Délibération CNIL n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel

02/12/2010

La Commission nationale de l'informatique et des libertés ;

Saisie par l'Agence des Systèmes d'Information Partagés (ASIP Santé) le 8 octobre 2010, d'une demande d'autorisation relative aux applications informatiques mises en œuvre au sein des établissements de soins et par les professionnels de santé qui seront nécessaires à la première phase de déploiement généralisé du dossier médical personnel;

Vu la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la 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 de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment ses articles 8-IV et 25-I, 1 ;

Vu les articles L.1110-4, L.1111-7, L.1111-8, L.1111-8-1, L.1111-14 à L.1111-24 et R.1111-9 à R.1111-16 du code de la santé publique ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ; Vu l'article L.162-5-3 du Code de la sécurité sociale ;

Vu la délibération n°2010-351 du 30 septembre 2010 portant avis sur la demande d'agrément présentée par la société Santeos à l'hébergement des données de santé à caractère personnel du dossier médical personnel (DMP1);

Après avoir auditionné M. Michel Gagneux, M. Jean-Yves Robin, et Mme Jeanne Bossi, respectivement Président, Directeur Général et Secrétaire Général de l'Agence des Systèmes d'Information Partagés de santé (ASIP) sur les grands axes du programme de relance du Dossier Médical Personnel, le 22 octobre 2009;

Après avoir entendu M. Jean MASSOT, commissaire, en son rapport, et Mme Elisabeth ROLIN, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :
L'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) a saisi la Commission nationale de l'informatique et des libertés le 8 octobre 2010, d'une demande d'autorisation relative aux traitements de données à caractère personnel qui seront nécessaires à la mise en œuvre du déploiement généralisé du Dossier Médical Personnel (DMP).

La présente demande intervient dans le cadre de la relance du projet, qui devrait être mise en œuvre selon une trajectoire développée par étapes et orientée sur la notion de services rendus aux patients et aux professionnels de santé.

Au cours d'une première phase, objet de la présente demande d'autorisation, un dossier patient « socle » permettra le déploiement, à l'échelle nationale, des services initiaux de partage de documents (comptes-rendus hospitaliers, de radiologie, résultats d'analyse de biologie…) entre professionnels de santé en charge du suivi du patient sous le contrôle de ce dernier.

Cette première phase de déploiement du DMP, appelée DMP 1, devrait durer trois ans.

Progressivement, le DMP offrira des services supplémentaires « à valeur ajoutée » axés sur la prise en charge de pathologies particulières telles que le diabète ou sur des techniques spécifiques (imagerie médicale, prescription électronique), ce qui devra donner lieu à de nouvelles formalités préalables auprès de la CNIL si leur mise en œuvre modifie le périmètre et les principes de fonctionnement du DMP.

Le DMP1 reposera sur une infrastructure technique d'hébergement national, assurée par le groupement solidaire d'entreprises constitué des sociétés Santeos, Atos Wordline (filiales d'ATOS Origin) et Extelia (Filiale du groupe La Poste), groupement qui a été retenu à l'issue d'un appel d'offres lancé en 2009 par l'ASIP Santé.

Lors de sa séance du 30 septembre 2010, la Commission s'est prononcée sur la candidature à l'agrément de ce groupement en qualité d'hébergeur du DMP1, conformément aux dispositions de l'article R. 1111-10 du Code de la santé publique. Cette candidature a été depuis, et conformément aux dispositions du décret n° 2006-6 du 4 janvier 2006, examinée par le comité d'agrément des hébergeurs placé auprès du ministre de la santé qui a, par décision du 10 novembre 2010, décidé de son agrément.

Cadre juridique du dossier médical personnel

Le Dossier Médical Personnel (DMP) a été créé par la loi du 13 août 2004 relative à l'assurance maladie, dans un souci affirmé d'une amélioration de la coordination, de la continuité, donc de la qualité des soins.

La volonté du législateur de créer ce dossier a été confirmée par la loi n°2009-879 du 21 juillet 2009, portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, dite « loi HPST » qui a transféré dans le Code de la santé publique les dispositions relatives au DMP (C. santé publ., art. L.1111-14 à L.1111-24).

L'article L.1111-14 du Code de la santé publique prévoit :

« 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 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, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention.
Ce dossier médical personnel est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8 ».

La Commission rappelle qu'une expérimentation du dispositif, autorisée par elle le 30 mai 2006, a été conduite de juin à décembre 2006 dans treize régions et dix-sept sites pilotes retenus par le groupement d'intérêt public du dossier médical personnel (le GIP-DMP). Elle avait pour objet de tester la faisabilité et l'acceptabilité de ce dispositif.

