Données de santé à caractère personnel : les enjeux de la diffusion des TIC

L'organisation de la santé en France est confrontée depuis une quinzaine d'années à des défis majeurs parmi lesquels : le vieillissement de la population, qui s'accompagne de l'accroissement de pathologies chroniques complexes à prendre en charge, la baisse des effectifs de professionnels de santé et leur inégale répartition géographique, ainsi que l'exigence de qualité toujours plus forte des soins prodigués.

L'émergence progressive de ces enjeux est concomitante avec les évolutions sans précédent des technologies de l'information et de la communication (TIC) : développement des capacités de stockage des données numériques, des systèmes d'information permettant leur exploitation, des réseaux les transportant, et la démocratisation d'internet qui ouvre l'appropriation de ces nouveaux usages.

De sorte que, l'intégration des technologies de l'information dans le domaine de la santé est aujourd'hui une réalité et va encore s'accroître significativement dans les années à venir. Elles participent aux mutations en cours et permettent de répondre aux défis que doit relever un système de santé modernisé et qui sont :

• la coordination accrue des professionnels de santé dans la prise en charge de leurs patients, qui s'appuie notamment sur le partage et l'échange d'informations.

• l'accès de tous à des soins de qualité, dans un contexte de démographie médicale défavorable, qui nécessite la mise en place de nouvelles pratiques relevant de la télémédecine (1). La téléconsultation est en ce sens exemplaire car elle permet un accès à des compétences spécialisées souvent éloignées. Elle optimise les déplacements des patients vers les spécialistes. Elle régule également l'activité des spécialistes, en limitant le risque d'embouteillage provoqué par le manque d'effectif dans les principales spécialités, et l'afflux d'actes qui auraientt pu être traités dans le premier recours.

• la qualité des soins par l'informatisation, par exemple, du circuit du médicament en établissement de santé, de la prescription par les médecins jusqu'à l'administration des médicaments aux patients.

Toutefois, le développement accéléré de la numérisation des données de santé de chaque citoyen-patient n'est pas sans poser de nouvelles questions éthiques et juridiques quant à la protection des données personnelles de santé des citoyens-patients. Cet article propose une cartographie des enjeux juridiques posés par le déploiement des technologies de l'information et de la communication dans le système de santé. Il fait le point sur la protection des données personnelles de santé et les problématiques qui n'ont aujourd'hui pas de réponses claires, que ce soit aux niveaux de la collecte des données dans le cadre d'un partage entre professionnels, de l'exercice du droit d'accès et de communication du dossier patient, de l'exercice du droit d'opposition, et enfin de la sécurité et la confidentialité des données patients.

LA COLLECTE DES DONNÉES DANS LE CADRE D'UN PARTAGE ENTRE PROFESSIONNELS

Les informations relatives à la santé des personnes sont des données sensibles au sens de l'article 8 de la loi Informatique et libertés du 8 janvier 1978, modifiée le 6 août 2004. A ce titre, les responsables de traitements sont soumis à des obligations renforcées au niveau de la collecte de ces données et des mesures de sécurité (2).

En effet, le principe général de l'article 8 de ladite loi est l'interdiction de traiter ce type de données (3), sauf consentement exprès de la personne concernée (4).

Fort heureusement, ce principe souffre d'une exception dans la sphère santé, puisque la simple information du patient est admise pour collecter ses données médicales dans le cadre de « *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 » (5), lorsque ceux-ci sont « mis en œuvre 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* » (6).

C'est en ce sens, par exemple, que la norme simplifiée de la Cnil relative à la gestion des cabinets libéraux des professionnels de santé (7) précise que : « les personnes dont les données sont enregistrées et conservées dans le fichier du cabinet sont informées, par un document affiché dans les locaux du cabinet médical ou paramédical ou remis en main propre, de l'identité du responsable du traitement, de sa finalité, des destinataires des informations et des modalités pratiques d'exercice de leurs droits, en particulier du droit d'accès aux informations qui les concernent » (8).

Il ressort de cette norme simplifiée de la Cnil, que l'information du patient doit être suffisamment claire et précise, afin de respecter le principe de collecte loyale (9) et les exigences de l'article 32 de la loi Informatique et libertés concernant les obligations d'information qui incombent aux responsables de traitements.

