



Groupement d'intérêt public- Dossier médical personnel

Le DMP : un dossier très sécurisé

Le dossier médical personnel s'inscrit dans un cadre juridique rigoureux qui exige notamment le strict respect de la confidentialité des données de santé. Elle est garantie, à toutes les étapes de la vie du DMP, par des procédures hautement sécurisées.

Le DMP appartient au patient. Le professionnel de santé ne pourra y accéder qu'avec son autorisation. Les professionnels de santé sont les seuls à pouvoir entrer des données médicales dans son dossier. C'est le patient qui crée son DMP et qui en gère les accès via le portail Internet DMP. Il peut, après discussion avec le professionnel de santé, masquer certaines données.

La création du DMP

Le patient procède tout d'abord à l'ouverture de son dossier, puis active son compte Internet s'il souhaite consulter son DMP depuis Internet par la suite. Ces deux étapes se déroulent sur un espace sécurisé du portail DMP. Elles bénéficient toutes deux d'un double rempart :

- l'identification du patient repose sur son identifiant national de santé. Personnel, celui-ci garantit la sécurité médicale : pas de confusion possible entre deux patients. Suite à la décision rendue par la Cnil le 20 février dernier, cet identifiant national de santé ne pourra pas être le NIR (numéro de Sécurité sociale), mais sera un nouveau numéro, anonyme, construit à partir du NIR (cf. ci-après).
- l'authentification se fait grâce aux codes reçus par courrier de son organisme d'assurance maladie. Le premier de ces codes servira pour l'ouverture du DMP, le second pour l'activation de l'accès Internet.

Un identifiant santé spécifique

La Cnil a rendu le 20 février dernier son avis sur l'identifiant national de santé. Elle a indiqué clairement qu'elle n'était pas favorable à ce que le numéro de Sécurité sociale (NIR) soit utilisé comme identifiant direct des dossiers médicaux, et notamment du dossier médical personnel (DMP). Elle estime en revanche qu'il convient de bénéficier des qualités d'unicité et de fiabilité du NIR. Elle recommande donc que le nouvel identifiant national de santé, créé par la loi du 30 janvier 2007, soit généré à partir du NIR certifié. La carte Vitale 2, en cours de déploiement, inclura ce nouvel identifiant de santé.

Les accès au DMP

Pour accéder à son dossier depuis un compte Internet, le patient s'identifie via son identifiant national de santé.

Puis il s'authentifie grâce à un code secret choisi par lui à l'ouverture de son compte et un mot de passe à

usage unique, valable seulement quelques minutes et généré par le portail. Le patient peut le recevoir sur son téléphone portable ou sur son courriel. Le niveau de sécurité est au moins équivalent à celui des services bancaires en ligne.

Le professionnel de santé se connectera au portail Internet DMP via son logiciel professionnel de santé « DMP compatible ». Il saisira l'identifiant national de santé de son patient, puis s'identifiera avec sa carte de professionnel de santé (CPS). Si le professionnel de santé travaille en établissement, l'identification se fera directement via le système informatique de l'établissement grâce au certificat CDE.

Si le patient a donné les droits d'accès à la création de son DMP, après vérification des autorisations d'accès, il pourra ouvrir le DMP et, éventuellement, l'alimenter, en accord avec son patient. Si le patient n'a pas donné les droits d'accès au professionnel de santé, il peut donner son autorisation au professionnel de santé au cours de la consultation. Le professionnel de santé peut alors accéder au DMP.

Il est à noter que chaque consultation ou dépôt d'informations sur le dossier laisse une trace informatique, visible par le patient.

Les échanges et le stockage des données

Les informations envoyées pour enrichir le DMP sont chiffrées lors de leur transfert sur Internet. Il s'agit d'une solution de chiffrement standard de l'Internet, utilisée entre autres par toutes les banques, le protocole SSL. Cela garantit l'intégrité des données conservées dans le DMP et la confidentialité des données du DMP lorsque celles-ci transitent sur Internet. L'hébergeur qui stocke les DMP a reçu pour cela un agrément de l'État, attestant qu'il est conforme à des référentiels publics, notamment en matière de sécurité (protection contre les accès illégitimes). Il n'a pas accès au contenu des dossiers.

Sécurité des données : quelles bonnes pratiques ?

La sécurité de l'hébergement des données et celle du portail sont sous la responsabilité et le contrôle du groupement d'intérêt public chargé du DMP. Deux éléments de la chaîne de confidentialité se situent en dehors de son périmètre : l'ordinateur du patient et celui du professionnel de santé. Les pouvoirs publics engageront des opérations de sensibilisation et de formation aux bonnes pratiques vers les professionnels de santé dans les mois à venir. 