Annoncée en 2007, la généralisation du DMP a été sans cesse reportée. Le projet a fait l'objet d'un « audit », d'une revue de projet et est aujourd'hui en cours de relance. Cette relance est désormais placée sous la responsabilité de l'Agence des Systèmes d'Information Partagés de santé, qui en assure la maîtrise d'ouvrage.

L'ASIP Santé a défini la finalité de cette première phase de déploiement et les moyens à mettre en œuvre pour y parvenir, en particulier par la définition des conditions imposées au candidat hébergeur lors de l'appel d'offres qui a permis de le retenir. Il en va de même des applications mises en œuvre par les établissements et professionnels de santé qui devront se conformer aux cadres d'interopérabilité et de sécurité et de « DMP-compatibilité » définis par l'ASIP Santé.

Elle est donc considérée comme responsable des applications informatiques mises en œuvre chez les professionnels de santé et auprès des établissements de soins pour ce qui est nécessaire au fonctionnement du DMP.

La Commission observe que l'ensemble des textes qui commandent la mise en œuvre du DMP n'est pas aujourd'hui adopté. Deux textes de nature réglementaire prévus par la loi doivent encore lui être soumis.

- Le décret pris en application de l'article L.1111-21 du Code de la santé publique, qui aura vocation à déterminer le contenu et les conditions d'accès aux différentes catégories d'informations qui figurent dans le DMP.
- Le décret pris en application de l'article L.1111-8-1 du Code de la santé publique, qui doit déterminer la nature et les modalités d'utilisation de l'identifiant national de santé qui sera utilisé dans la cadre du DMP, mais plus largement dans l'ensemble du système de santé.

La Commission admet que l'élaboration du cadre juridique dépend de retours d'expériences. Comme elle l'a elle-même déploré, les expérimentations conduites en 2006 n'ont pas permis de tirer des enseignements sur les conditions d'utilisation du DMP.

La Commission rappelle qu'elle avait considéré en 2006 qu'il était admissible de se prononcer sur ces expérimentations sans que le cadre juridique soit complètement défini.

Elle admet, en outre, que le cadre juridique dans lequel le DMP va se déployer doit être apprécié au regard de la nouvelle gouvernance du projet qui a permis à l'ASIP Santé, à travers l'élaboration de référentiels, de préciser le cadre de déploiement du DMP au regard, en particulier, du niveau de sécurité qui doit entourer la mise en œuvre du projet.

Compte tenu de ces précédents, de ce nouveau contexte et malgré l'insuffisance du cadre juridique, la Commission se prononce en l'état sur la première phase de déploiement généralisé du projet.

Elle considère toutefois que la définition d'un cadre juridique stable est indispensable à la conduite de ce projet. La deuxième phase de déploiement du DMP devra donc s'inscrire dans le cadre réglementaire qui aura été fixé en ce qui concerne, en particulier, le contenu du DMP et ses conditions d'accès, ainsi que la nature de l'identifiant national de santé et ses modalités d'utilisation.

La Commission estime, en outre, devoir être saisie, à l'appui de cette nouvelle demande, des évaluations réalisées au cours de la première phase de déploiement et à son terme.

Emet dans ces conditions la décision suivante :

Sur la finalité et le périmètre du projet

Dans le cadre de cette première phase de déploiement du projet, la finalité principale du dispositif est la généralisation immédiate et progressive sur l'ensemble du territoire des services initiaux de partage de documents, c'est à dire la possibilité offerte aux bénéficiaires de l'assurance maladie de disposer d'un dossier médical personnel et partagé entre professionnels de santé.

Il s'agit de mettre l'ensemble des professionnels de santé en mesure de partager des documents obéissant à un format normalisé et commun, avec l'accord et sous le contrôle du patient.

Le DMP n'a pas vocation à se substituer aux dossiers papier ou informatisés établis dans les cabinets des médecins libéraux et dans les établissements de santé, mais à s'y ajouter.

Un autre des objectifs de cette première phase de déploiement du DMP sera de dégager des orientations qui vont permettre d'effectuer les choix qui seront finalement retenus par les textes encore à venir.

La Commission relève, à cet égard, que l'ASIP Santé procèdera en 2011 à une première évaluation de la mise en place du projet et souhaite être destinataire des résultats de cette évaluation.