En revanche, dès lors que les données personnelles du patient sont hébergées auprès d'un prestataire de service, ou si celles-ci sont partagées avec d'autres destinataires que les professionnels de santé (10) ou les membres de l'équipe de soins (11) prenant en charge la personne, hors les cas prévus par la loi ou les normes de la Cnil (12), le recueil du consentement préalable a vocation à s'appliquer de nouveau (cf. §4.).

Le dossier pharmaceutique (13), dont le traitement est actuellement partagé entre 16 756 officines de ville (14) (sur un total d'un peu moins de 23 000 officines), illustre parfaitement cette exigence de loyauté pour le recueil du consentement exprès. En effet, ce consentement exprimé auprès d'un pharmacien d'officine s'effectue après avoir pris connaissance des informations figurant sur le dépliant d'informations du dossier pharmaceutique, dont le modèle, validé par la CNIL, a été élaboré par le Conseil national de l'ordre des pharmaciens.

Suite à cette information, la création du dossier peut avoir lieu et le pharmacien remet alors une copie papier de l'attestation de création dûment remplie au bénéficiaire ou à son représentant légal, qui y confirme son consentement (15). Le patient qui s'y inscrit consent alors à l'ouverture de son dossier, au partage de ses informations entre les officines pharmaceutiques, ainsi qu'à l'hébergement de ses données chez un prestataire désigné par l'Ordre national des pharmaciens (conformément à l'article L. 1111-8 du Code de la santé publique).

Cet automne, l'Agence des systèmes d'information partagés de santé (ASIP Santé) (16) doit publier, en association avec des représentants des patients, des professionnels de santé et de la Cnil, un guide pratique précisant, pour chacune des situations d'exercice des professionnels de santé, si c'est le régime d'information ou de consentement qui s'applique. Ce guide a pour objectif d'aider les professionnels à mettre en œuvre les procédures d'information et/ou de recueil du consentement garantissant le caractère libre et éclairé de l'accord des patients.

Cette démarche est fondamentale, puisque de la qualité de cette information et des modalités pratiques de la mise en place du consentement dépend l'effectivité de l'exercice des droits d'accès, de rectification et d'opposition de la loi Informatique et libertés.

L'orientation de ce guide devrait annoncer la volonté des pouvoirs publics de privilégier une expression dématérialisée du consentement. Ce consentement (17) pourra être recueilli par les professionnels de santé mais aussi par le personnel d'accueil des structures de soins.Cette dématérialisation du consentement doit toutefois s'accompagner d'une information des patients par la remise d'une plaquette explicative relative aux objectifs du traitement et à leurs droits Informatique et libertés. Ce choix de la dématérialisation du consentement est également annoncé pour le décret à venir relatif à la télémédecine.

Nous pensons que cette probable généralisation du consentement dématérialisé devra s'accompagner d'un travail de pédagogie auprès des patients, qui pourra être porté notamment par les associations de patients.

L'EXERCICE DU DROIT D'ACCÈS ET DE COMMUNICATION DU DOSSIER PATIENT

« *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* » (18).

Ce droit d'accès s'applique à l'ensemble des informations concernant la santé, détenues, à quelque titre que ce soit, par des professionnels et établissements de santé, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé. Il s'agit, notamment, des résultats d'examen, comptes-rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en oeuvre, des feuilles de surveillance et 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 (19).

Concrètement, l'accès aux informations relatives à la santé d'une personne, mentionnées à l'article L. 1111-7 du code de la santé publique, et détenues par un professionnel de santé, un établissement de santé ou un hébergeur agréé, peut être demandé

par la personne concernée, son ayant droit en cas de décès, la personne ayant l'autorité parentale, le tuteur ou, le cas échéant, par le médecin qu'une de ces personnes a désigné comme intermédiaire (20). La demande est alors adressée au professionnel de santé ou à l'hébergeur et, dans le cas d'un établissement de santé, au responsable de cet établissement ou à la personne qu'il a désignée à cet effet et dont le nom est porté à la connaissance du public par tous moyens appropriés (21).

Enfin, le code de la santé publique prévoit que le délai de communication doit être réalisé au plus tard dans les huit jours suivant la demande et au plus tôt après qu'un délai de réflexion de quarante-huit heures aura été observé. Ce délai peut être porté à deux mois lorsque les informations médicales datent de plus de cinq ans (22). Néanmoins, force est de constater que l'exercice du droit d'accès et de communication du dossier patient n'est pas aisé dans la pratique.

