Conclusions des missions de contrôles relatives à l'expérimentation du DMP

Le dossier médical personnel, le DMP, a été créé par la loi du 13 août 2004 relative à l'assurance maladie et a vocation à améliorer la qualité des soins en facilitant la coordination et les échanges d'information entre les professionnels de santé. A cette fin, il est prévu que chaque bénéficiaire de l'assurance maladie dispose d'un DMP, créé auprès d'un hébergeur de données de santé à caractère personnel agréé par le ministère de la santé, dans lequel seront stockées, en particulier, des données médicales le concernant et auxquelles pourront avoir accès certains professionnels de santé.

Le Groupement d'intérêt public du dossier médical personnel (GIP-DMP) a estimé nécessaire, avant la phase de généralisation du DMP, de procéder à **une préfiguration** afin, notamment, d'évaluer les options techniques, l'adéquation fonctionnelle et les hypothèses d'organisation et d'accompagnement des usages.

Six groupes de sociétés[1] ont été retenus, à l'issue d'un appel d'offres lancé en juillet 2005 par le GIP-DMP, pour expérimenter la mise en œuvre du DMP sur seize sites pilotes pour une période s'étalant, théoriquement, d'avril à décembre 2006.

La Commission s'est prononcée, conformément au code de la santé publique, le 21 mars 2006 **sur les dossiers de demande d'agrément** présentés par chacun des hébergeurs afin d'examiner « *les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données* ».

Dans ses avis, la CNIL a, d'une part, pris acte d'un **certain nombre d'engagements** formulés par les candidats à l'agrément, et d'autre part, formulé **un certain nombre de remarques tendant à améliorer la protection des données hébergées.** Elle a également autorisé la mise en place des traitements nécessaires à la conduite des expérimentations.

La Commission a estimé nécessaire de procéder, en application de l'article 44 de la loi du 6 janvier 1978 modifiée le 6 août 2004, à **des missions de vérification sur place auprès des principaux acteurs de l'expérimentation** : hébergeurs bien sûr, mais aussi centres hospitaliers, réseaux de santé, médecins libéraux et centres d'appel.

Ces contrôles ne visaient pas à avoir une vision exhaustive des pratiques des hébergeurs et des professionnels de santé dans le cadre de l'expérimentation du DMP, mais à apprécier la réalité des engagements pris par les hébergeurs et l'application des garanties demandées par la CNIL dans ses

[1] Il s'agit des consortiums D3P, France Télécom-CapGémini-SNR, de la société Invita, du consortium Santénergie, de GIE Santéos, et du consortium Thalès-Cégédim.

décisions de mars 2006.

Dans la mesure où la phase d'expérimentation du DMP a été très courte – quelques mois seulement – et les modalités d'ouverture du DMP assez longues, la CNIL n'a pas été en mesure d'apprécier au cours de ces contrôles le fonctionnement effectif et réel des DMP. En particulier, l'exercice de droits nouveaux, comme la possibilité de masquer certaines informations, ou l'accès en urgence au dossier médical n'a pu être apprécié.

L'ensemble des conclusions de la CNIL est présenté dans ce **document public**.

1. Les conditions d'ouverture du DMP

a) Les modalités d'ouverture du DMP et la définition du cercle de confiance

Il a été constaté que les modalités pratiques de création des DMP retenues pour l'expérimentation sont « chronophages ». En effet, le professionnel de santé propose l'ouverture d'un DMP et complète avec le patient, le formulaire destiné à l'hébergeur. Ainsi, certains établissements de soins ont dû affecter une ou deux personnes à cette tâche.

■ **L'ouverture d'un DMP** chez un hébergeur nécessite l'obtention d'un Numéro Identifiant Santé (NIS) et d'une Adresse Qualité Santé (AQS). Le délai de réception de ces codes par le patient s'échelonne de dix jours à quatre semaines. De nombreux hébergeurs ont souligné la lenteur et la complexité de cette procédure.

Ces envois sont effectués par courriers séparés en recommandé avec accusé de réception, par le GIP-DMP et l'hébergeur concerné.