Le déploiement progressif s'appuiera notamment sur la convergence de cinq projets régionaux. Dotés de structures de pilotage efficaces, ces projets régionaux, déjà impliqués dans des dispositifs d'échanges de données de santé, constitueront des relais essentiels pour le développement du DMP en région, pour accompagner les acteurs dans l'appropriation du dispositif et engendrer la confiance nécessaire. Le déploiement du DMP dans ces régions ira de pair avec l'arrêt des dispositifs régionaux expérimentaux qui assurent la même fonction.

Le DMP devra également être alimenté par les données du dossier pharmaceutique conformément aux dispositions de l'article L.1111-23 du Code de la santé publique. Toutefois, cette alimentation est renvoyée à une échéance plus lointaine.

Il est également envisagé, à terme, de permettre la consultation de l'historique des remboursements, prévu par l'article L.162-4-3 du Code de la sécurité sociale, à partir du DMP.

De nouvelles demandes d'autorisation devront être déposées en ce sens auprès de la CNIL et devront préciser les moyens d'assurer l'alimentation du DMP ou la consultation des données depuis le DMP dans le respect du cadre juridique, des droits des personnes et des règles de sécurité.

Sur les principes de fonctionnement du dossier médical personnel

Le dossier médical personnel est un dossier informatisé et hébergé par un organisme agréé, ouvert, pour chaque bénéficiaire de l'assurance maladie qui le souhaite, afin de permettre le regroupement et le partage entre les professionnels et établissements de santé qui le prennent en charge, des informations nécessaires à la coordination des soins. Il sera constitué notamment des informations qui permettent le suivi des actes et prestations de soins.

Tout bénéficiaire de l'assurance maladie doté d'une carte Vitale individuelle pourra ouvrir un DMP auprès d'un professionnel de santé ou à l'accueil d'un établissement de soins et y accéder directement, s'il le souhaite, depuis son ordinateur personnel.

La création d'un DMP est volontaire et chaque patient donne son consentement à sa création. Le patient a également la faculté de fermer son DMP à tout moment en s'adressant à un professionnel de santé ou au médecin de l'hébergeur. Le DMP sera alors archivé pendant dix ans, conformément aux dispositions de l'article L.1111-18 du Code de la santé publique, à l'issue desquels le dossier sera supprimé. Pendant ces dix ans, le DMP pourra être réactivé à la demande du patient. Une suppression définitive est également possible sans délai à sa demande.

Chaque professionnel de santé, qu'il exerce en ville ou à l'hôpital, devra compléter le DMP à l'aide des documents qu'il juge utiles à la coordination des soins, sous réserve de l'accord du patient dans les conditions définies ci-après.

Après la mise à jour des logiciels « métiers » par les éditeurs de logiciels selon les exigences définies par l'ASIP Santé, les

systèmes d'information existants seront en mesure de « communiquer » avec le DMP sans ressaisie de la part du professionnel. S'ils n'ont pas encore adapté leurs outils métiers, les professionnels accèderont au DMP sur internet à partir du site dmp.gouv.fr.

Sur l'identification du patient

Pour associer sans risque d'erreur un patient et son DMP, ce dernier sera identifié provisoirement par un identifiant national de santé calculé, dénommé « INS-C », dans l'attente de la mise en œuvre de l'identifiant national de santé, prévu par l'article L. 1111-8-1 du Code de la santé publique.
L'INS-C, dérivé par hachage de traits d'identité figurant sur la carte Vitale de l'assuré (NIR, jour de naissance, prénom), sera calculé automatiquement et localement par les logiciels métiers des professionnels. Ainsi créé à l'occasion de la proposition d'ouverture d'un DMP, cet identifiant sera adressé à l'hébergeur et conservé par lui. Il pourra également être stocké dans les logiciels des professionnels de santé.

La Commission rappelle, comme elle l'a indiqué par courrier du 25 novembre 2009, que l'utilisation d'un INS ainsi calculé est envisageable, dans l'attente de la mise en place de l' INS aléatoire prévu à terme. Cela permet, en effet, d'améliorer l'identification des patients dans le cadre de projets impliquant des échanges et partages d'informations et apparaît conforme aux préconisations de la CNIL de recourir à un identifiant spécifique, non signifiant, fondé sur une anonymisation du NIR.

Toutefois, l'INS-C ne permet pas d'apporter la garantie absolue de non collision et d'absence de doublon et tous les bénéficiaires de l'assurance maladie n'en seront pas dotés. C'est pourquoi l'acceptation de cette solution provisoire ne vaut pas accord pour qu'elle se perpétue au-delà de ce qui est nécessaire et suffisant pour mettre en place l'INS aléatoire.

