ou privé (l'hébergeur de données de santé à caractère personnel agréé dans le cas du DMP).

Le coffre-fort lui-même peut être compartimenté en zones, des clefs différentes donnant accès aux différentes zones. Ainsi, au lieu d'une clef unique, il existe un

⁸⁸ Voir le Livre Blanc « Administration électronique et protection des données personnelles », *La Documentation Française*, 2002, p. 67

⁸⁹ www.fr.wikipedia.org

⁹⁰ Exemples : Secure Socket Layer (SSL), protocole de sécurisation des échanges sur l'internet ; NTLM, protocole d'identification utilisé dans diverses implémentations des protocoles réseau Microsoft ; Kerberos, protocole d'authentification réseau créé au MIT utilisant un système de clés de chiffrement privées au lieu de mots de passe en texte clair ; ...

trousseau de clefs électroniques. Cela traduit le besoin d'un accès gradué au DMP des professionnels de santé en fonction de leur spécialité.

Dans le cadre du DMP deux moyens d'authentification seront utilisés : la carte Vitale de l'assuré et la carte de professionnel de santé du médecin (CPS).

L'article L. 161-31 du Code de la sécurité sociale modifié par l'article 21 de la loi du 13 août 2004 dispose que « *l'utilisation de cette carte (Vitale) permet d'exprimer l'accord du titulaire* ».

La CNIL a eu l'occasion de rappeler dans son avis du 10 juin 2004 que l'obligation de faire porter la photographie de l'assuré sur sa carte Vitale est consacrée par l'article L. 161-31 du Code de la Sécurité sociale qui dispose que : « *les organismes d'assurance maladie délivrent une carte électronique individuelle inter-régimes à tout bénéficiaire de l'assurance maladie qui comporte une photographie de celui-ci. Cette carte est valable partout en France et tout au long de la vie de son titulaire, sous réserve que la personne bénéficie de prestations au titre d'un régime d'assurance maladie et des mises à jour concernant un changement de régime ou des conditions de prise en charge. Elle est délivrée gratuitement* ».

L'article 21 de la loi du 13 août 2004 prévoit qu'une photographie sera apposée sur la carte Vitale lors du prochain renouvellement des cartes, qui est prévu pour mi-2006. Il est donc prévu que cette carte ait un véritable rôle de carte d'identité de santé, jouant le rôle de clef d'accès au dossier patient et contenant des données médicales en cas d'urgence. Le décret en Conseil d'Etat correspondant devait cependant être publié au premier semestre 2005...

Concernant le volet d'urgence prévu dans la carte Vitale, l'article L. 161-31, 2° du Code de la Sécurité sociale dispose que « *cette carte électronique comporte un volet d'urgence destiné à recevoir les informations nécessaires aux interventions urgentes. Les professionnels de santé peuvent porter sur le volet, avec le consentement exprès du titulaire de la carte, les informations nécessaires aux interventions urgentes. Un décret en Conseil d'Etat, pris après avis du Conseil national de l'ordre des médecins et de la Commission nationale de l'informatique et des libertés, fixe les conditions d'application de cette mesure ainsi que les conditions d'accès aux différentes informations figurant dans ce volet d'urgence* ».

La loi autorise les médecins, à l'occasion des soins qu'ils délivrent, à consulter les données issues des procédures de remboursement ou de prise en charge détenues par l'organisme dont relève l'assuré. Le patient donne son accord en permettant au professionnel de santé d'utiliser la carte Vitale.

La loi du 13 août 2004 prévoit donc que la carte Vitale soit la clef d'accès au DMP. Des adaptations sécuritaires, dont les grandes orientations techniques sont encore discutées, vont apparaître sur la carte Vitale 2 qui sera distribuée entre fin 2006 et fin 2008⁹¹. Elle disposera d'un volet d'urgence, d'une clef d'accès au dossier des prestations de l'Assurance maladie pour les professionnels de santé, un « sésame »

⁹¹ Voir « Dossier médical personnel : un flou technique qui dure », *Le Monde informatique*, 4 février 2005, p. 16

pour ouvrir le DMP stocké chez un hébergeur distant, ainsi que l'adresse électronique du « e-DMP ». Elle intégrera des moyens de cryptologie⁹² et pourrait aussi comporter une fonction antifraude avec identification biométrique du porteur, ce qui n'est pas du goût de tout le monde⁹³.

Cette carte sera conçue pour être conforme au standard IAS (identification, authentification, signature) et pourra aussi servir d'outil de signature de formulaire d'administration électronique. Elle devra donc répondre aux conditions posées à la signature électronique par la directive européenne du 13 décembre 1999⁹⁴ et transposées par la loi du 13 mars 2000⁹⁵, et notamment elle doit mettre en œuvre un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache⁹⁶.

La CNIL a eu l'occasion de rappeler que les informations figurant sur les feuilles de soins contenues dans le DMP comportaient, outre les éléments d'identité de la personne et son numéro de sécurité sociale l'indication précise du code détaillé de l'acte pratiqué et des prestations servies qui peuvent révéler, dans certains cas, la pathologie dont est atteint le patient. Elles revêtent donc une sensibilité particulière.

Elle considère également que la remise de sa carte Vitale par l'assuré devra s'accompagner d'une information claire sur l'accès qui sera ainsi autorisé et sur sa signification.