Le Président de l'association INJENO (23), Monsieur Luc Masson, papa d'une petite fille polyhandicapée (Inès), nous a fait part de son retour d'expérience qui illustre les difficultés de nombreux parents confrontés aux parcours de soins de leurs enfants. Dans un premier temps, les parents de la petite Inès ont obtenu sans trop de difficultés une copie de son dossier médical de naissance pour une prise en charge hospitalière en dehors de leur ville de domiciliation. Cependant son dossier était très incomplet : peu des événements qui étaient survenus lors de l'accouchement avaient été reportés dans le compte-rendu officiel.

A ce titre, il est utile de préciser que les informations de santé formalisées, au sens de l'article L. 1111-7 du code de la santé publique, doivent être comprises au plus simple : « *il s'agit des informations auxquelles est donné un support (écrit, photographie, enregistrement, etc.) avec l'intention de les conserver et sans lequel elles seraient objectivement inaccessibles* (24) » .

De sorte que, « *le mot « dossier » ne doit pas être envisagé de manière restrictive, car toutes les informations formalisées détenues par un professionnel, un établissement de santé ou un hébergeur en dehors du dossier sont communicables* » (25) .

C'est uniquement « *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* » (26).

Ensuite, le parcours de soins d'Inès l'amène à rencontrer des professionnels du cerveau exerçant dans différents hôpitaux parisiens et régionaux. Là encore, les communications de ses différents dossiers médicaux pèchent par leur manque d'exhaustivité.

Ainsi, le dossier « papier » que remet le premier établissement où les soins ont été prodigués n'a jamais été complet (résultats d'EEG, d'IRMs, de prises de sang), de sorte que les professionnels de santé destinataires de ce document vital ont eu une vision incomplète de l'histoire médicale de l'enfant, entraînant de facto de nouveaux examens parfois stressants ou invasifs. Dans le cas du polyhandicap pas moins de quatre spécialités médicales sont susceptibles de collaborer à la prise en charge de l'enfant : neurologue (neuropédiatre) généticien, orthophoniste, pédiatre.

Idéalement, l'association INJENO aimerait que « *toutes les informations concernant les parcours de soins des enfants puissent être stockées chez un hébergeur spécialisé avec toutes les garanties de sécurité que la nature de ces données impose. Ainsi, suivant des droits d'accès définis conjointement par les parents et l'hébergeur, tous les professionnels de santé, quelle que soit leur spécialité, auraient accès à un dossier complet, fidèle au parcours de santé du patient pris en charge, même si leur intervention n'est que ponctuelle* ». Dans les établissements de santé, c'est au médecin DIM (27) qu'incombe la tâche de consolider les dossiers médicaux des patients et de vérifier que ceux-ci comprennent les éléments définis à l'article R. 1112-2 du code de la santé publique.

Rappelons que des manquements relatifs à l'information contenue dans les dossiers médicaux peuvent constituer des anomalies sanctionnées par les agences régionales de santé et constituer un motif légitime de retrait d'autorisation pour un établissement de santé (28).

L'EXERCICE DU DROIT D'OPPOSITION

L'article 38 de la loi Informatique et libertés permet à toute personne de s'opposer « *pour des raisons légitimes* » à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. De plus, la partie législative du Code de la santé publique prévoit, dans son article L. 1110-4, un droit d'opposition du patient à l'échange d'informations entre deux professionnels de santé qui le prennent en charge afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible.

Il peut donc se poser le cas de figure du patient refusant l'enregistrement de ses données dans un système d'information de santé ou en demandant la suppression.

Néanmoins, le droit d'opposition ne peut s'exercer que pour des motifs légitimes (29) et il ne s'applique pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ce droit a été écartée par une disposition expresse de l'acte autorisant le traitement.

La Cnil a ainsi considéré comme légitime le cas d'un patient, suivi aux Hospices civils de Lyon, qui avait demandé l'effacement des informations relatives à ses différentes hospitalisations conservées sur support informatique au motif que, atteint d'une affec-

tion, et ayant appris que son beau-frère médecin avait été nommé dans cet hôpital, il craignait que la consultation du système informatique par ce dernier permette à ses proches de connaître la nature de sa pathologie, alors qu'il ne souhaitait pas la révéler (30).

Dès lors, en cas de refus de suppression suite à la demande d'un patient qui considèrerait que certaines de ses données de santé n'ont plus à figurer dans son dossier, il reviendra au professionnel de santé ou à l'établissement, responsable du traitement, de démontrer la nécessité de conserver ces informations médicales. Au final, seule l'appréciation souveraine des tribunaux pourra trancher le litige.