En outre et dans la mesure où la détention de la carte Vitale n'atteste pas de l'identité de son porteur, la Commission estime qu'il importe de rappeler aux personnels concernés qu'en cas d'indices pouvant faire douter de l'identité du porteur de la carte, il est de leur responsabilité de procéder aux vérifications indispensables.

La Commission prend acte qu'à l'occasion de la généralisation de l'INS-A, une conservation conjointe de l'INS-C et l'INS-A interviendra, qui n'aura pas vocation à être pérennisée puisque l'usage de l'ISN-C sera interdit après la généralisation de l'INS-A.

Elle demande à être destinataire en temps utile des éléments techniques et juridiques liés à la mise en place de l'INS-A.

Sur l'information et le recueil du consentement du patient à la création d'un DMP

Le consentement du patient à l'ouverture d'un DMP à son nom est légalement requis, en tant qu'il est un dossier médical partagé et en tant qu'il est un dossier médical hébergé (C. santé publique, art. L.1111-8). L'article L.1111-8 du Code de la santé publique précise que le consentement à l'hébergement doit être un consentement « exprès ».

Il ressort du dossier soumis à la Commission que le consentement du patient à l'ouverture d'un DMP à son nom sera recueilli par un professionnel de santé ou le personnel d'accueil d'une structure de soins après remise d'une brochure d'information sous format papier, rédigée notamment pour assurer le respect des dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée.

Cette brochure comportera des informations relatives respectivement à l'identité du responsable du traitement (ASIP Santé) et de l'hébergeur (le groupement d'entreprises solidaires Atos-La Poste), à la finalité poursuivie par l'ouverture d'un DMP, à son contenu, aux modalités de création, d'alimentation, d'utilisation et de conservation, ainsi qu'aux conditions d'exercice des droits des patients.

Cette information individuelle sera complétée par la mise en place d'un site ouvert au public (dmp.gouv.fr) et par une campagne nationale de communication et de sensibilisation du public qui accompagnera progressivement le déploiement.

Il ressort, en outre, du dossier soumis à la Commission que l'ASIP Santé a fait le choix d'un recueil du consentement à l'ouverture d'un DMP qui puisse intervenir dès que l'information est délivrée.

- La Commission souhaite que la brochure d'information remise à l'assuré soit rédigée dans un langage clair, accessible à chacun et relève qu'elle fait mention de l'absence de conséquence du refus de création ou d'utilisation du DMP sur le remboursement des prestations par l'assurance maladie, ainsi que sur la mise en œuvre du tiers payant.

Ce document souligne, en outre, l'interdiction pour les organismes d'assurance, les mutuelles, les banques, les médecins du travail et les employeurs d'avoir accès au DMP, qui résulte l'article L.1111-18 du Code de la santé publique.

La Commission en prend acte avec satisfaction. Il importe, en effet, de sensibiliser les patients à la nécessaire confidentialité qui s'attache aux données de santé qui les concernent en raison de leurs potentialités discriminatoires et d'en appeler à la vigilance à l'égard des pressions qui pourraient être exercées à leur encontre.

Elle estime, toutefois, nécessaire que les spécificités du DMP au regard des autres dossiers médicaux (vocation à la pérennité, centralisation des données, portée nationale du partage) soient plus clairement soulignées. Seule une information claire, complète et explicite sur ce point est de nature à permettre aux patients de prendre clairement conscience de la portée de la démarche consistant à ouvrir un DMP compte tenu du risque d'amalgame entre le dossier médical personnel et le dossier médical du patient détenu par le médecin ou l'établissement.

La Commission estime, en outre, qu'il aurait été souhaitable que la campagne d'information et de sensibilisation du public soit antérieure au déploiement du DMP afin que les patients soient mis en mesure de connaître le dispositif avant que l'ouverture d'un DMP leur soit proposée et avant même qu'ils se trouvent dans la situation parfois critique du nécessaire recours au système de soins.

- Le consentement sera recueilli sous forme « dématérialisée ».

Le traitement comportera, à cet effet, la déclaration, sous forme électronique, par les personnels habilités à créer un DMP selon laquelle après avoir procédé à l'information indiquée plus haut, ils ont effectivement recueilli le consentement du patient ; cette déclaration se matérialisera par une croix dans une case à cocher prévue à cet effet.