Enfin, compte tenu des risques de divulgation et d'utilisation détournée des informations inhérents au réseau Internet, la confidentialité des informations médicales nominatives appelées à circuler sur le réseau devrait être garantie par le recours systématique à des moyens de chiffrement⁹⁷.

c) Le cas de la CNIE :

Le projet INES (Identité nationale électronique sécurisée) annoncé mi-avril 2005 par le ministre de l'Intérieur, Dominique de Villepin et prévoyant la création de la carte nationale d'identité électronique (CNIE) obligatoire et payante en 2007, amène le même type d'interrogations que celles soulevées par la carte Vitale 2: les données biométriques⁹⁸. En effet, le projet prévoit qu'une puce électronique comportant l'empreinte digitale et la photo du détenteur sera intégrée sur la CNIE. Pour gérer ces données et effectuer les vérifications nécessaires à l'authentification du porteur de la

⁹² L'article 30 de la loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 dispose que : « *l'utilisation des moyens de cryptologie est libre* ».

⁹³ La Ligue des Droits de l'Homme y est fermement opposée.

⁹⁴ Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E* n° L. 013 du 19 janvier 2000, p. 12 à 20

⁹⁵ Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *J.O* n° 62 du 14 mars 2000 p. 3.968

⁹⁶ Art. 1316-4 du Code civil

⁹⁷ Délibération CNIL n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au publics, www.cnil.fr

⁹⁸ Voir le dossier de présentation du programme INES sous <http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

CNIE, le projet prévoit également la création d'un fichier central de données biométriques, comme le prévoit le DMP concernant les données de santé à caractère personnel.

Selon la Ligue des droits de l'homme et plusieurs syndicats et organisations professionnelles, la constitution de ce fichier central de données biométriques serait contraire au principe de proportionnalité par rapport au but poursuivi de traitement de données à caractère personnel, tel qu'édicté par la loi informatique et libertés⁹⁹. Les pouvoirs publics n'auraient selon eux pas les moyens nécessaires pour contrôler ce fichier.

§2 : L'obligation de conservation des données

a) Antérieurement au DMP : conservation des dossiers médicaux dans les cabinets libéraux et les établissements hospitaliers

Pour le médecin libéral, l'obligation de conserver et de protéger les dossiers de ses patients est inscrite dans les articles 45 et 73 du Code de déontologie médicale.

L'article 45¹⁰⁰ dispose que : *« 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 »*.

L'article 73¹⁰¹ dispose que : *« le médecin doit protéger contre toute indiscretion les documents médicaux, concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents. Il en va de même des informations médicales dont il peut être le détenteur. Le médecin doit faire en sorte, lorsqu'il utilise son expérience ou ses documents à des fins de publication scientifique ou d'enseignement, que l'identification des personnes ne soit pas possible. A défaut, leur accord doit être obtenu »*.

Le dossier de suivi médical est la propriété du patient donc le médecin se doit de la conserver jusqu'à ce que le patient décide de changer de médecin (l'ancien médecin doit transférer au nouveau le dossier), jusqu'à ce qu'il cesse son activité (il doit alors assurer le transfert des dossiers de ses malades aux médecins qu'ils auront désignés), ou jusqu'au décès du patient.

⁹⁹ Voir l'article d'Arnaud Devillard, « La carte d'identité électronique fait l'unanimité contre elle », 26 mai 2005, www.01net.com

¹⁰⁰ Art. R. 4.127-45 CSP

¹⁰¹ Art. R. 4.127-73 CSP

Concernant les établissements de soins, les dispositions prévues pour l'archivage¹⁰² précisent que nombreux dossiers médicaux peuvent être éliminés about de 20 ans. Mais ceux qui concernent les affections de pédiatrie, de neurologie et les maladies chroniques doivent être conservés 70 ans. Les dossiers ayant trait à des affections héréditaires doivent être conservés indéfiniment.

Les dossiers médicaux administratifs doivent être conservés 5 ans dans la base informatique active au-delà de la dernière consultation puis devront être archivés sur support fiable pendant 20 ans (et de 20 à 38 ans pour les patients mineurs)¹⁰³.

b) Durée de conservation des données de santé dans le DMP

En ce qui concerne la durée de conservation des données de santé intégrées dans le DMP, il faut combiner les obligations imposées par la législation informatique et libertés à celles définies par la déontologie médicale.

Aux termes de l'article 6, 1, e, de la directive du 25 octobre 1995¹⁰⁴, les Etats membres sont tenus de prévoir que les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

Ce principe a été repris à l'article 10.1 de la recommandation n° R (97) 5 du 13 février 1997 relative à la protection des données médicales¹⁰⁵.

L'article 6, 5° de la loi du 6 août 2004 transposant la directive du 25 octobre 1995 prévoit que les données « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ».

Dans le cas du DMP, les données seraient donc conservées jusqu'à la fin du traitement d'une pathologie ou jusqu'au décès du patient. Cette seconde hypothèse serait la plus probable.

Il n'est donc pas possible de conserver le DMP indéfiniment. Dans les cas où les données sont conservées alors qu'elles ne sont plus nécessaires au but d'origine du traitement mais sont conservées pour l'intérêt de la santé publique dans le cas du DMP, la directive précise que les Etats membres doivent prévoir des garanties appropriées. La recommandation du 13 février 1997 prévoit elle que des dispositions

¹⁰² Règlement des archives de France établi par un décret de 1943 et un arrêté du 11 mars 1968

¹⁰³ Projet de rapport de la Commission nationale paritaire DMP de l'Ordre des médecins

¹⁰⁴ 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

¹⁰⁵ Recommandation n° R (97) 5 relatives à la protection des données médicales, adoptée par le comité des ministres du Conseil de l'Europe le 13 février 1997

techniques doivent assurer la conservation et la sécurité des données en tenant compte de la vie privée du patient.