Les pratiques constatées lors de certaines missions de contrôle consistant :

- pour certains hébergeurs, lors de l'ouverture d'un DMP, à transférer des AQS de patients aux établissements de soins par voie électronique sans protection particulière,
- pour certains centres d'appel, en cas de perte des identifiants permettant la consultation ou l'alimentation des DMP, à envoyer un mot de passe par courrier électronique non crypté au patient, ou à lui communiquer ce mot de passe par téléphone,

sont **de nature à compromettre la confidentialité de ces informations.**

Par ailleurs, lors de leur inscription, les patients remplissent des **« questions défi »**[2] qui permettront au centre d'appel de les authentifier. Il est à noter que ceux-ci ne comprennent pas toujours l'intérêt de ces questions et, en conséquence, ne renseignent pas correctement ces questions dans le formulaire d'adhésion.

Certains établissements de soins, où sont remplis les formulaires d'adhésion, ont pris l'initiative de conserver systématiquement une copie de ces formulaires, sur lesquels figurent notamment le « cercle

[2] Les « questions défis » ont pour fonction de s'assurer de l'identité de l'interlocuteur, et portent sur des points de la vie courante du patient (ex. : nom de jeune fille de sa mère, couleur de sa première voiture).

de confiance » (cf. infra) et les questions défi renseignées par le patient. Or, seuls le patient et l'hébergeur sont habilités à conserver ce formulaire[3].

■ **La définition du « cercle de confiance »** revient au patient, qui doit désigner nominativement les professionnels de santé qui pourront consulter et alimenter son DMP et déterminer les droits qui leur sont reconnus.

Certains hébergeurs prévoient la possibilité pour un professionnel de santé, avec l'autorisation du patient, de gérer le « cercle de confiance » de ce dernier. D'autres, en raison de la difficulté de désigner nominativement des professionnels de santé exerçant dans un établissement de soins, incitent les patients à étendre de manière importante leur « cercle de confiance », notamment en fournissant dans le dossier d'inscription au DMP une liste d'établissements, de cabinets médicaux, de laboratoires et de praticiens que les patients peuvent inclure dans leur cercle, sans qu'ils soient toujours à même de savoir s'ils doivent les accepter ou les refuser

b) L'information des patients

L'information délivrée au patient sur ses droits (droits d'accès et de rectification, droit de masquage, droit de définition du « cercle de confiance ») doit être claire et complète quant aux finalités et fonctionnalités du DMP. Or, le choix opéré par les hébergeurs et les établissements de soins de faire compléter les formulaires d'adhésion, non par le patient lui-même, mais par un tiers – un professionnel de santé ou une personne *ad hoc* appartenant à leurs propres personnels – afin notamment de faciliter les inscriptions, a pu conduire à délivrer aux patients concernés une information de faible qualité.

Ainsi, les patients n'ont pas tous été parfaitement informés que l'accès aux données médicales contenues dans leur DMP nécessitait une connexion internet. De plus, il leur a été parfois indiqué que l'accès à ces données était possible par l'intermédiaire du centre d'appel de l'hébergeur, alors que ce dernier n'a pour fonction que d'assister techniquement les patients ou leur permettre de modifier les données administratives les concernant, leur mot de passe ou la composition de leur cercle de confiance.

[3] Le consentement du patient, nécessaire à l'ouverture du dossier médical personnel, s'est matérialisé par la signature du contrat passé avec l'hébergeur comme l'exigent les dispositions de l'article R. 1111-13 du Code de la santé publique issu du décret n°2006-6 du 4 janvier 2006. Le formulaire d'adhésion, qui contient la liste des autorisations d'accès accordées à certains professionnels de santé par le patient et les questions défis destinées à permettre d'identifier un patient qui prend contact avec le centre d'appel pour modifier les habilitations et exercer son droit de masquage, est uniquement accessible par les parties au contrat, c'est-à-dire l'hébergeur et le patient. On comprend dès lors la confidentialité qui s'attache à ce document contractuel, toute personne tiers au contrat ayant accès à ces données pouvant exercer ces prérogatives aux lieu et place du patient.