La Commission estime que pour être satisfaisante et conforme aux textes, la procédure envisagée doit permettre le recueil d'un consentement qui soit éclairé et exprès.

Elle rappelle qu'elle n'a pas admis, à ce jour, que le recueil complètement dématérialisé du consentement du patient puisse valablement attester de l'expression d'un consentement explicite au partage de données de santé le concernant.

C'est ainsi que dans le cadre du Dossier Pharmaceutique, la Commission a estimé que la production et la remise au patient d'un document attestant du recueil de son consentement éclairé à l'ouverture d'un DP était de nature à conditionner la validité des modalités de recueil de son consentement et a pris acte des engagements du Conseil National de l'Ordre des Pharmaciens de contrôler l'effectivité de cette remise.

La Commission admet qu'on pourrait voir une certaine contradiction à vouloir matérialiser l'expression d'un consentement requis pour un dossier médical lui-même complètement dématérialisé.

Toutefois, étant donné le taux d'équipement informatique très inégal des personnes et le caractère limité du service qui ne sera généralisé que provisoirement sur l'ensemble du territoire, les patients qui bénéficieront, dans un premier temps, d'un accès par internet à leur DMP qui leur permettra d'en assurer personnellement la gestion seront en nombre limité.

Compte tenu de l'enjeu du dossier médical personnel en termes de protection des données à caractère personnel du fait notamment de son caractère national, la Commission estime qu'il importe de veiller à ce que le recueil du consentement à la création d'un DMP soit réel et que le patient puisse clairement apprécier les conséquences de l'accord qu'il donne. La Commission rappelle que la confiance des patients, inhérente à une bonne compréhension du DMP, est un gage de son succès.

A cet égard, la remise au patient d'un document formalisant son accord apparaît de nature à solenniser l'ouverture d'un DMP.

La Commission prend acte que, par un courrier du 1er décembre 2010, le Directeur de l'ASIP Santé s'est engagé à systématiser la remise au patient, lors de la création d'un DMP, d'un document qui attestera du recueil de son consentement exprès.

Sur l'information des professionnels de santé

Une brochure sera adressée à l'ensemble des professionnels de santé les informant de la finalité et des fonctionnalités du dispositif, de la conservation par l'hébergeur de données d'identité les concernant, des données relatives à leurs connexions à la plate-forme et leurs actions, ainsi que de leur droit d'accès et de rectification. Cette brochure leur rappellera également les obligations qui leur incombent au regard des droits des patients (informer, recueillir le consentement, faire droit aux oppositions, au droit de masquage…).

En outre, un guide de bonnes pratiques en matière d'information et de recueil du consentement, actuellement soumis pour avis au Conseil d'éthique et de déontologie de l'ASIP Santé, sera diffusé auprès d'eux.

La Commission en prend acte et demande que ces documents lui soient adressés.

Sur le droit d'accès du patient

La Commission relève que le patient pourra accéder à son DMP directement sur internet depuis son poste informatique. Ce mode d'accès a vocation à être généralisé progressivement sur l'ensemble du territoire.

La création d'un compte d'accès « patient » pourra intervenir à la création du DMP ou être réalisée ultérieurement par tout personnel habilité à créer un DMP.

Ainsi doté d'un compte internet, le patient sera en mesure d'accéder au contenu de son DMP ainsi qu'à un journal d'événements récapitulant les accès à son DMP qui précisera la date, l'heure et les opérations effectuées sur les données contenues dans son DMP.

Seuls certains documents « sensibles » pourront lui être rendus provisoirement invisibles, de même que les traces relatives à ces documents en l'attente d'un dialogue préalable avec le professionnel de santé, dans le cadre d'une « consultation d'annonce ».

La Commission en prend acte et demande que la brochure d'information soit complétée pour mentionner de façon explicite la possibilité d'un accès direct pour le patient à son DMP depuis un ordinateur relié à internet.

L'accès par Internet du patient à son DMP nécessitera un identifiant et un mot de passe initial qui sera communiqué au patient par le personnel habilité à initier un compte d'accès à la création du compte et devra obligatoirement être modifié lors de la première connexion. Ensuite, lors de chaque connexion, un mot de passe à usage unique (OTP) sera nécessaire et communiqué au patient par téléphone ou message électronique.

En cas de perte ou d'oubli, ce même personnel pourra à tout moment communiquer au patient de nouveaux codes d'accès et modifier le média de réception du code d'accès à usage unique, initialement choisi par le patient.

