ASSEMBLÉE NATIONALE

15ème législature

Sécurité des données du dossier médical partagé

Question écrite n° 15112

Texte de la question

M. Bastien Lachaud appelle l'attention de Mme la ministre des solidarités et de la santé sur la mise en place du dossier médical partagé (DMP). Si la mise en place d'un dossier médical numérique part de l'intention louable d'améliorer le suivi des patients, de conserver en un lieu unique accessible au patient comme aux différents praticiens des informations de santé précises, il n'en pose pas moins un certain nombre de problèmes relatifs à la sécurité des données qui y sont enregistrées. La présentation officielle du DMP précise qu'il permet notamment d'avoir accès immédiatement aux informations médicales du patient lors d'une hospitalisation, d'une première consultation ou, en cas d'urgence, de faciliter son suivi notamment lorsqu'il souffre d'une maladie chronique ou lorsque qu'il consulte un autre praticien que celui qui le suit habituellement, par exemple lors qu'il est loin de chez lui, d'éviter de prescrire des examens ou traitements déjà réalisés, ou encore d'éviter les interactions médicamenteuses. En outre, le DMP permet de retrouver l'historique de soins des 24 derniers mois, étant alimenté automatiquement par l'assurance maladie, et permet de connaître les antécédents médicaux (pathologie, allergies...), les résultats d'examens (radios, analyses biologiques...), les comptes rendus d'hospitalisations, les coordonnées des proches à prévenir en cas d'urgence ou encore les directives anticipées pour la fin de vie. Tout ceci peut contribuer à une meilleure information sur l'état de santé du patient et éviter de refaire inutilement des examens déjà subis. En revanche, la quantité de données *stockées* pose question, car si elle est utile pour le médecin, leur divulgation accidentelle peut porter d'immenses préjudices à la vie privée des personnes. En outre, les données de santé sont extrêmement sensibles, ainsi que les coordonnées personnelles de toutes les personnes à prévenir en cas d'urgence. Se pose donc nécessairement la question de la cyber sécurité des données qui y sont conservées. Outre la vie privée des personnes, l'état de santé précis est une donnée sensible, qui doit être particulièrement protégée contre des intérêts privés qui pourraient être tentés de vendre ou d'exiger des assurances spécifiques, voire de cibler des publicités selon ces données. Mais elles doivent aussi être protégées contre les menaces propres au cyberespace comme l'espionnage, le sabotage par la suppression ou la modification de données ou encore le vol de données qui pourraient être commis par des *hackeurs* individuels ou institutionnels. Entre de mauvaises mains, ces données pourraient donner lieu à toute sorte de chantages ou d'intimidations. Face à un tel risque, l'assurance maladie indique que ces données sont « hautement protégées ». Étant entendu que le détail des précautions prises n'a pas vocation, par principe, à être rendu public, il souhaite néanmoins savoir la nature des protections prises pour sécuriser les données, notamment concernant les restriction d'accès aux données et concernant le lieu physique, le droit s'appliquant aux serveurs qui conservent ces données.

Texte de la réponse

La loi de modernisation de notre système de santé, dans son article 96, a réaffirmé le positionnement du dossier médical partagé (DMP) comme 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 Caisse nationale d'assurance maladie (CNAM) est la responsable du traitement de données au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée. A ce titre, elle 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. 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. Il convient de rappeler que la centralisation des données numériques n'a pas été inaugurée avec le DMP. En effet, depuis plus de 15 ans, la 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. 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 collectées et conservées dans le DMP est assuré par la société Worldline. Worldline fait appel à l'hébergeur Santeos (société filiale de Worldline), qui bénéficie d'un agrément pour une prestation d'hébergement des données de santé à caractère personnel collectées dans le cadre du Dossier Médical Partagé. L'hébergeur Santeos est situé sur le territoire français. 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 est stocké de façon chiffrée. 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. Ainsi, la CNAM, tout comme le service d'assistance du DMP, n'accèdent pas aux données de santé à caractère personnel contenues dans le DMP. 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 d'Hébergeur de Données de Santé ainsi que des mesures de sécurité découlant de l'analyse de risque effectuée sur le périmètre du projet. Par ailleurs, afin de préserver la sécurité de l'application et des données de l'utilisateur, l'utilisation de l'application DMP est impossible si l'appareil de ce dernier est considéré comme corrompu, il en sera dès lors ainsi si l'appareil de l'utilisateur est « rooté », « jailbreaké » ou qu'une faille de sécurité est détectée. Ainsi au lancement de l'application, si la corruption de l'appareil de l'utilisateur est détectée, un message d'avertissement apparaitra pour alerter l'utilisateur et l'application se fermera automatiquement. De nombreux audits du DMP ont été organisés régulièrement, de 2011 à 2018, par des d'acteurs spécialisés dans l'évaluation de la sécurité des systèmes d'information. En tant que responsable de traitement, la CNAM a défini une procédure de gestion des incidents, mais également des violations de données qui permet de répondre aux exigences prévues par les articles 32 et suivants du règlement général sur la protection des données (RGPD). Ainsi, s'il devait y avoir une violation susceptible d'engendrer des risques pour les droits et libertés des personnes physiques, 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, une communication directe auprès des 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 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.

Données clés

Auteur : M. Bastien Lachaud
Circonscription : Seine-Saint-Denis (6e circonscription) - La France insoumise
Type de question : Question écrite

Version web : https://www.assemblee-nationale.fr/dyn/15/questions/QANR5L15QE15112

Numéro de la question : 15112
Rubrique : Santé
Ministère interrogé : Solidarités et santé
Ministère attributaire : Solidarités et santé

Date(s) clée(s)

Date de signalement : Question signalée au Gouvernement le 12 octobre 2020
Question publiée au JO le : 11 décembre 2018, page 11333
Réponse publiée au JO le : 1er décembre 2020, page 8791