ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 19608	De **Mme Nadia Ramassamy** (Les Républicains - Réunion)	**Question écrite**

Ministère interrogé > Solidarités et santé	**Ministère attribuataire** > Solidarités et santé

Rubrique >santé	**Tête d'analyse** >Protection des données de santé du dossier médical partagé	**Analyse** > Protection des données de santé du dossier médical partagé.

Question publiée au JO le : **14/05/2019**
Réponse publiée au JO le : **06/08/2019** page : **7401**

Texte de la question

Mme Nadia Ramassamy interroge Mme la ministre des solidarités et de la santé sur la protection des données contenues dans le dossier médical partagé. Prévu par le projet de loi relatif à l'organisation et à la transformation du système de santé, la généralisation du dossier médical partagé (DMP) fait actuellement l'objet d'une vaste campagne de communication visant à sa promotion. Néanmoins, ce projet lancé il y a quinze ans et dont le coût est estimé entre 600 millions et 1,5 milliards d'euros, soulève de nombreuses questions en termes de protection des données privées. En effet, à la suite de cette généralisation, chaque Français pourra ouvrir son propre DMP avec ou sans son médecin traitant. A première vue, ce dossier virtuel cumule tous les prétendus avantages : il permet de stocker ses informations de santé, données sensibles selon le RGPD (Règlement général sur la protection des données), sur une seule plateforme, d'y avoir accès facilement, de simplifier la consultation des antécédents médicaux ce qui permet d'éviter les examens inutiles, de gagner en efficacité et en rapidité dans le traitement des urgences médicales et de s'adapter au nomadisme médical. Or, la centralisation numérique de tous les traitements, de tous les résultats des tests, de toutes les analyses, de toutes les prescriptions de patient est un risque majeur pour la confidentialité des données. En effet, des GAFAM aux hackeurs, ces données se révèlent être des butins de choix, permettant potentiellement chantage, fichage, atteinte à la vie privée et vente par et vers des acteurs privés peu regardants. *Facebook* n'a-t-il pas, aux États-Unis, selon le *Wall Street Journal*, commencé en 2017 à contacter des hôpitaux dans le but de collecter les données de santé anonymisées de leurs patients pour les associer aux comptes des utilisateurs du réseau social afin de leur proposer des soins de santé personnalisés ? A Singapour, les autorités n'ont-elles pas révélées, fin février 2017, qu'un ressortissant américain avait divulgué avec la complicité d'un médecin sur internet les identités et adresses de 14 200 porteurs du VIH ? Que fera l'État lorsque ce DMP sera piraté ? L'État a-t-il donné les moyens humains, financiers et techniques suffisants à l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) pour protéger ces données ? Quelles réparations pour ceux dont la séropositivité aura été révélée à leurs collègues ? Et pour celui qui se sera vu refuser un prêt ou qui verra ses primes d'assurance exploser ? Est-ce à un assureur, certes public, de gérer ces masses de e-données ? Faut-il, une nouvelle fois, charger les médecins d'une nouvelle tâche administrative à l'heure où leur temps médical se réduit ? La fuite de données privées valent-elles les mesures d'économies annoncées pour l'Assurance maladie ? Les logiciels actuels des praticiens sont-ils compatibles avec celui du DMP ? Ainsi, elle lui demande ce que le Gouvernement compte entreprendre pour sécuriser les données de santé, parties intégrantes de la vie privée des Français.