La Commission relève, en outre, que le compte d'accès sera bloqué pendant une heure après trois tentatives d'accès infructueuses sur une même session. Ces accès infructueux seront affichés dans le journal des traces du DMP accessible au patient et l'ASIP Santé assurera un suivi statistique des tentatives d'accès aux comptes « patient » et des blocages rencontrés.

Les modalités d'authentification du patient n'appellent pas, en tant que telles, d'observations de la part la Commission. Toutefois, celle-ci observe que la gestion de l'identifiant, du code accès provisoire et du média de réception de l'identifiant à usage unique sera centralisée auprès des professionnels de santé habilités à accéder au DMP.

Compte tenu que le personnel habilité à gérer un compte d'accès est en mesure de renseigner et de modifier le média de réception du mot de passe à usage unique, cette solution paraît contraire aux préconisations de la CNIL qui recommande de veiller à ce que l'ensemble des clés permettant l'accès et la modification d'une application ne puisse pas être concentré entre les mêmes mains.

La Commission estime, en conséquence, qu'une solution alternative devrait être recherchée afin de garantir la sécurité des accès.
- Le patient aura la possibilité d'exercer son droit d'accès à son DMP et à l'historique des traces, en formalisant une demande de copie auprès du « service en charge du support ».

Cette demande devra être effectuée à l'aide d'un formulaire disponible sur le site du DMP, accompagné des justificatifs nécessaires au contrôle de son identité. Le patient pourra obtenir ce formulaire en s'adressant à tout professionnel de santé habilité à accéder à son DMP qui pourra le lui imprimer, en le téléchargeant sur le portail du DMP ou en téléphonant au service de support aux utilisateurs qui le lui adressera.

Une copie sur support papier ou, à sa demande, sur CD-ROM de son DMP sera alors adressée au patient dans un délai de 8 jours par courrier avec accusé de réception à l'adresse indiquée dans le formulaire, après contrôle des pièces justificatives.

La Commission prend acte des engagements pris par l'ASIP Santé pour que toutes les précautions soient prises pour que ces documents soient bien remis à la personne concernée, conformément aux dispositions de l'article 34 de la loi du 6 janvier 1978, modifiée en 2004.

Elle prend acte également du fait que l'édition du dossier sera effectuée sous la responsabilité du médecin de l'hébergeur dans des conditions de sécurité physiques et logiques de nature à garantir la confidentialité.

La Commission relève, en outre, que le patient pourra obtenir un document, en s'adressant à un professionnel ou un établissement de santé qui sera en mesure de l'éditer et le journal des traces, en s'adressant au médecin traitant dont le rôle est défini ci-après.

La Commission estime que ces modalités sont de nature à permettre l'exercice du droit d'accès, conformément aux dispositions de l'article 39 de la loi du 6 janvier 1978, modifiée.

La maîtrise par le patient du contenu de son DMP et des accès à son DMP

Sur la définition du cercle de confiance,

Le DMP sera accessible aux seuls professionnels de santé auxquels le patient concerné aura souhaité ouvrir des droits et conféré, en conséquence, les autorisations d'accès nécessaires.

Ces autorisations d'accès, valables un an et renouvelables, seront délivrées par le patient lui-même (ou son représentant légal), s'il dispose d'un accès informatique personnel à son dossier qui lui permettra de gérer les droits d'accès à son DMP par internet. A défaut, la gestion de ces habilitations sera effectuée par les professionnels de santé qui se déclareront autorisés par le patient à sa demande à l'aide d'une case à cocher.

Lorsque l'autorisation d'accès sera délivrée à un établissement, l'ensemble des professionnels de santé appartenant à l'équipe de soins pourra y accéder, conformément aux dispositions de l'article L.1110-4 du Code de la santé publique.

Le patient se verra également reconnaître la possibilité de délivrer des interdictions d'accès à l'encontre d'un professionnel de santé, par l'inscription de celui-ci sur la liste des médecins « non autorisés » à accéder à son DMP. Cette faculté s'exercera directement par le patient s'il dispose d'un accès informatique personnel à son dossier ou par l'intermédiaire du médecin traitant dans le cas contraire.

Le médecin traitant aura également la possibilité de lever les interdictions d'accès à la demande du patient.

L'ensemble de ces opérations sera tracé et le patient sera en mesure d'exercer un contrôle a posteriori en accédant à l'historique des traces.

En outre, l'ASIP Santé envisage de prévoir, dans une version ultérieure du DMP, une notification par mail aux patients qui le souhaitent des ajouts et retraits de la liste des professionnels autorisés et du médecin traitant. La Commission prend acte de cette mesure qui sera de nature à améliorer les conditions de contrôle a posteriori des patients qui disposent d'un équipement informatique et d'un accès internet.