Ainsi, l'article 36 de la loi du 6 août 2004 prévoit notamment qu'il peut être fait exception à la conservation dans la durée nécessaire à la finalité du traitement pour les données traitées à des fins historiques, statistiques ou scientifiques, mais également pour des données de santé dont le traitement est justifié par l'intérêt public et autorisé dans les conditions prévues aux articles 25 et 26. Cette exception semblerait donc pouvoir s'appliquer à la conservation des données de santé contenues dans le DMP, qui pourraient être conservées plus longtemps

L'article 226-20 du Code pénal, modifié par l'article 14 de la loi du 6 août 2004, prévoit que :

« le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi ».

Une fois le délai de conservation achevé il est procédé à un tri pour déterminer les données destinées à être conservées et celles, dépourvues d'intérêt scientifique, statistique ou historique, destinées à être détruites.

Les catégories de données destinées à la destruction ainsi que les conditions de leur destruction sont fixées par accord entre l'autorité qui les a produites ou reçues et l'administration des archives¹⁰⁶.

Il convient de souligner le fait qu'une trop longue durée légale de conservation pose d'importants problèmes de support de stockage. La durée de vie limitée de supports comme le CD en est la preuve.

¹⁰⁶ Art. L. 212-4 du Code du patrimoine

Chapitre 2 : Quant aux acteurs du traitement

Dans le cadre du DMP, le traitement des données de santé à caractère personnel est notamment effectué par les professionnels de santé (Section 1), les données étant stockées chez un hébergeur agréé (Section 2).

Section 1 : Les professionnels de santé

§1 : Le secret médical au centre du DMP

a) Le principe de protection

« La crainte de voir l'homme s'emparer totalement de l'homme est devenue le cœur de toutes les angoisses »¹⁰⁷.

La vie privée embrasse tour à tour le secret et la liberté des choix des modes de vie personnelle. Elle est notamment protégée par la Convention européenne des droits de l'homme en son article 8 et par le Code civil en son article 9¹⁰⁸.

Selon le Professeur Jacques Ravanas, le secret se rattache étroitement au privé, à tel point que la jurisprudence et la doctrine ont commencé par reconnaître un droit au secret de la vie privée : le demandeur Dreyfus « *est fondé à empêcher qu'une publicité indiscrete ne pénètre dans sa vie intime et ne trahisse le secret de ses croyances religieuses* »¹⁰⁹. La Cour d'appel de Paris a ensuite affirmé que « *chacun a droit au secret de sa vie intime* »¹¹⁰.

Il s'agit d'un droit subjectif qui énonce que chacun a le pouvoir de s'opposer à une investigation et à une divulgation de sa vie privée.

Le secret médical est également une obligation déontologique. Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a

¹⁰⁷ M. Contamine-Raynaud, *Le secret de la vie privée, ouvrage coll., L'information en droit privé*, LGDJ, 1978, p. 454, n° 36

¹⁰⁸ J. Ravanas, « Jouissance des droits civils », *JCP*, 5 mars 2002, fasc. 10

¹⁰⁹ T. corr. Lyon, 15 décembre 1896, *D.* 1897, 2, p. 179

¹¹⁰ CA Paris, 16 mars 1955, *D.* 1955, p. 295

été confié, mais aussi ce qu'il a vu, entendu ou compris¹¹¹. Il convient par ailleurs de citer l'obligation de confidentialité¹¹².

Le secret médical est une obligation légalement sanctionnée. La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession (ce qui est le cas des professionnels de santé), soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15.000 euros d'amende¹¹³.

Le secret médical est une obligation générale et absolue. Pour assurer la confiance nécessaire à l'exercice de certaines professions ou de certaines fonctions, l'obligation de secret professionnel s'impose aux médecins, hormis le cas où la loi en dispose autrement, comme un devoir de leur état. Cette obligation, sous cette seule réserve, est générale et absolue¹¹⁴.

« Le secret professionnel ne représente qu'un petit chapitre dans l'ensemble de la déontologie médicale, mais il est un symbole : le symbole du respect que le médecin doit avoir pour son malade. Il appartient à une certaine idée de la médecine qui suppose la liberté du malade, l'indépendance du médecin dans ses décisions, la responsabilité personnelle »¹¹⁵.

Le secret médical a fait l'objet d'une doctrine abondante, notamment en ce qui concerne la nature de l'obligation de secret : obligation d'ordre public ou d'intérêt privé ?

Ainsi que l'affirme Gérard Mémeteau¹¹⁶, la profession médicale est une profession d'intérêt public autant que d'intérêt particulier, régie par des règles générales qui protègent autant l'individu que l'ordre public. Ces règles protectrices de l'ordre public s'immiscent donc dans les relations contractuelles entre le médecin et son patient. Ceci est à la base de la relation de confiance nécessaire à l'exercice médical. Le malade doit donc être assuré que ce qu'il confie ou laisse voir ou entendre au médecin ne sera pas révélé par celui-ci.

Il faut néanmoins signaler que la Cour européenne des Droits de l'Homme, le 18 mai 2004¹¹⁷, a fait une application modérée de cette obligation de secret, contrairement aux juges nationaux¹¹⁸, en déclarant contraire à l'article 10 de la Convention européenne des Droits de l'Homme protégeant la liberté d'expression l'interdiction définitive de publication par le médecin personnel de François Mitterrand, le docteur Gubler, d'un livre intitulé « Le Grand Secret » qui faisait état des difficultés rencontrées par le docteur Gubler pour dissimuler la maladie de François Mitterrand, dont le cancer avait été diagnostiqué peu après son élection en 1981, alors qu'il s'était engagé à diffuser un bulletin de santé tous les six mois.

