Les questions autour du dossier médical personnel

Plusieurs questions se posent autour du DMP : la protection des données personnelles, le droit au masquage des informations et la sécurité du système. Pour les médecins, des retombées sur leur responsabilité sont à envisager. Enfin, l'évaluation des dossiers médicaux électroniques est difficile car les systèmes sont complexes. L'efficacité et les résultats économiques dépendent du contexte, d'un pilotage et d'une mise en œuvre bien menés.

Accès aux informations de santé et DMP

Jeanne Bossi
Chef de la Division des affaires publiques et sociales, Cnil

Le législateur a créé en 2004 un nouveau dossier médical partagé, le dossier médical personnel. Inscrit à l'article L. 161-36-1 du Code de la Sécurité sociale, il est mis en place dans un souci affirmé de meilleure coordination des soins et d'amélioration de la qualité et de la continuité des soins. Chaque bénéficiaire de l'assurance maladie devra disposer de son propre dossier médical (DMP), hébergé par un organisme agréé présentant les conditions nécessaires pour garantir la confidentialité des données. Le DMP sera constitué notamment des informations qui permettent le suivi des actes et prestations de soins.

Ces premières caractéristiques ne le distinguent pas *a priori* des autres dispositifs déjà mis en place, par exemple dans le cadre des réseaux de soins. C'est un dossier médical partagé institué pour une meilleure prise en charge médicale de la personne.

Il sera accessible directement au patient, conformément aux dispositions de l'article L. 1111-7 du Code de la santé publique et selon les modalités de l'article 40 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Mais, alors que jusqu'à présent le droit d'accès aux données de santé s'exerçait à l'égard de données par ailleurs détenues par les seuls professionnels de santé dans le cadre de l'exercice de leurs fonctions, le dossier médical personnel se présente aujourd'hui comme celui du patient, accessible aux seuls professionnels de santé autorisés par le patient à y accéder et à y inscrire certaines données.

La reconnaissance par la loi de modalités particulières d'exercice du droit d'accès, comme le droit de masquage de certaines données, la possibilité de désigner de façon nominative chacun des professionnels de santé à qui le patient souhaite ouvrir des droits en lecture ou en écriture, la possible mise en place de dispositifs techniques permettant au patient d'accéder lui-même directement de son poste informatique à son dossier médical illustre la singularité du DMP par rapport à d'autres projets de dossiers médicaux partagés.

Certes, le rappel de ces premiers éléments reste aujourd'hui encore très théorique, les récentes expérimentations du DMP n'ayant pas permis — loin s'en faut — de mesurer les conséquences de leur application. Mais la prochaine généralisation du DMP dans un contexte qui s'accompagnera nécessairement de changements importants des mentalités et d'exigences en matière de sécurité permettra certainement de le mesurer.

Il appartient dès lors à la Commission nationale de l'informatique et des libertés, autorité chargée de veiller

au respect de la protection des données personnelles, de s'assurer des conditions de sécurité dans lesquelles le DMP sera mis en place — un contexte de sécurité garantie étant seul de nature à permettre un exercice effectif des droits des patients prévus par la loi.

La maîtrise du DMP par le patient

La volonté du législateur de créer un nouveau dossier médical personnel doté de caractéristiques qui lui sont propres, associée à celle exprimée dans la loi du 4 mars 2002 sur les droits du malade de consacrer le droit d'accès direct aux données médicales, assure ainsi en principe la maîtrise par le patient du contenu et des accès à son dossier médical personnel.

Le contrôle du contenu et le choix des accès

L'ouverture du DMP s'effectuera par voie électronique. Les bénéficiaires de l'assurance maladie pourront ouvrir leur DMP auprès de l'administrateur d'un portail géré par la Caisse des dépôts et consignations, qui leur présentera une liste des hébergeurs de données de santé agréés parmi lesquels les intéressés choisiront l'hébergeur avec lequel ils concluront un contrat[1].

Le dossier médical personnel sera composé de données relatives à l'identification du titulaire du DMP, de données concourant à la coordination, la qualité et la continuité des soins et de la prévention — les données, définies au regard de ce critère de pertinence, sont regroupées en quatre volets (les données médicales générales, les données de soins, les données de prévention et les images radiographiques ou autres imageries médicales) —, ainsi que d'un espace personnel d'expression du titulaire dans lequel il pourra faire figurer les informations qu'il estime utile de porter à la connaissance des professionnels de santé[2].