Le patient aura également la possibilité d'interdire l'accès en mode « bris de glace » (urgence ou SAMU) à son DMP dans les paramétrages de son compte d'accès Internet ou en s'adressant à un professionnel de santé, conformément aux dispositions de l'article L.1111-17 du Code de la santé publique.

Sur le rôle spécifique dévolu au médecin traitant dans la gestion d'un DMP et l'exercice des droits des patients

La Commission observe qu'en vertu des dispositions de l'article L. 162-5-3 du Code de la sécurité sociale, le médecin traitant, défini comme un médecin « favorisant la coordination des soins», « participe à la mise en place et à la gestion du dossier médical personnel».

Afin d'assister le patient dans la gestion de son DMP et l'exercice de ses droits, le patient aura la possibilité de recourir au médecin traitant qui disposera de droits supplémentaires au regard des autres médecins (inscription et désinscription d'un médecin sur la liste d'interdiction, accès aux données masquées et démasquage de celles-ci, consultation de l'historique de l'ensemble des accès).

La Commission comprend la nécessité de recourir à l'assistance du médecin traitant pour permettre à un patient de gérer son DMP et exercer ses droits à défaut d'accès direct par Internet.

Toutefois, elle estime qu'afin d'être mis en mesure d'exercer pleinement ses droits, le patient doit être clairement informé du rôle et des prérogatives de son médecin traitant dans le cadre du DMP et de la portée de la désignation d'un médecin traitant.

Sur les droits du patient sur le contenu du DMP

Le patient disposera, d'un droit d'opposition et de suppression (droit à l'oubli). Il aura la possibilité de demander que certains documents ne soient pas mentionnés dans le DMP. Il aura également la possibilité de demander la suppression d'un document ou de l'ensemble de son dossier en sollicitant l'intervention du médecin de l'hébergeur.

Le patient disposera également d'un « droit de masquage » qui lui permettra de rendre inaccessibles à certains professionnels de santé des données présentes dans son DMP. L'existence de documents masqués ne sera pas signalée.

Ce droit de masquage pourra être exercé par le patient lui-même si le dossier lui est accessible par internet ou par l'intermédiaire d'un médecin, après information par ce dernier sur les risques associés.

En cas de masquage d'un document, le document restera visible à son auteur, au patient, au médecin traitant de celui-ci et au médecin de l'hébergeur.
La Commission s'interroge sur le caractère étendu de cette exception au droit de masquage. Elle comprend la nécessité du recours à un ou plusieurs médecins traitants pour permettre à un patient de gérer son DMP et d'exercer ses droits à défaut d'accès direct par internet. Toutefois, elle estime, là encore, qu'il importe que le patient prenne clairement conscience des prérogatives de ce(s) médecins(s) dans le cadre du droit de masquage.

Le patient disposera également d'un espace d'expression personnelle.

La sécurité du dispositif

L'appréciation du niveau de sécurité proposé par l'hébergeur était l'un des points essentiels de l'avis que la Commission a rendu le 30 septembre 2010.

Sur les principes d'accès au DMP par les professionnels de santé

Les professionnels de santé accèderont au DMP à partir de leur logiciel « métier » ou par internet à partir d'un navigateur.

Ces logiciels devront faire l'objet d'une homologation par l'ASIP Santé. Dans la mesure où elle conditionne le bon fonctionnement d'un système d'information centralisé et alimenté à partir de systèmes techniquement hétérogènes et pour lesquels de nombreuses failles peuvent apparaître, la Commission prend acte des engagements de l'ASIP Santé en ce sens.

Les conditions d'accès des professionnels de santé seront déterminées en fonction de la profession de l'utilisateur et des types de documents accessibles. Une matrice permettant la gestion des habilitations pour la consultation du DMP a été créée à cet effet.

Seuls les professionnels de santé dotés d'une carte CPS délivrée par l'ASIP Santé, seront en mesure de consulter les documents présents dans le DMP d'un patient. Ces accès seront tracés nominativement grâce au certificat présent dans la carte.

La Commission en prend acte avec satisfaction et estime qu'une sensibilisation des professionnels de santé à une utilisation strictement personnelle de leur carte doit être effectuée.

Les professionnels de santé dotés d'une carte CPS ou authentifiés par le certificat de personne morale de leur établissement délivré par l'ASIP Santé seront en mesure de créer un DMP et de l'alimenter.