En revanche, en cas d'accord entre le patient et son médecin, il est utile de préciser que l'effacement de ses données devra alors s'effectuer également auprès d'autres professionnels de santé dès lors qu'il y a eu partage de celles-ci.

Toujours dans un souci de traçabilité et donc de véracité de l'information médicale, la Cnil recommande dans ce cas que la mention de cette suppression soit conservée dans le fichier.

A noter que l'effacement d'une donnée sur le dossier informatique n'interdit pas qu'elle fasse l'objet par ailleurs d'un archivage chez le professionnel de santé, soit sur un support informatique distinct, soit sur un support papier (31).

LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES DE SANTÉ DES PATIENTS

Les données de santé à caractère personnel sont des données sensibles susceptibles de révéler l'intimité de la vie privée. À ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objectif de garantir leur confidentialité.

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (32) a renforcé le principe du respect de la vie privée de toute personne prise en charge par un professionnel, un établissement de santé ou un réseau de santé (33). Cette loi introduit des dispositions afin de garantir aux patients une protection à la fois juridique et technique relatives à ses données de santé, tant au niveau des échanges que du partage.

Une de ces protections juridiques décrites dans le code de la santé publique s'articule avec les dispositions du code pénal et concerne les sanctions applicables en cas de violation du secret professionnel (34). D'autres sanctions s'appliquent en cas de manquements à l'obligation de sécurité du responsable de traitement (35) (loi Informatique et libertés du 6 janvier 1978, modifiée le 6 août 2004) (36).

Plusieurs décrets concernant l'obligation de sécurité du responsable de traitement ont été publiés, mais leur application s'avère laborieuse, ce qui pose des difficultés aux professionnels de santé dans l'exercice de leurs pratiques.

L'addition successive de textes a mis en lumière une inadaptation face à une réalité des pratiques qui s'accommodent difficilement de garanties lacunaires ou partielles. L'application des règles quant à la sécurité et à la confidentialité est compliquée par la multiplicité des niveaux de réglementation. Ces lacunes, ce manque de clarté et d'uniformité dans l'application des règles peuvent avoir des effets pervers.

En effet, bien que les organismes de santé aient une obligation renforcée d'assurer la confidentialité et la sécurité des données, ils doivent néanmoins veiller à ce que l'information puisse être facilement accessible lorsqu'elle est requise pour la prestation des soins, en particulier dans les situations d'urgence.

Ainsi, « *la confidentialité des informations médicales [...], 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* » (37).

Ce décret, dit décret « confidentialité », a été publié le 15 mai 2007 (38) et codifié aux articles R. 1111-1 à R. 1111- 3 du code de la santé publique. Il précise les mesures techniques et organisationnelles à mettre en œuvre en termes de sécurité et de confidentialité.

Ce décret d'application de l'article L. 1110-4 du code de la santé publique soumet notamment les professionnels de santé à l'obligation d'utiliser la Carte de professionnel de santé (CPS) (39) pour l'accès, l'échange et le partage des données de santé. Cette carte permet notamment d'authentifier son porteur et de tracer les actions de celui-ci.

Aujourd'hui, après plusieurs expérimentations lancées de l'utilisation de la CPS dans des établissements de santé, il semble difficile d'envisager sa généralisation en l'état. En effet, « *l'usage de la CPS [s'inscrit] dans un contexte caractérisé par : les difficultés des premiers sites expérimentaux à assurer la pérennité de leurs solutions applicatives ; la faiblesse de la dynamique de déploiement, en raison notamment de l'absence de services associés à la carte et d'industrialisation des solutions ; le développement croissant de cartes d'établissements multifonctions ; la réticence de nombre d'établissements à payer leurs cartes, ce qui génère des créances douteuses dans les comptes du GIP CPS* » (40).

De plus, la non-utilisation de la CPS met les professionnels et les établissements de santé en situation délicate puisque cette obligation s'impose à tous depuis le 15 mai 2010 (41).

Le décret « confidentialité » prévoit, par ailleurs, la publication d'arrêtés devant définir les règles de sécurité et de confidentialité. En effet, l'article R. 1110-1 du code de la santé publique prévoit que ces référentiels soient définis par arrêtés du ministre

chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés.