Tel est aujourd'hui défini le contenu du dossier médical personnel dont la généralisation est prévue en 2007.

Le titulaire accédera en consultation à toutes les informations de son DMP conformément aux dispositions de l'article L. 1111-7 du Code de la santé publique. Il aura également accès aux traces relatives aux actions effectuées sur son DMP, qui lui indiqueront l'identité des personnes ayant accédé au DMP, l'heure, la date de leurs interventions, les documents consultés, modifiés (le texte vise les documents « *reportés* ») ou supprimés.

La seule partie où le titulaire pourra inscrire des informations est son espace personnel d'expression.

Il reviendra au patient de désigner nominativement les professionnels de santé qui pourront consulter et alimenter son DMP, et de déterminer les droits qui leur sont reconnus. Chaque professionnel de santé autorisé par le patient à accéder au dossier médical y reportera les éléments concourant à la coordination des soins et s'inscrivant dans les formats ainsi définis[3].

Le projet de décret prévoit également que, pour créer son DMP, y accéder et le gérer, le titulaire du DMP utilisera la carte Vitale 2 ou un dispositif d'identification et d'authentification offrant des garanties de sécurité équivalentes, agréé par les ministres chargés de la Santé et de la Sécurité sociale. Il conviendra sur ce point que l'agrément soit également délivré après avis de la Cnil. Il devra en tout état de cause être conforme au référentiel national de sécurité prévu par l'ordonnance du 8 décembre 2005 sur l'administration électronique et agréé par les ministres chargés de la Santé et de la Sécurité sociale.

Le droit de masquage

Le droit reconnu au titulaire du DMP de masquer des informations de son DMP, prévu dans le cadre des expérimentations du DMP et par les dispositions de l'avant-projet de décret sur le DMP, peut apparaître comme une application du droit reconnu par l'article 40 de la loi informatique et libertés à toute personne physique dont des données à caractère personnel font l'objet d'un traitement de les rectifier, les compléter ou les supprimer lorsqu'elles s'avèrent inexactes, incomplètes, équivoques ou périmées.

De façon générale, la Cnil a considéré, jusqu'à présent, que la requête d'un patient qui demanderait à son médecin l'effacement de données qui ne seraient ni inexactes, ni incomplètes, ni équivoques ou périmées, ne peut être satisfaite, sauf si le patient invoque des motifs légitimes. En effet, conformément aux dispositions de l'article 38 de la loi du 6 janvier 1978 modifiée, « *toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que les données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Si l'exercice du droit d'opposition reconnu par l'article 38 de la loi du 6 janvier 1978 doit être apprécié au regard du caractère obligatoire de la tenue du dossier médical personnel, que le législateur a souhaité inscrire dans la loi en conditionnant le niveau de remboursement des soins à son ouverture, la reconnaissance d'un droit de masquage des informations du DMP peut être de nature à équilibrer la relation entre le patient et le professionnel de santé.

L'exercice du droit de masquage permettra également de traduire une certaine réalité de la relation médecin-patient dans laquelle le patient ne se dévoile pas immédiatement. L'argument selon lequel la reconnaissance d'un droit de masquage serait de nature à

1. Afin d'éviter que l'ouverture du DMP se fasse au détriment des personnes non équipées en informatique, le projet de décret donne également la possibilité d'ouvrir un DMP auprès de guichets de services publics qui auront reçu une habilitation à cet effet.

2. On y trouvera également la mention indiquant qu'il a pris connaissance des dispositions de la réglementation sur les dons d'organes, les coordonnées des personnes à prévenir en cas de nécessité si le titulaire a consenti à cette mention et les « directives anticipées » qu'une personne peut rédiger pour le cas où elle serait un jour hors d'état d'exprimer sa volonté quant à la limitation ou à l'arrêt des traitements médicaux en fin de vie.

3. Le titulaire gérera les droits d'accès des professionnels de santé, prérogative qu'il peut, de même que l'ouverture du DMP, confier à un mandataire. Les conditions de ce mandat seront précisées et le mandataire n'aura pas accès au contenu du DMP du mandant.

nuire à l'efficacité des soins apparaît alors sans objet, dans la mesure où la relation médecin-patient s'est toujours accompagnée de « non-dits » et qu'une information « cachée » à un moment donnée pourra être révélée à un autre moment de la relation ou par l'intermédiaire de la nature des soins prodigués.