Enfin, les personnels d'accueil des établissements dotés de CPE nominatives ou indirectement nominatives auront la possibilité de créer un DMP.
La Commission prend acte du fait que l'utilisation d'un certificat de personne morale d'un établissement ouvre des droits restreints.

Elle relève, en outre, que lorsqu'un professionnel de santé ou un membre du personnel s'authentifie par le certificat de personne morale de l'établissement ou par CPE, le système d'information de la structure transmet les nom et prénom de l'utilisateur ainsi que l'identification de la structure. La transmission de ces données est de nature à permettre d'assurer la traçabilité des actions effectuées dans le dossier médical personnel.

La Commission en prend acte.

Les professionnels de santé pourront accéder au DMP d'une personne hors d'état de manifester sa volonté en mode « bris de glace » en présence d'une situation comportant un risque immédiat et à condition que le patient ne s'y soit pas préalablement opposé.

Cet accès devra être motivé et tracé pour s'assurer que la situation d'urgence justifiait bien cet accès.

Les médecins exerçant dans un centre d'appels d'urgence (15 ou 18) pourront également avoir accès au DMP des patients qu'ils prendront en charge, conformément aux dispositions de l'article L.1111-17 du Code de la santé publique. Dans la mesure où, répondant à un appel téléphonique, ils n'ont pas accès à la carte Vitale d'un patient, un service de « recherche d'un DMP en l'absence de l'INS » sur la base de traits d'identité a été mis en place.

Sur la traçabilité des accès et des actions

La Commission relève avec satisfaction qu'une traçabilité des actions des professionnels de santé sur les données sera effectuée, indiquant la date, l'identifiant du dossier patient, l'identifiant du processus ou de la personne à l'origine de l'événement.

Chaque professionnel de santé n'accèdera qu'à ses propres traces et aux traces liées aux DMP pour lesquels il est déclaré médecin traitant.
La Commission en prend acte.

Elle relève que les accès en mode « bris de glace » seront tracés dans l'historique des accès mais ne feront pas l'objet d'un signalement particulier.
La Commission estime que le patient et le médecin traitant devraient en être spécifiquement alertés de façon « proactive

».

De façon générale, la Commission relève que le médecin de l'hébergeur aura accès à l'ensemble des traces et de leur imputabilité, afin d'être mis en mesure de veiller au bon usage du DMP.

Dans la mesure où la traçabilité des actions n'est utile que si un contrôle effectif de celles-ci est effectué, la Commission estime qu'un dispositif d'alerte, à l'attention du médecin de l'hébergeur, devrait être mis en place afin de détecter les mésusages effectués sur les données de santé et, en particulier, les accès excessifs en mode « bris de glace ».

Sur le chiffrement des données

La Commission constate que, conformément à ce qu'elle préconise, les données de santé à caractère personnel seront conservées chiffrées dans les serveurs de l'hébergeur (chiffrement par AES-256). Elle relève que les clés de chiffrement sont différentes pour chaque dossier et elles-mêmes stockées chiffrées.

Elle relève également que le chiffrement mis en œuvre permettra une séparation logique des données d'identification et des données médicales.
Elle relève enfin que l'ensemble des flux sur les réseaux sera sécurisé.

La Commission juge ces mesures de chiffrement des bases de données et des échanges satisfaisantes.

La Commission prend acte enfin des engagements pris par l'ASIP Santé de rendre le DMP compatible avec le référentiel général de sécurité (RGS) prévu par l'article 5 de l'ordonnance n°2005-1516 du 8 décembre 2005.

Sur le système d'information de pilotage

Un Système d'information de pilotage (SIP) visant à évaluer l'usage et le service rendus par le DMP ainsi qu'à piloter le fonctionnement et la performance des systèmes sera mis en place. Le SIP intègrera des données fournies par le système d'hébergement DMP après anonymisation.

La Commission prend acte qu'aucune information envoyée au système de pilotage ne permettra l'identification directe ou indirecte d'un patient.

En revanche, elle observe, que les données concernant les professionnels de santé transmises au SIP seront directement nominatives afin de permettre d'effectuer des enquêtes qualitatives ciblées auprès d'eux.

La Commission demande que les professionnels de santé en soient préalablement et clairement informés.

Dans ces conditions, la Commission autorise l'ASIP Santé, à mettre en place les applications informatiques nécessaires à la généralisation du dossier médical personnel sur l'ensemble du territoire.

Le Président,
Alex TURK