2) Le fonctionnement du DMP

a) Les modalités d'accès

L'accès à un DMP est offert au patient lui-même et aux professionnels de santé qui sont inclus dans son cercle de confiance.

■ Il est prévu que **le patient** pourra accéder à son DMP par un accès direct sur Internet, sécurisé, en utilisant son AQS, un identifiant et son mot de passe. Toutefois, les missions de contrôles effectuées par la CNIL n'ont pas permis de vérifier l'effectivité de cette fonctionnalité.

De même, il est prévu, dans la majorité des cas, que le patient, et lui seul, peut consulter un journal d'événements récapitulant les accès à son dossier médical personnel, qui précise la date, l'heure, le type de documents auquel une personne aura accéder, en lecture ou en écriture.

Les missions de contrôle révèlent **l'insuffisance des mesures d'identification-authentification mises en œuvre dans les centres d'appel.** Ainsi, l'authentification des patients ne s'opère pas systématiquement par une interrogation à partir des questions défis, et l'identification des professionnels de santé peut parfois être opérée uniquement à partir de leur numéro ADELI (numéro d'inscription au répertoire national des professionnels de santé délivré par la DDASS).

■ **Les conditions d'accès et d'alimentation d'un DMP par les professionnels de santé** qui peuvent légitimement y prétendre – soit parce qu'ils sont inclus dans le « cercle de confiance » du patient concerné, soit parce qu'ils agissent en cas d'urgence – doivent respecter des impératifs précis de sécurité.

La procédure normale d'authentification des professionnels de santé pour toute action relative au DMP doit reposer, selon les recommandations de la CNIL, sur l'usage de **la carte de professionnel de santé (CPS)**.

Or, les missions de contrôle ont permis de constater que l'alimentation des DMP au sein de la majorité des établissements de soins s'effectuait par l'intermédiaire, soit du logiciel métier utilisé par l'établissement, soit de « dossiers patient partagés ». En tout état de cause, ces procédures, qui ne requièrent pas l'utilisation de la CPS, **ne permettent pas d'authentifier le professionnel de santé** à l'origine de cette alimentation, mais authentifient uniquement l'échange entre l'hébergeur et l'établissement de soins.

Au surplus, certains hébergeurs, prenant acte du fait que certains établissements de soins n'ont pas équipé leurs professionnels de santé de CPS, organisent l'accès aux DMP depuis leur site internet sur la base d'un simple identifiant et d'un mot de passe. **Cette solution ne saurait être acceptée et est manifestement contraire aux décisions de la CNIL du 21 mars et du 30 mai 2006.**

L'alimentation des DMP par les médecins libéraux soulève la question de la compatibilité des logiciels métiers avec le DMP afin d'éviter la « double saisie », qui risquerait de rendre inopérante la mise en œuvre du DMP.
Sur ce point, certains hébergeurs ont développé des interfaces entre les logiciels métiers utilisés par les médecins libéraux et les DMP qu'ils hébergent.

Ainsi, un hébergeur propose aux médecins libéraux **une fonction d'importation des documents** de santé du DMP dans leur propre logiciel métier. Cette fonctionnalité n'est pourtant pas précisée dans le contrat signé par le patient lors de l'ouverture d'un DMP.

Par ailleurs, cette importation n'est pas tracée dans les journaux d'événements du DMP. Le patient n'en est donc pas informé. Enfin, les documents importés dans le logiciel métier du médecin y demeurent, même si, par la suite, ce médecin est exclu du cercle de confiance du patient. Dans cette hypothèse, le patient conserve les droits qui lui sont reconnus aux termes de l'article 38 de la loi du 6 janvier 1978 modifiée.

Le médecin hébergeur rattaché auprès de chaque hébergeur peut avoir accès, dans le cadre de l'expérimentation, au DMP de certains patients.