Texte de la réponse

La loi de modernisation de notre système de santé (LMSS, 2016), dans son article 96, a repositionné le DMP comme un Dossier Médical Partagé permettant le partage de documents que les professionnels de santé estiment utiles à la prévention, la continuité, la coordination et la qualité des soins. La relance du DMP par l'Assurance maladie est effective depuis la publication du décret 2016-914 du 4 juillet 2016. Il est rappelé que l'assurance maladie et les médecins conseils n'ont pas accès aux informations contenues dans le DMP des assurés. Après environ deux ans de pré-séries dans neuf départements sur une version améliorée du DMP (permettant notamment la création de son DMP par l'usager lui-même), la généralisation du DMP sur tout le territoire est effective depuis le 8 novembre 2018. Les grands principes du DMP : Le DMP est un carnet de santé électronique. Il peut être créé par tout professionnel de santé, quel que soit son mode d'exercice (ainsi que par les personnes exerçant sous sa responsabilité), par les personnes assurant des fonctions d'accueil des patients au sein des établissements de santé, des laboratoires de biologie médicale, et par les agents des organismes d'assurance maladie obligatoire. La création du DMP par un tiers nécessite au préalable le recueil du consentement exprès et éclairé du patient. Le DMP peut également être créé en ligne par le patient lui-même via le site www.dmp.fr . Le DMP est accessible aux professionnels de santé de l'équipe de soins du patient. Néanmoins, le patient titulaire du DMP peut décider de refuser l'accès à son DMP à tout professionnel de santé qu'il choisirait, y compris au sein de son équipe de soins. Le patient ne peut pas modifier les informations contenues dans son DMP (sauf rectification en application de son droit de rectification qu'il doit mettre en œuvre en lien avec le professionnel de santé auteur de l'information). Il peut néanmoins « masquer » certaines informations présentes dans son DMP. Les informations masquées sont invisibles aux professionnels de santé néanmoins autorisés à accéder au DMP, mais elles restent accessibles au médecin traitant et au professionnel de santé auteur de l'information masquée. De la même manière, les professionnels de santé peuvent rendre une information « sensible » temporairement inaccessible au titulaire du DMP. Il s'agit d'une information dont la connaissance nécessite d'être accompagné (compte rendu d'anatomopathologie posant le diagnostic de cancer, résultat d'analyse concluant à une maladie neurologique, etc.). Toute information sensible postée dans le DMP est notifiée au médecin traitant qui a alors la responsabilité d'organiser dans les 15 jours une consultation d'annonce. La sécurisation du DMP et la confidentialité des données : La centralisation des données numériques n'a pas été inaugurée avec le DMP. En effet, depuis plus de 15 ans, la caisse nationale de l'assurance maladie (CNAM) gère la base centralisée des données issues du remboursement des actes médicaux / médicaments, le système national d'information inter-régimes de l'assurance maladie (SNIIRAM). Le risque de piratage existe déjà pour les données du SNIIRAM. Pourtant, force est de constater que les mesures de sécurité mises en œuvre pour protéger le SNIIRAM depuis sa création ont été efficaces. Le DMP contient des données de santé à caractère personnel, couvertes à ce titre par le secret professionnel dans les conditions prévues aux articles L. 1110-4 du code de la santé publique dont la violation est réprimée par le code pénal. La CNAM est le responsable du traitement des données au sens de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. A ce titre, la CNAM s'engage à 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. Ainsi, la protection et la confidentialité des données du DMP sont garanties tant par des mesures de sécurisation techniques qu'organisationnelles. Ces mesures impliquent la mise en place de concepts tels que la séparation des rôles, le moindre privilège, la non répudiation des actes, le chiffrement unitaire des données. L'hébergement des données du DMP est assuré par l'hébergeur Santeos, hébergeur situé sur le territoire français, qui bénéficie d'un agrément pour une prestation d'hébergement des données de santé à caractère personnel collectées dans le cadre du DMP. Le droit français s'applique donc aux serveurs conservant les données. L'hébergeur du DMP est notamment garant de la maîtrise et la protection des échanges, via notamment l'identification et l'authentification des professionnels de santé et des patients pour préserver la confidentialité ; la protection des données pour garantir leur intégrité ; l'imputabilité des données ; la traçabilité de toute action (accès, alimentation, consultation…) ; la sauvegarde des données de santé et des traces. L'ensemble des données de santé confiées au DMP sont stockées de façon chiffrée. Chaque clé de chiffrement est protégée selon l'état de l'art. La nature des données hébergées implique que les accès d'administrations inhérents à toute structure informatique ne permettent pas d'accéder aux données des patients. L'hébergeur s'attache la collaboration d'un ou plusieurs médecins dit médecins hébergeurs. Ces derniers sont les seuls collaborateurs habilités à accéder, dans des cas précis et uniquement sur demande, aux