Dans la mesure également où la liberté de la personne quant à l'ouverture de son DMP est relative (puisqu'un lien sera établi avec le niveau de remboursement de soins), le droit de masquage apparaît comme une garantie pour le patient. Il sera aussi de nature à rassurer le patient et à contrebalancer les inquiétudes manifestées quant à la confidentialité du dispositif. Il constitue, à cet égard, une condition de l'acceptabilité du DMP par les patients. Toutefois, le masquage organisé pour l'heure est un masquage générique et non par spécialité médicale ou *intuitu personae*.

Mais l'exercice du droit de masquage doit nécessairement s'accompagner d'une information complète et claire du patient sur les conséquences du masquage. D'une part à l'égard de son professionnel de santé, d'autre part à l'égard de son niveau de remboursement.

Dans la mesure également où le DMP pourra être accessible directement par le patient en dehors de toute relation médicale, le droit de masquage apparaît également comme une garantie de confidentialité à l'égard des tiers. Le patient choisira les données qu'il souhaite communiquer.

Le « masquage du masquage »

Le masquage du masquage, c'est la traduction du « droit à l'oubli », c'est-à-dire la possibilité de ne pas conserver des données au-delà de la durée nécessaire ou de souhaiter que ces données soient définitivement supprimées. (Par exemple, une interruption volontaire de grossesse ou une consultation chez un infectiologue.)

Le masquage peut également apparaître dans certains cas comme la conséquence logique du droit de masquage. En effet, lorsque le niveau de classement de l'information est si fin que signaler le masquage revient à faire connaître l'information (par exemple, signaler qu'une information est masquée dans un dossier de sérologie revient à délivrer l'information), il constitue une garantie supplémentaire pour le patient. Dès lors, plus l'architecture du DMP sera précise, plus transparente sera l'information masquée.

Il est vrai que la reconnaissance du droit de masquer les informations elles-mêmes masquées pourra être de nature, au moins dans les premiers temps, à faire douter de l'efficacité du dispositif pour la coordination des soins.

La sécurité du DMP, condition de l'exercice des droits du patient

L'identification du patient : la position de la Cnil

La loi du 13 août 2004 prévoyait dans son article 5 qu'« *un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et pour la tenue du dossier médical personnel tel que défini à l'article L. 161-36-1 du Code de la Sécurité sociale, dans l'intérêt de la personne concernée et à des fins exclusives de coordination des soins* ».

Le nouvel article L. 1111-8-1 du Code de la santé publique, issu de la loi du 30 janvier 2007 sur les professions de santé, prévoit la création d'un identifiant de santé des personnes prises en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé, notamment pour l'ouverture et la tenue du DMP. Un décret pris après avis de la Cnil doit déterminer cet identifiant ainsi que ses modalités d'utilisation.

La Commission nationale de l'informatique et des libertés, interrogée par le ministère de la Santé sur l'utilisation du numéro de Sécurité sociale comme identifiant du dossier médical personnel, a récemment précisé sa position[4].

La question posée à la Cnil est importante à plusieurs égards. En premier lieu, parce que le numéro de Sécurité sociale a toujours occupé dans la loi du 6 janvier 1978, y compris depuis sa modification en 2004, une place symbolique particulière. Ensuite parce que, sur ce fondement, la commission a construit tout au long des années une doctrine particulière cherchant à limiter l'usage de cet identifiant unique à la sphère sociale et n'acceptant qu'à titre exceptionnel qu'il soit utilisé dans d'autres secteurs dans sa fonction de certification de l'identité. Enfin, parce que la position que prend la Cnil, quelle qu'elle soit, comporte des conséquences importantes pour le fonctionnement et l'architecture des systèmes d'information de santé.

Le NIR, numéro d'inscription au Répertoire national d'identification des personnes physiques (RNIPP), communément appelé numéro de Sécurité sociale, est un numéro particulier car il est signifiant, unique et pérenne et *a priori* fiable puisqu'il est certifié par l'Insee à partir des données d'état civil transmises par les mairies.

La commission n'ignore pas que des informations relatives à la santé (informations nécessaires à la prise en charge des assurés et à une meilleure connaissance des dépenses de santé) figurent dans les fichiers de l'assurance maladie et, chez les professionnels et établissements de santé, dans les fichiers de gestion administrative des patients identifiés alors par leur numéro de sécurité sociale[5].