Il a notamment pour mission :

- de gérer les cas de collision ou de doublon dans un même dossier médical personnel. Dans ce cas, il peut, selon les hébergeurs, invalider le document sans le supprimer ou, après contact avec le professionnel de santé à l'origine de l'erreur, lui demander de rectifier les données erronées ou recueillir son autorisation pour effectuer la rectification à sa place ;
- de suivre les accès effectués en mode « bris de glace », qui permet à un professionnel de santé, non habilité par un patient, de consulter le DMP de ce dernier.

Les missions de contrôle ont établi que **le rôle du médecin hébergeur et son périmètre d'intervention n'étaient manifestement pas clairement définis**, certains d'entre eux ne possédant pas de CPS.

Enfin, les missions de contrôle ont permis de vérifier que les personnels administratifs et techniques, tant de l'hébergeur que des centres d'appel, n'ont pas accès aux données de santé contenues dans les DMP.

■ **Le droit de masquage** dont bénéficie le patient lui permet de rendre inaccessibles à certains professionnels de santé des données présentes dans son DMP, à l'exclusion de l'auteur du ou des documents concernés. Lors de l'expérimentation, peu de patients ont utilisé cette faculté.

Selon le dispositif mis en place par l'hébergeur concerné, le professionnel de santé aura ou non la possibilité de savoir à quel type de document (compte-rendu d'opération, analyses médicales, images radio, etc.) appartiennent les données masquées.

La Commission a relevé que certains hébergeurs avaient mis en place une délégation de masquage au bénéfice du médecin traitant après une activation auprès du centre d'appel.

■ L'accès en **mode « bris de glace »** ne peut s'effectuer que dans le cadre d'une urgence, le professionnel de santé devant alors s'en justifier.

Chaque accès en mode « bris de glace » conduit **le patient concerné à en être systématiquement informé** par une alerte affichée lors de la prochaine ouverture de son DMP, voire par l'envoi d'un courrier en accusé réception expédié par le médecin hébergeur.

Plusieurs situations contradictoires avec la finalité même du mode d'accès « bris de glace » ont été relevées :

- l'obligation de renseigner l'identifiant du patient – son AQS – alors que ce dernier n'est pas toujours en mesure de le communiquer ;
- l'accès du professionnel de santé à l'intégralité du contenu du DMP, y compris l'espace personnel du patient et les documents masqués ;
- l'absence systématique d'un journal des accès en mode « bris de glace » au bénéfice du médecin hébergeur.

b) La sécurité des traitements

L'appréciation des dispositifs de sécurité proposés par chaque hébergeur était l'un des points essentiels des avis que la Commission a rendus le 21 mars 2006.

■ A ce titre, la Commission avait recommandé **un chiffrement complet** des bases de données mises en œuvre, et non pas uniquement le chiffrement des canaux de communication.

Sur ce point, les missions de contrôle attestent que cette préconisation n'était pas systématiquement mise en œuvre. En effet, la plupart des hébergeurs cryptent uniquement les documents de santé dans leur base de données[4].

En outre, l'expérimentation a permis de relever une importante faille de sécurité sur le site internet d'un hébergeur, où l'accès au DMP par les patients reposait sur des identifiants et mots de passe identiques et facilement déductibles. Bien que résolue dans de brefs délais, cette faille a démontré l'intérêt qui s'attache à la définition d'**un mot de passe « robuste »**, c'est-à-dire composé d'au moins huit caractères alphanumériques. L'obligation, imposée par certains hébergeurs, de modifier le mot de passe lors de la première connexion est de nature à améliorer le niveau de sécurité concernant l'accès au DMP des patients.

Afin de renforcer la sécurité de leur portail DMP en ligne, certains hébergeurs ont mis en place un système de fermeture automatique de la session qui s'exécute au-delà de dix minutes d'inactivité. Cette garantie doit être généralisée.

Certains hébergeurs proposent l'utilisation **du certificat logiciel**, téléchargé par le patient, qui est stocké sur son ordinateur et garantit qu'aucune connexion au DMP ne pourra se faire depuis un autre poste. Cette solution est de nature à sécuriser l'accès des patients à leur DMP.