¹¹¹ Art. 4 du Code de déontologie médicale (art. R. 4.127-4 CSP)

¹¹² Art. 73 du Code de déontologie médicale (art. R. 4.127-73 CSP)

¹¹³ Art. 226-13 du Code pénal

¹¹⁴ Cass. crim., 8 avril 1998, *D.* 1999, somm. P. 381

¹¹⁵ R. Villey, *Histoire du secret médical*, Séghers, 1986, p. 163

¹¹⁶ G. Mémeteau, *Cours de droit médical*, Les études hospitalières, 2001, p. 217

¹¹⁷ CEDH, 18 mai 2004, « Plon c. France » ; *Comm. com. électr.* 2004, comm. 96

¹¹⁸ CA Paris, 27 mai 1997 confirmée par : Cass. 1^{ère} civ., 14 décembre 1999, *D.* 2000, n° 17, p. 372

La Cour avait en l'espèce pris en compte des éléments de faits, et notamment la diffusion sur l'internet du livre, pour affirmer qu'une interdiction provisoire n'était pas contraire à l'article 10 susvisé mais qu'une interdiction définitive ne répondait pas à un besoin impérieux de protection. En effet, selon la Cour, les données de santé à caractère personnel contenues dans le livre avaient, du fait de leur large diffusion, perdu l'essentiel de leur confidentialité et qu'en conséquence la sauvegarde du secret médical ne répondait plus à un impératif prépondérant.

b) Application au DMP

L'introduction de l'informatique dans le domaine de la santé consacre le passage du colloque singulier au « colloque électronique »¹¹⁹. Elle soulève le problème de la coexistence entre le secret médical et le partage des données de santé entre professionnels de santé.

Le Conseil national de l'Ordre des médecins (C.N.O.M.) a ainsi souvent pris position en faveur d'une autorisation conditionnelle du partage de l'information qui doit être encadrée en vue de respecter le secret médical.

Notamment, lors de sa session d'avril 2000 portant sur « l'exercice médical en ligne », et à l'occasion de sa session des 29 et 30 juin 2000 relative à « la commercialisation des informations médicales », le CNOM a eu l'occasion d'indiquer que « *le réseau internet ne permettant pas d'assurer la totale confidentialité des transmissions, le médecin doit veiller à ce qu'aucune information médicale nominative ne circule lorsque des données relatives à des dossiers médicaux sont mises en ligne* ».

La CNIL se fonde plutôt sur la nécessité de conserver la confidentialité des informations dans un but de respect de la vie privée des patients.

Dans son avis du 10 juin 2004¹²⁰, elle considère que les dispositions de l'article 2 de la loi du 13 août 2004 doivent être complétées par une mention particulière indiquant que les données susceptibles d'être portées dans le dossier médical personnel sont couvertes par le secret professionnel tel que celui-ci est défini par le code pénal et que quiconque aura obtenu ou tenté d'en obtenir la communication en violation des dispositions du présent article s'exposera à des sanctions pénales, de même que quiconque aura modifié ou tenté de modifier les informations portées sur ce même dossier.

L'article 2 de la loi du 13 août 2004 introduit un article L. 161-36-1 dans le Code de la sécurité sociale¹²¹ qui dispose 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 ».

¹¹⁹ C. Chabert, « Le dossier médical on line et le secret médical », *Gaz. Pal.*, 15-17 juillet 2001, p. 25

¹²⁰ Délibération CNIL 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

¹²¹ Cet article est la reproduction de l'article L. 1110-4 CSP introduit par la loi du 5 mars 2002

Ce secret couvre l'ensemble des informations concernant la personne. Cependant il ne fait pas obstacle au partage des données entre professionnels de santé, sauf opposition de la personne dûment avertie, afin d'assurer la finalité posée au DMP : la coordination des soins et la meilleure prise en charge sanitaire possible.

L'article prévoit par ailleurs que la conservation sur support informatique et la transmission par voie électronique entre professionnels des informations médicales à caractère personnel doivent respecter des règles qui seront définies par décret en Conseil d'Etat pris après avis motivé de la CNIL¹²².

L'article L. 161-36-1 du Code de la sécurité sociale dispose par ailleurs que chaque bénéficiaire de l'assurance maladie dispose d'un DMP, dans le respect du secret médical.

Actuellement les données de santé transmises par la carte Vitale font figurer le numéro de sécurité sociale du patient et le numéro de carte professionnelle de santé du médecin.

Avec le projet de carte Vitale 2, les données relatives aux antécédents médicaux et autres données (notamment biométriques) seront « exposées ».

Ainsi, certains médecins refusent de s'informatiser « pour ne pas violer le secret médical »¹²³.

Tandis que la loi informatique et libertés protège toutes les données à caractère personnel, en accordant une protection renforcée aux données médicales qui sont considérées comme des données sensibles, le secret médical possède un champ d'application beaucoup plus large car il couvre toutes les confidences faites par le patient à son médecin et comprend notamment les notes, les pensées, les constatations et examens réalisés par le professionnel de santé.

§2 : Nouveaux risques ou dilution des responsabilités ?

L'utilisation du DMP va-t-il être une source de nouvelles responsabilités pour les professionnels de santé ou au contraire va-t-on assister à une « dilution des responsabilités » liée à la centralisation du dossier patient ? Il convient d'étudier les différentes sanctions posées dans la loi relative à l'assurance maladie et celles de la loi informatique et libertés.