Or, trois ans et demi plus tard, ces arrêtés ne sont toujours pas publiés ! Mais est-ce aux pouvoirs publics d'élaborer les référentiels qui déterminent « les *fonctions de sécurité nécessaires à la conservation ou à la transmission des informations médicales en cause et fixant le niveau de sécurité requis pour ces fonctions* » (42) ? Il est aujourd'hui question de l'abrogation de ce décret « confidentialité », ce qui sortirait les professionnels et établissements de santé d'une situation délicate. Un nouveau décret est en cours d'élaboration.

Enfin, la loi du 4 mars 2002 autorise l'externalisation de l'hébergement, chez une personne physique ou morale, de « *données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* », qu'à la condition que ce dernier soit préalablement agréé. Ces dispositions ont pour objectif d'organiser et d'encadrer le dépôt, la conservation et la restitution des données de santé à caractère personnel, dans des conditions de nature à garantir leur confidentialité et leur sécurité.

Dans ce cas, le patient doit être informé que ses données vont être hébergées chez un tiers et le recueil de son consentement exprès est obligatoire .

Le décret du 4 janvier 2006 fixe les conditions d'agrément des hébergeurs de données de santé à caractère personnel. Il est délivré par le ministre en charge de la santé, après avis motivé d'un comité d'agrément et de la Cnil, pour une durée de trois ans.

Les principales conditions pour obtenir cet agrément sont d'offrir toutes les garanties pour l'exercice de l'activité d'hébergement, notamment par la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées. Elles sont également de définir et mettre en œuvre une politique de confidentialité et de sécurité, d'individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés et, enfin, d'identifier les personnes en charge de l'activité d'hébergement, dont un médecin.

Au 30 septembre 2010, la ministre de la Santé et des Sports avait délivré douze agréments. Certains de ces agréments ont été délivrés pour l'hébergement de dossiers déployés sur tout le territoire national, tels que le Dossier pharmaceutique et le dossier médical personnel qui doit être lancé au mois de décembre 2010. D'autres ont été délivrés à des sociétés hébergeant des dossiers patients d'établissements ou de groupement d'établissements.

Si la procédure d'agrément semble apporter les garanties de sécurité et de confidentialité des données de santé à caractère personnel qui sont confiées à ces hébergeurs, on imagine la volonté des pouvoirs publics de voir progressivement les acteurs de santé faire héberger les données de leurs patients. La question est donc de savoir si les industriels vont pouvoir tous offrir cette prestation d'hébergement avec des coûts supportables par la collectivité et les acteurs privés (assureurs, mutuelles, laboratoires, ...).

Le succès ou l'échec de la mise en œuvre des pratiques médicales associées aux technologies de l'information dépendra notamment de la confiance quant à la sécurité et la confidentialité des données de santé numérisées et échangées ressentie par tous. Toutefois, cette seule confiance ne sera pas suffisante. L'appropriation de la e-santé par les patients-citoyens et les professionnels de santé nécessitera une politique active de la gestion du changement pour l'acceptation de ces nouveaux outils. L'année 2011, avec notamment la mise en place du dossier médical personnel, devrait être une année de réels retours d'expériences qui viendront consolider les pratiques en la matière.

Nicolas SAMARCQ
Juriste
Consultant TIC / Cnil
LEXAGONE

Sébastien BRIOIS
Cofondateur de la société de conseil Acsantis
Animateurs du groupe de travail « Données de Santé » de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel)

(1) La télémédecine est définie par la loi n° 2009-879 du 21 juillet 2009 comme « une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé [...] »
(2) Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé. Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique.
(3) Article 8-I de la loi Informatique et libertés : « Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ».
(4) Article 8-II 1°) de la loi Informatique et libertés : « Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :
1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ».
(5) Article 8-II. 6°) de la loi Informatique et libertés.
(6) Ibidem.
(7) Norme simplifiée n°50 : Délibération n°2005- 296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet.
(8) Article 6 de la norme simplifiée n° 50
(9) Article 6-1°) de la loi Informatique et libertés : « Les données sont collectées et traitées de manière loyale et licite ».
(10) Article L. 1110-4 du Code de la santé publique : « Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible ».
(11) Article L. 1110-4 du code de la santé publique : « Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe ».
(12) Article 4 de la norme simplifiée n° 50 : sont