D'autres hébergeurs fournissent au patient une crypto-clé (USB), contenant un certificat électronique et son AQS, associée à un mot de passe, qui lui permet de se connecter à son DMP avec une authentification plus forte. Toutefois, cette solution contraint les personnes à disposer de systèmes d'exploitation et d'équipements informatiques récents (dotés de port USB) pour accéder au DMP.

■ Les données traitées par les hébergeurs sont **sauvegardées**, sous forme cryptée, de façon automatisée quotidiennement, hebdomadairement, et mensuellement. Pour autant, les services informatiques gérant eux-mêmes leurs sauvegardes ne stockent pas toujours les supports de sauvegarde sur un site distant, au risque de perdre la totalité des données en cas de sinistre majeur. Il

[4] La solution la plus sécurisée consisterait à chiffrer à la fois chaque dossier en base de données (en utilisant des clés de chiffrement uniques et distinctes), les échanges de données (document « poussés » dans la base), ainsi que les liens (adresses) reliant les documents de santé aux données administratives du patient

est à noter que plusieurs hébergeurs externalisent leur activité de stockage et de sauvegarde à des sous-traitants spécialisés.

■ L'ensemble des hébergeurs possèdent une expérience en matière de **sécurité physique** des locaux et des matériels informatiques. Leurs infrastructures sont généralement équipées de systèmes de détection d'intrusion (alarmes volumétriques, vidéo-surveillance), de matériels de servitude (inondation, climatisation, fourniture ininterrompue d'énergie électrique), etc. L'accès aux « salles blanches » (c'est-à-dire les salles des serveurs informatiques) est généralement sécurisé de manière satisfaisante, même si certaines missions de contrôle ont mis en lumière des insuffisances, notamment en ce qui concerne l'identification des personnels intervenant à des fins de maintenance occasionnelle.

Au total, les missions de contrôle ont permis de mettre en évidence que **certains hébergeurs attendent la phase de généralisation pour mettre en place la totalité de leur architecture matérielle et système, telle qu'elle a été définie dans le cahier des charges**. Ainsi, plusieurs hébergeurs n'ont pas mis en place, dans le cadre de l'expérimentation, de dispositif de réplication des données sur un site distant - pourtant prévu dans le cahier des charges du GIP-DMP –, ce qui peut engendrer, en cas de sinistre majeur, une perte de données substantielle.

Conclusions

Quelles sont les exigences de la CNIL pour les nouvelles demandes d'autorisation qui lui seront soumises ?

Les constatations effectuées lors des contrôles conduisent la CNIL à **rappeler au Ministère de la santé, au GIP-DMP, aux hébergeurs et aux établissements de soins les points suivants qui constituent à ses yeux des conditions indispensables au déploiement sécurisé du dossier médical personnel :**

- La nécessité d'une **authentification forte** de toute personne ayant accès au DMP, qu'elle soit professionnel de santé ou patient. L'utilisation de la carte de professionnel de santé ou d'un certificat logiciel équivalent pour les premiers et le recours à un système de certificat logiciel individuel ou à tout autre procédure offrant un même niveau de garantie pour les seconds sont indispensables et doivent être accompagnés de la mise en place des moyens nécessaires.

- La nécessité du recours à un **chiffrement complet** des données contenues dans le DMP. A cet égard, le chiffrement doit porter non seulement sur les données médicales mais aussi sur les données administratives dès lors qu'un lien technique existe entre les deux. La sécurisation de toute connexion à distance doit également être rendue effective.

- La nécessité d'i**nformer clairement et complètement les patients** sur le fonctionnement du DMP et sur les modalités d'exercice de leurs droits, en particulier le droit de masquage. Alors que se développent plusieurs projets de dossiers de santé sur internet qui, pour certains, sont appelés à enrichir le dossier médical personnel (dossier pharmaceutique, dossier de cancérologie, dossiers de réseaux de soins), il est important que l'information destinée au patient soit suffisamment claire et explicite pour lui permettre de participer activement à ces dispositifs et d'exercer pleinement ses droits.

Un état de la situation individuelle des hébergeurs est transmis au ministère de la santé et au GIP-DMP.