¹²² Décret en Conseil d'Etat n° 2002-637 du 29 avril 2002 publié au J.O du 30 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 111-7 et L. 1112-1 CSP

¹²³ Association « Acis Vipi »

a) Sanctions issues de la loi du 13 août 2004

L'article 2, I de la loi rappelle tout d'abord l'obligation pour les professionnels de santé de respecter la vie privée et le secret du patient. Ils ont la possibilité de s'échanger des informations, ce qui est la principale raison d'être du DMP, mais ils ont également la nécessité de respecter l'obligation de confidentialité des informations médicales. Leur conservation sur support informatique et leur transmission par voie électronique entre professionnels sont ainsi soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la CNIL, ce décret déterminant également les cas où l'utilisation de la carte de professionnel de santé est obligatoire.

L'alinéa 5 de l'article 2 sanctionne le fait d'obtenir ou de tenter d'obtenir la communication des informations médicales des patients en violation des obligations de secret professionnel et de confidentialité d'un an d'emprisonnement et de 15.000 euros d'amende.

Cette sanction pèsera sur le professionnel de santé qui n'aura par exemple pas pris en compte l'opposition du patient à la transmission de ses données.

Afin d'encadrer l'accès au DMP, ce dernier n'est pas accessible dans le cadre de la médecine du travail, ce qui résulte de l'article L. 161-36-3 du Code de la sécurité sociale introduit par l'article 3 de la loi. Tout manquement à ces dispositions est passible des sanctions pénales prévues à l'article 226-13 du Code pénal qui dispose que « *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* ».

Selon le Conseil national de l'Ordre des médecins, cette interdiction d'accès par le médecin du travail reflète leur manque d'indépendance vis-à-vis de leur employeur, ce que le Conseil déplore.

Le souci exprimé à plusieurs reprises par la CNIL¹²⁴ d'affirmer dans la loi le principe de l'interdiction de toute commercialisation des données de santé a été repris par le législateur¹²⁵ : « *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* » (cinq ans d'emprisonnement et 300.000 euros d'amende).

b) Sanctions issues de la loi informatique et libertés¹²⁶

Quatre types de sanctions peuvent être prononcées sur la base de la loi informatique et libertés.

¹²⁴ Voir « Assurance maladie : le point sur la loi adoptée », www.cnil.fr

¹²⁵ Art. L. 1111-8 CSP introduit par l'article 4 de la loi du 13 août 2004

¹²⁶ Voir A. Lepage, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Droit pénal*, mars 2005, p. 6 ; M-L Laffaire, Protection des données à caractère personnel, *Editions d'Organisation*, 2005

Concernant les sanctions pénales, un abaissement des peines maximales avait été envisagé mais a été abandonné au moment du vote de la loi du 6 août 2004. En effet, même si ces peines paraissent élevées, le maximum n'est pratiquement jamais prononcé et les poursuites sont très rares¹²⁷. L'auteur de l'infraction est en principe le responsable du traitement qui sera pénalement responsable, mais la complicité du sous-traitant ou d'une autre entité impliquée dans la réalisation de l'infraction pourrait selon le cas d'espèce être retenue.

Concernant le traitement effectué dans le cadre du DMP, il convient de retenir certaines infractions : le non respect de l'obligation de sécurité¹²⁸, le non respect du droit d'opposition fondé sur des motifs légitimes¹²⁹, le traitement de données sensibles sans l'accord exprès de l'intéressé¹³⁰ sont punis de 5 ans d'emprisonnement et de 300.000 euros d'amende, les données à l'origine de l'infraction étant effacées.

Pour l'infraction visant les données sensibles, le consentement de la victime n'agit pas comme fait justificatif mais est pris en compte au plan de la constitution même de l'infraction.

Des sanctions civiles peuvent être prononcées sur le fondement de l'article 1382 du Code civil. Elles peuvent résulter des diverses obligations posées dans la loi : négligences ou inobservations vis-à-vis des dispositions traitant notamment des conditions de licéité du traitement sont susceptibles d'occasionner un préjudice à la personne concernée par le traitement litigieux.

La CNIL, autorité administrative indépendante, dispose d'un pouvoir de prononcer des sanctions administratives¹³¹. Elle peut donc prononcer des avertissements, des mises en demeure, et, après une procédure contradictoire, des sanctions pécuniaires, des injonctions de cesser un traitement litigieux ou le retrait de l'autorisation. Le plafond des sanctions pécuniaires est fixé à 150.000 euros mais peut doubler en cas de manquement réitéré dans les cinq ans par une personne morale.

Une procédure d'interruption du traitement ou de verrouillage des données est prévue, mais ne s'applique pas aux traitements de données de santé.

Ces sanctions sont indépendantes des éventuelles sanctions disciplinaires qui pourraient intervenir. Par exemple, l'Ordre des médecins dispose d'un pouvoir disciplinaire. Il s'exerce en première instance par les conseils régionaux et en appel par la section disciplinaire du Conseil national, sous le contrôle du Conseil d'Etat, juge de cassation¹³².

¹²⁷ Pour exemple, l'opération « boîte à spams » de la CNIL qui n'a abouti qu'à une seule condamnation à 3.000 euros d'amende

¹²⁸ Art. L. 226-17 CP

¹²⁹ Art. L. 226-18-1 CP

¹³⁰ Art. L. 226-19, alinéa 1 CP

¹³¹ Art. 45 à 49 de la loi informatique et libertés

¹³² Voir G. Mémeteau, *Cours de droit médical*, Les Etudes Hospitalières, 2001

Section 2 : L'hébergeur de données de santé à caractère personnel agréé

§1 : Les obligations de l'hébergeur

a) L'article L. 1111-8 CSP

Aux termes de l'article L. 161-36-1 du Code de la sécurité sociale introduit par l'article 3 de la loi du 13 août 2004, le DMP 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 CSP.