données de santé des patients. L'objectif de cette organisation est de garantir le secret médical entourant les données de santé. La sécurité physique et informatique est garantie par l'ensemble des mesures de sécurité devant être mises en œuvre par l'hébergeur dans le cadre de son agrément Hébergeur de Données de Santé ainsi que les mesures de sécurité découlant de l'analyse de risque effectuée sur le périmètre du projet. Les audits sécurité du DMP : De nombreux audits du DMP ont été organisés régulièrement par un certain nombre d'acteurs spécialisés dans l'évaluation de la sécurité des systèmes d'information :Fin 2011 : Audit sécurité (test d'intrusion) commandité par l'ANSSI 2019, Audit sécurité dans le cadre de la certification HDS de Worldline par Bureau Veritas (tout environnement santé dont DMP)Printemps 2012 : Audit portant sur la construction et le fonctionnement récurrent du DMP commandité par l'ASIP Santé, réalisé par PricewaterhouseCoopersPrintemps 2012 : Audit documentaire du plan de continuité de service pour le DMP commandité par l'ASIP Santé, réalisé par ThalèsAutomne 2014 : Audit basé sur une analyse du code logiciel du SI DMP commandité par l'ASIP Santé, réalisé par Henix2013 et 2016 : audits sécurité commandités par Worldline à des cabinets externes pour le renouvellement de l'agrément HDS spécifique au DMPPrintemps 2018 : audit sécurité de l'hébergement du DMP commandité par la CNAM, réalisé par E&Y Les réparations pour ceux dont les données de santé auront été divulguées : En tant que responsable de traitement, la CNAM a défini une procédure de gestion des incidents, mais également des violations de données. permettant notamment de répondre aux exigences prévues par les articles 32 et suivants du Règlement général sur la protection des données (RGPD). A ce titre, s'il devait y avoir une violation susceptible d'engendrer des risques pour les droits et libertés des personnes physiques alors une notification à la Commission nationale de l'informatique et des libertés serait réalisée dans les délais impartis (article 33 RGPD). Si cette violation était susceptible d'engendrer un risque élevé pour une ou des personnes alors une communication directe auprès de ces personnes serait également réalisée (article 34 RGPD). Cette communication devant décrire en des termes clairs et simples la nature de la violation (perte de confidentialité, d'intégrité ou encore de disponibilité), les impacts et les moyens mis en œuvre pour y remédier. La CNAM a surtout mis en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir le niveau de sécurité adapté au risque lié au traitement des données de santé au sein du DMP. L'hébergeur du DMP est agréé hébergeur de données de santé, et toutes les mesures sont mises en œuvre pour assurer, à tout moment, le niveau de sécurité permettant une protection maximale des données. La DMP compatibilité des logiciels métier : 100% des logiciels métier sont DMP compatibles. Pourtant, tous les professionnels de santé n'utilisent pas forcément les dernières versions DMP compatibles de leur logiciel métier. L'objectif de la CNAM est d'accompagner la migration des logiciels métier vers DMP-compatibilité. Aussi, une procédure a été mise en œuvre afin de guider les éditeurs dans l'évolution de leur offre logicielle. Des normes d'échange ont été définies dans un guide d'intégration (disponible sur le site du GIE à l'adresse suivante : http://www.sesam-vitale.fr/web/industriels/dmp). Par ailleurs, des actions ciblées vont être menées à compter du second semestre 2019, l'objectif étant que tous les médecins soient vus par les conseillers informatique service de la CNAM afin qu'ils puissent se connecter au DMP via leur logiciel métier DMP-compatible dont les dernières versions intègrent directement les fonctionnalités du DMP et permettent d'y accéder en un clic. Pour les professionnels de santé non équipés d'un logiciel DMP-compatible, la connexion peut aussi se faire à travers l'accès web « Professionnels de santé » du site ameli.fr.