Le recours à l'identifiant fiable (car associé à des

4. Conclusions du groupe de travail sur l'identifiant de santé du 20 février 2007.

5. Ces données permettent de connaître, pour chaque bénéficiaire de l'assurance maladie, les consultations et les actes médicaux effectués, ainsi que les médicaments prescrits. Cette évolution, initiée en son temps par l'instauration du codage des actes, des prescriptions et des pathologies, s'accentue encore avec la mise en place de la nouvelle tarification des actes médicaux, qui associe à une catégorie tarifaire un acte codé selon une classification détaillée des actes médicaux, et par la création par le législateur du « webmédecin » permettant d'établir un lien automatique entre les données de remboursement et certaines données de santé.

éléments d'état civil certifiés) et disponible qu'est le NIR peut apparaître comme la solution permettant de résoudre les problèmes qui résulteraient de la création d'un identifiant spécifique pour une population de plus de 60 millions de personnes.

Toutefois, partant de la constatation que les données de santé ne sont pas des données personnelles comme les autres et qu'elles appellent une protection renforcée, la Cnil estime que le NIR, compte tenu de son usage répandu, du fait qu'il est signifiant et facile à reconstituer et des risques précédemment évoqués, ne constitue pas, aujourd'hui, un numéro adapté pour identifier le dossier médical de chacun.

En effet, le recours à un tel identifiant devrait bénéficier de mesures de protection toutes particulières qui, aux dires mêmes des professionnels concernés, ne sont actuellement assurées ni dans les établissements de santé, ni chez les professionnels de santé, ni dans les réseaux de soins.

La commission estime donc que la méthode la plus à même d'apporter les garanties souhaitables serait la création d'un identifiant de santé spécifique, généré à partir du NIR, certifié selon les procédures déjà éprouvées actuellement utilisées pour les bénéficiaires de l'assurance maladie, mais transcodé selon des techniques reconnues d'anonymisation. Ce numéro, non signifiant, constituerait l'identifiant de santé utilisable dans l'ensemble du système de soins[6].

L'authentification du patient et du professionnel de santé et la question plus générale de la sécurité

La Cnil a autorisé, le 30 mai 2006[7], les applications informatiques mises en œuvre au sein des établissements de soins et par les professionnels de santé participant à l'expérimentation du dossier médical personnel dans treize régions et dix-sept sites pilotes retenus par le groupement d'intérêt public du dossier médical personnel.

Les constatations effectuées lors des contrôles conduisent la Cnil à rappeler aujourd'hui 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 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. À 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.

Les conditions de l'authentification du patient à son dossier médical personnel sont actuellement en cours de définition et feront l'objet, de la part de la Cnil, d'une expertise particulière.

L'information claire et préalable sur les utilisations du DMP

Conformément aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'information délivrée au patient sur ses droits doit être claire et complète quant aux finalités et fonctionnalités du DMP.

Dans le cadre des expérimentations réalisées, la Cnil a pu constater que 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 de leur permettre de modifier les données administratives les concernant, leur mot de passe ou la composition de leur cercle de confiance.

Enfin, si la difficulté de désigner nominativement des professionnels de santé exerçant dans un établissement de soins peut conduire une personne à inclure dans son cercle de confiance la notion d'« équipe de soins », cela ne doit pas la conduire à autoriser l'ensemble du personnel d'un établissement de santé à accéder à son DMP, comme cela a pu être relevé lors de certaines missions de contrôle.

Alors que se développent plusieurs projets de dossiers de santé sur Internet qui, pour certains, sont appelés à enrichir le dossier médical personnel et qui obéissent à des régimes juridiques distincts (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.

6. Le choix de l'identifiant de santé, quel qu'il soit, ne permettra toutefois pas de faire l'économie des procédures de vérification de l'identité du patient et de normalisation qui sont nécessaires en particulier dans les établissements de soins, tant lors de l'admission que tout au long du parcours de soins, afin d'éviter tout risque de confusion dont les conséquences pourraient être particulièrement graves pour les personnes. Il est indispensable de mettre en place, dans l'ensemble des structures de soins, des procédures spécifiques d'« identité-vigilance » permettant de s'assurer que le dossier médical se rapporte bien à la personne concernée, en particulier au vu des autres éléments d'identité produits par la personne et des actes médicaux réalisés.

7. Délibération n° 2006-151du 30 mai 2006.