Lors de sa délibération du 8 mars 2001¹³³, la CNIL souhaitait que soit réglementée l'activité des hébergeurs de données de santé à caractère personnel.

Ainsi, l'obligation d'agrément de l'hébergeur de données de santé à caractère personnel a été incorporée dans la loi du 4 mars 2002¹³⁴ qui a défini les grandes lignes de l'encadrement de l'activité d'hébergement des données médicales¹³⁵.

L'article 11 de la loi de 2002 a introduit l'article L. 1111-8 dans le Code de la santé publique qu'il convient d'étudier ici dans son intégralité et qui dispose que : « *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.* ».

L'article poursuit en rappelant que le traitement de ces données de santé à caractère personnel doit être effectué dans le respect de la loi informatique et libertés et la prestation d'hébergement doit faire l'objet d'un contrat qui, lorsqu'il est à l'initiative d'un professionnel de santé ou d'un établissement de santé, doit préciser que l'hébergement de ces données et leurs modalités d'accès et de transmission requièrent le consentement préalable de la personne concernée, c'est-à-dire le patient.

Seuls les patients et les professionnels de santé ou établissements de santé dûment désignés ont accès aux données qui ont fait l'objet de l'hébergement. Ces données sont mises à disposition de ceux qui les ont confiées (dans la mesure où la

¹³³ Délibération CNIL n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public

¹³⁴ Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite « loi Kouchner »

¹³⁵ Voir C. Féral-Schuhl, « L'hébergement des données médicales numériques : un dispositif légal spécifique », *Le Quotidien du médecin*, 6 mars 2003, p. 37

procédure d'accès est respectée en aval), les hébergeurs ne peuvent les utiliser à d'autres fins¹³⁶.

Les hébergeurs ne peuvent pas garder copie des données hébergées lorsqu'il est mis fin au contrat, mais doivent les restituer intégralement à l'établissement ou au patient ayant contracté avec lui.

L'obligation de secret professionnel s'applique aux hébergeurs, dans la mesure où les données hébergées sont des données de santé à caractère personnel¹³⁷.

Des procédures de contrôle sont prévues et sont effectuées par l'inspection générale des affaires sociales et des agents de l'Etat.

Sous l'impulsion des recommandations effectuées par la CNIL dans son avis du 10 juin 2004, les rédacteurs de la loi du 13 Août 2004 relative à l'assurance maladie ont complété l'article L. 1111-8 par l'alinéa suivant : « *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.* ».

Enfin, l'article L. 1111-9 du CSP prévoit que l'Agence nationale d'accréditation et d'évaluation en santé (ANAES)¹³⁸ émet des recommandations de bonnes pratiques sur les modalités d'accès aux informations et l'accompagnement de cet accès.

b) L'agrément : gage de sécurité et d'indépendance

Les hébergeurs doivent, conformément à l'article 1111-8 du CSP, être agréés. Les conditions de l'agrément sont fixées dans un décret en Conseil d'Etat pris après avis de la CNIL et des Ordres professionnels.

L'hébergeur doit notamment fournir les modèles de contrats prévus, les mécanismes de contrôle et de sécurité dans le domaine informatique ainsi que les procédures de contrôle interne.

Il est donc vérifié que l'hébergeur va bien pouvoir répondre à l'obligation de sécurité que va faire peser sur lui la loi informatique et libertés¹³⁹ dans le cadre du traitement de données de santé visé.

Il est également vérifié si l'audit interne est suffisant pour éviter les risques de détournements de données. En effet, la « valeur marchande » des données qui seront hébergées est très importante et peut donner envie à certaines sociétés d'assurances complémentaires ou autres de « jouer avec le feu » ! La sécurisation

¹³⁶ Notamment à des fins commerciales !

¹³⁷ La sanction de la violation du secret professionnel est prévue à l'article 226-13 CP qui dispose que « *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* ».

¹³⁸ Remplacée par la Haute autorité de santé par la loi du 13 août 2004

¹³⁹ Art. 34 de la loi informatique et libertés

des données de santé est donc exigée par rapport aux risques externes¹⁴⁰ mais également par rapport aux risques internes¹⁴¹.

Ainsi, pour éviter les risques de pressions sur les hébergeurs de données de santé, l'article L. 1111-8 prévoit qu'est applicable aux contrats d'hébergement conclus les dispositions de l'article L. 4113-6 du CSP qui dispose qu' « *est interdit le fait, pour les membres des professions médicales mentionnées au présent livre, de recevoir des avantages en nature ou en espèces, sous quelque forme que ce soit, d'une façon directe ou indirecte, procurés par des entreprises assurant des prestations, produisant ou commercialisant des produits pris en charge par les régimes obligatoires de sécurité sociale. Est également interdit le fait, pour ces entreprises, de proposer ou de procurer ces avantages* ».

Les hébergeurs de données de santé sont donc assimilés à des professions médicales par cet article, afin de leur assurer une indépendance vis-à-vis des entreprises présentes sur ce marché. Cette indépendance a toujours été recherchée pour les médecins, afin d'assurer leur totale liberté professionnelle quant à leurs prescriptions.

L'agrément peut faire l'objet d'un retrait en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

Il convient désormais d'étudier le projet de décret en Conseil d'Etat fixant les conditions d'agrément des hébergeurs, qui devait être pris en application de l'article L. 1111-8 du CSP issu de la loi du 4 mars 2002 mais qui n'a à ce jour toujours pas été voté.

§2 : Les règles à venir

a) Projet de décret relatif à l'hébergement de données de santé à caractère personnel

Le décret en Conseil d'Etat pris en application de l'article L. 1111-8 du CSP¹⁴² et fixant les conditions d'agrément des hébergeurs de données de santé à caractère personnel est toujours en attente de publication, alors que le projet de décret était circularisé dès 2003.