destinataires des informations :
« - Afin d'assurer la continuité des soins et avec l'accord de la personne concernée, les professionnels de santé et dans les établissements de santé, les membres de l'équipe de soins, chargés de la prise en charge du patient peuvent être destinataires des données figurant dans l'application.
- Les personnes affectées à la gestion du secrétariat n'ont accès, dans le respect des dispositions sur le secret professionnel, qu'aux informations relatives à la gestion du cabinet et en particulier à la gestion des rendez-vous.
- Afin de permettre le remboursement des actes, des prestations et leur contrôle, les personnels des organismes d'assurance maladie ont connaissance, dans le cadre de leurs fonctions et pour la durée nécessaire à l'accomplissement de celles-ci, de l'identité de l'assuré, de son numéro de sécurité sociale et du code des actes effectués et des prestations servies. Outre ces données, les médecins conseils des caisses accèdent au code des pathologies diagnostiquées dans les conditions définies à l'article L. 161-29 du code de la sécurité sociale.
- Les personnels des organismes d'assurance maladie complémentaire sont destinataires dans le cadre de leurs attributions, de l'identité de leurs assurés, de leur numéro de sécurité sociale et sous la forme de codes regroupés, aux catégories des actes et prestations effectués.
- Les organismes de recherche dans le domaine de la santé et les organismes spécialisés dans l'évaluation des pratiques de soins peuvent être destinataires de données personnelles de santé dans les conditions définies par la loi du 6 janvier 1978 modifiée ».
(13) Le dossier pharmaceutique permet au pharmacien d'avoir accès à l'historique des médicaments délivrés au cours des quatre derniers mois, afin de déceler les risques d'interactions médicamenteuses qui constituent un danger pour les personnes.
(14) Au 20 septembre 2010, 9 725 704 dossiers pharmaceutiques ont été créés dans 16 756 officines, http://www.ordre.pharmacien.fr/DP/index4.htm. La France compte 23 000 officines.
(15)
(16) L'ASIP Santé est l'opérateur public chargé du développement des systèmes d'information de santé www.esante.gouv.fr.
(17) Accord oral tracé informatiquement.
(18) Article 43 de la loi Informatique et libertés.
(19) Article L. 1111-7 du code de la santé publique.
(20) Article R. 1111-1 du code de la santé publique.
(21) Ibidem.
(22) Ibidem.
(23) Association de parents d'enfants, d'adolescents et d'adultes polyhandicapés et neurolésés, www.injeno.fr.
(24) 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, JORF n°65 du 17 mars 2004 page 5206.
(25) Ibidem.
(26) Ibidem.
(27) Médecin responsable du Département d'Information Médicale.
(28) Arrêt du Conseil d'Etat du 26 juillet 2006 : en l'espèce retrait d'autorisation d'une clinique pour mauvaise tenue des dossiers médicaux des patients par le personnel paramédical.
(29) Article 38 de la loi Informatique et libertés : « 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.
Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.
Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement ».
(30) 15ème rapport d'activité de la Cnil, 1995.
(31) Circulaire n° 2005-068 du 28 juillet 2005 du Conseil départemental de l'ordre des médecins de la Marne, Section Ethique et Déontologie.
(32) Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JORF du 5 mars 2002 page 4118.
(33) La loi du 4 mars 2002 pose l'article L1110- 4 du code de la santé publique : « 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 au secret des informations la concernant ».
(34) Article 226-13 du code pénal : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende ».
(35) Art. 226-17 du code pénal : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».
(36) Article 34 : « 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 ».
(37) Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique, JORF n°113 du 16 mai 2007 page 9362.
(38) Ibidem.
(39) Art. R. 1110-3. En cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire.
(40) Les systèmes de cartes de l'Assurance Maladie, rapport public annuel 2010 de la Cour des comptes.
(41) Cette obligation s'applique pour les professionnels de santé qui exercent en libéral depuis le 15 mai 2007 !
(42) Art. R. 1110-1 du code de la santé publique.
(43) Il existe une dérogation à la nécessité de recueillir le consentement du patient lorsque « Les professionnels et établissements de santé peuvent, par dérogation [...], utiliser leurs propres systèmes ou des systèmes appartenant à des hébergeurs agréés, sans le consentement exprès de la personne concernée dès lors que l'accès aux données détenues est limité au professionnel de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée dans les conditions prévues par l'article » (article L. 1111-8 al.5 du code de la santé publique).
(44) Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JORF n°4 du 5 janvier 2006 page 174.
(45) Le comité d'agrément est constitué d'un membre de l'Inspection des affaires sociale, de deux représentants des associations compétentes en matière de santé, de deux représentants des professionnels de santé et de trois personnalités qualifiées dans les domaines de l'éthique et du droit, de la sécurité des systèmes d'information, et dans le domaine économique et financier.