Le projet de décret insère tout d'abord un article R. 1111-9 dans le Code de la santé publique, définissant l'activité d'hébergement de données de santé à caractère

¹⁴⁰ Attaques virales, tentatives d'intrusion frauduleuse, détournement de données,...

¹⁴¹ Il convient de faire un parallèle avec les normes de sécurité (« vendor compliance ») exigées aux commerçants en ligne par les principaux groupements de cartes bancaires avant le 30 juin 2005 et qui prévoit notamment des règles strictes quant aux contrôles internes

¹⁴² Art. 11, al. 34 de la loi du 4 mars 2002

personnel comme « *l'organisation du dépôt et la conservation des données, notamment de manière à en assurer la pérennité et la confidentialité* ».

Cette définition se distingue donc de celle de l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 qui définit également l'activité d'hébergeur de données : « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Cette différence de définition s'explique par le caractère sensible des données de santé hébergées.

Le projet de décret prévoit ensuite la création d'un comité d'agrément des hébergeurs de données de santé à caractère personnel qui a pour mission d'examiner et d'émettre un avis sur les demandes d'agrément qui lui sont adressées par les hébergeurs.

Au titre des conditions d'agrément, l'hébergeur devra « *mettre en œuvre des solutions techniques et organisationnelles conformes à l'état de l'art assurant la protection, la conservation, et la restitution des données confiées, et garantissant que celles-ci ne donneront lieu qu'à des usages conformes à la loi* ». Ces garanties sont appréciées par le comité d'agrément susvisé.

Il devra réaliser le service sur le territoire de l'Union européenne ou dans un Etat fournissant des garanties équivalentes à celles existant en droit français en matière de protection des données sensibles et du secret médical.

La gestion des données de santé devra enfin être spécifique et isolée de ses autres activités.

Le projet détaille ensuite les éléments du dossier de demande d'agrément. Puis il prévoit les clauses à insérer dans les contrats d'hébergement, les modalités de la politique de confidentialité qui doit être mise en place par l'hébergeur (notamment en matière de respect des droits des patients, de sécurité de l'accès aux informations, ainsi que d'organisation et de procédures de contrôle interne mises en place pour garantir la sécurité des traitements et des données), et enfin les modalités de l'audit technique externe.

L'agrément d'un hébergeur serait prononcé par arrêté du ministre chargé de la santé sur avis du comité d'agrément, il est prononcé pour trois ans, renouvelable sur demande auprès du comité d'agrément.

b) Recommandations quant aux hébergeurs

L'Institut Montaigne¹⁴³ a émis des recommandations s'agissant des obligations à remplir par l'hébergeur : la disponibilité du service 24 heures sur 24 et 7 jours sur 7, l'intégrité des données, la confidentialité des informations et la sécurité physique et logique du dispositif, la traçabilité des accès au DMP et la pérennité¹⁴⁴ de la conservation des informations lisibles.

Selon l'Institut, l'hébergeur devra être compétent en matière de : conception, développement et gestion d'applications informatiques critiques et sécurisées mais également intuitives, ergonomiques et adaptées aux situations de travail des utilisateurs ; gestion de la relation avec le grand public et les professionnels de santé (promotion du DMP, centres d'appels pour répondre aux questions, gestion du processus de l'ouverture à la fermeture du dossier) ; compréhension du monde médical, de ses enjeux et de ses valeurs propres ; gestion de la relation avec les professionnels de santé.

L'Institut remarque ensuite que certains hébergeurs sont d'ores et déjà prêts : ils ont constitué des groupements rassemblant les composantes nécessaires, ils ont développé des solutions techniques adaptables au DMP, ils bénéficient de premiers retours d'expériences sur des déploiements existants en France ou à l'étranger¹⁴⁵.

La Commission nationale paritaire DMP de l'Ordre des médecins recommande notamment que soient établies des garanties strictes concernant la fiabilité de l'hébergeur et la confidentialité des données de santé. Elle recommande également que soient prévues des dispositions pénales contraignantes et dissuasives en cas de faute de l'hébergeur.

¹⁴³ Laboratoire d'idées « think tank » indépendant, composé de chefs d'entreprise, de hauts fonctionnaires, d'universitaires et de représentants de la société civile et élaborant des recommandations sur les grands enjeux de société

¹⁴⁴ Terme souvent employé dans la « littérature DMP » !

¹⁴⁵ Dominique Vadrot, « Le Dossier Médical Personnel. Etat des lieux fin octobre 2004. Proposition d'une solution pour une installation rapide », *Institut Montaigne*, 25 octobre 2004, www.institutmontaigne.org

CONCLUSION :

Le projet de Dossier médical personnel (et son calendrier actuel¹⁴⁶) est-il réaliste et réalisable ?

Au point de vue juridique, de nombreux décrets sont encore attendus : le décret relatif aux conditions d'agrément des hébergeurs de données de santé à caractère personnel¹⁴⁷, le décret fixant les règles de conservation et de transmission des données de santé à caractère personnel¹⁴⁸, le décret fixant les conditions d'application des dispositions de la loi du 13 août 2004 sur le DMP¹⁴⁹ et enfin le décret fixant les conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et la tenue du DMP¹⁵⁰.

Au point de vue technique de nombreux défis sont à soulever et sont accueillis avec plus¹⁵¹ ou moins¹⁵² d'enthousiasme¹⁵³ par les opérateurs.

La réussite de la mise en place du DMP passera essentiellement par les professionnels de santé et par les patients, d'où l'intérêt d'une information constante et intelligible (ce qui n'est pas toujours le cas) sur le projet, afin d'éviter les malentendus.

Le DMP devra être un outil d'amélioration de la qualité du système de soins au service du patient et du professionnel de santé, ne portant pas atteinte au respect de la vie privée des patients. Il est à souhaiter que les garanties prévues et à prévoir seront suffisantes pour éviter les risques tirés de la mise en ligne des données de santé.

« Et demain, l'Europe ? »¹⁵⁴

¹⁴⁶ Dont on ne prend pas trop de risques en disant qu'il a été dicté par des exigences...électorales.

¹⁴⁷ Art. 11, al. 34 de la loi du 4 mars 2002- art. L. 1111-8 CSP

¹⁴⁸ Art. 2, I, al. 5 de la loi du 13 août 2004 – art. L. 161-36-1, A du Code de la sécurité sociale

¹⁴⁹ Art. 3, I, al. 13 de la loi du 13 août 2004 – art. L. 161-36-4 du Code de la sécurité sociale

¹⁵⁰ Art. 5, al. 1^{er} de la loi du 13 août 2004

¹⁵¹ Pour Pierre Bruneau, médecin et directeur médical d'une société éditrice de logiciels de santé et prestataire de services dans le domaine de la santé : « Nous pouvons être prêts en 48 heures »

¹⁵² Pour Ugo Haberman, directeur général technique d'une société fournissant un dossier médical partagé en mode hébergé : « Pour le DMP, dix ans est un délai réaliste »

¹⁵³ Voir « Les grandes réformes misent sur l'informatique », *Le Monde informatique*, 4 février 2005, p.

15

¹⁵⁴ *Bulletin de l'Ordre des médecins*, n° 3, mars 2005, p. 16

BIBLIOGRAPHIE

Principales notes juridiques

M. Fieschi, « 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

N. Beslay et J-F Forgeron, « La loi relative aux droits des malades : la consécration du droit de la santé électronique », *Gaz. Pal.*, 22-23 janvier 2003, p. 4

G. Kostic, Enseignement dirigé « Informatique, multimédia et protection des personnes », DESS DMI, 2004-2005

J-E Schoettl, « La réforme de l'assurance maladie devant le Conseil constitutionnel », *Petites affiches*, 15 septembre 2004, n° 185, p.6

Livre Blanc « Administration électronique et protection des données personnelles », *La Documentation Française*, 2002, p. 75

C. Féral-Schuhl, « Les conditions d'accès au dossier médical : guide pratique », *Le Quotidien du médecin*, 10 mars 2005, p. 44

T. Verbiest, « Le dossier médical informatisé : la délicate protection des données personnelles », 16 mars 2005, www.droit-technologie.org

J. Ravanas, « Jouissance des droits civils », *JCP*, 5 mars 2002, fasc. 10

C. Chabert, « Le dossier médical on line et le secret médical », *Gaz. Pal.*, 15-17 juillet 2001, p. 25

« Assurance maladie : le point sur la loi adoptée », www.cnil.fr

A. Lepage, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Droit pénal*, mars 2005, p. 6

C. Féral-Schuhl, « L'hébergement des données médicales numériques : un dispositif légal spécifique », *Le Quotidien du médecin*, 6 mars 2003, p. 37

Dominique Vadrot, « Le Dossier Médical Personnel. Etat des lieux fin octobre 2004. Proposition d'une solution pour une installation rapide », Institut Montaigne, 25 octobre 2004, www.institutmontaigne.org

Ouvrages

J-M Bruguière, *La diffusion de l'information publique : le service public face au marché de l'information*, thèse de doctorat soutenue le 23 juin 1995, Université de Montpellier I

Angelo Castelletta, *Responsabilité médicale – Droit des malades*, Dalloz, 2004

Liliane Dusserre, Henry Ducrot, François-André Allaert, *L'information médicale – L'ordinateur et la loi*, Editions Médicales Internationales, 1996

Jean Frayssinet, *Informatique, fichiers et libertés*, Litec, 1992

Marie-Laure Laffaire, *Protection des données à caractère personnel*, Editions d'Organisation, 2005

Isabelle de Lamberterie, Henri-Jacques Lucas, *Informatique, libertés et recherche médicale*, CNRS Droit, 2001

Agathe Lepage, *Libertés et droits fondamentaux à l'épreuve de l'internet*, LITEC, 3^e édition

Gérard Mémeteau, *Cours de droit médical*, Les Etudes Hospitalières, 2001

François Ponchon, *La loi du 4 mars 2002 : la mise en pratique*, Berger-Levrault, 2003

Isabelle Vacarie, *Le traitement informatique des données de santé – Question juridiques et éthiques*, Université de Paris I, 1988

Sites internet

Sur le DMP :

www.cnil.fr
www.dossier-medical.info
www.sante.gouv.fr
www.quotimed.com
www.delis.sgdg.org
www.institutmontaigne.org
www.conseil-national.medecin.fr
www.droit-medical.com
www.anaes.fr
www.gip-cps.fr
www.sesam-vitale.fr

Actualité juridique:

www.01net.com
www.zdnet.fr
www.droit-ntic.org
www.droit-technologie.org
www.juriscom.net
www.legalis.net
www.foruminternet.org
www.journaledunet.com

REMERCIEMENTS

Je tiens à remercier mes parents et mes amis, qui m'ont soutenu et aidé dans la rédaction de ce mémoire.

Je tiens également à remercier Monsieur le Professeur Jérôme Huet pour m'avoir permis d'intégrer le DESS DMI et Madame le Professeur Agathe Lepage pour ses conseils quant à la rédaction de ce mémoire.