ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 23034	De **Mme Sandrine Doucet** (Socialiste, républicain et citoyen - Gironde)	**Question écrite**

Ministère interrogé > Affaires sociales et santé	**Ministère attributaire** > Affaires sociales et santé

Rubrique >santé	**Tête d'analyse** >politique de la santé	**Analyse** > données médicales dématérialisées. protection.

Question publiée au JO le : **02/04/2013**
Réponse publiée au JO le : **30/08/2016** page : **7633**
Date de changement d'attribution : **12/02/2016**
Date de signalement : **12/07/2016**

Texte de la question

Mme Sandrine Doucet attire l'attention de Mme la ministre des affaires sociales et de la santé sur la question de la diffusion des données médicales sur internet. À la suite de plusieurs cas de négligence, ayant eu pour conséquence la diffusion de dossiers de patients sur internet, la protection des données médicales semble, aujourd'hui, être mise à mal. En effet, des données et fichiers médicaux ont pu, à cause d'imprudences ou d'erreurs commises par des prestataires peu scrupuleux, être révélés sur la toile et diffusés à la vue de tous, proches, employeurs, assureurs... Des règles de sécurité, régulant la mise en ligne des données médicales pour les hôpitaux, existent depuis pourtant plus de dix ans, obligeant, par exemple, à passer par un hébergeur de données de santé agréé. Cependant, de nombreux établissements ne connaissent pas forcément ces mesures de sécurité ou ne les appliquent pas. Ces cas de divulgation de données sensibles demeurent très embarrassants et peuvent conduire à des poursuites judiciaires. La CNIL a, ainsi, été interpellée par plusieurs établissements et a entrepris de vérifier le niveau de sécurité de plusieurs prestataires agréés mais aussi non agréés. En outre, les professionnels de santé s'inquiètent de la multiplication des moyens de diffusion de l'information due au passage du format papier au numérique dans les hôpitaux. Ces avancées technologiques améliorent fortement les conditions de travail des professionnels et personnels administratifs de la santé, mais, sans mesures de sécurité adéquates, elles peuvent conduire à des fuites, voire à des situations de chantage numérique autour d'informations médicales pouvant être piratées. Elle souhaite ainsi savoir comment le ministère des affaires sociales et de la santé souhaite s'emparer de ce problème et pallier ce manque de sécurité autour des dossiers de patients pouvant se retrouver sur internet. Elle la remercie de sa réponse et la prie de bien vouloir la tenir informée des suites données à ce dossier.

Texte de la réponse

Alors qu'une révolution numérique touche aujourd'hui le monde de la santé, comme de multiples autres secteurs d'activité, ses avantages sont de mieux en mieux perçus pour la qualité du système de santé. Toutefois, corrélativement, des menaces apparaissent et la « cybercriminalité » multiplie les attaques sur les sources de données de santé sensibles et sur les systèmes informatiques des professionnels et les établissements de santé avec un fort risque sur la sécurité des prises en charge des patients. Ce risque n'est pas propre à la France et au monde de la santé mais notre pays s'y prépare activement dans le cadre d'initiatives nationales et de démarches de coopération au niveau européen. Il est essentiel que le développement de l'e-santé (qui inclut le domaine médico-social) et des usages du numérique en santé se fasse dans un cadre de confiance permettant l'acceptation de l'innovation par les citoyens, les patients et les professionnels. Il importe donc que l'Etat et les pouvoirs publics, l'ensemble des acteurs

de santé, mais aussi l'ensemble des citoyens prennent toute la mesure de leurs responsabilités dans ce domaine pour en garantir le bon fonctionnement. Pour sa part, en articulation avec le plan gouvernemental contre la cybercriminalité, le ministère des affaires sociales et de la santé a pris la mesure de la menace et conduit avec détermination depuis plusieurs années, un ensemble d'actions visant à assurer un haut niveau de protection des systèmes d'information et des données de santé. Il s'agit bien sûr de lutter contre la malveillance (phénomène de piratage), mais également d'éviter les dysfonctionnements liés à des erreurs humaines ou à un défaut de formation ou de sensibilisation des utilisateurs. La politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS), déclinaison de la politique de sécurité des systèmes d'information de l'Etat, a été approuvée par arrêté ministériel du 1er octobre 2015. Par ailleurs, sous le pilotage de la délégation à la stratégie des systèmes d'information de santé (DSSIS), avec le concours de l'agence des systèmes d'information partagés de santé (ASIP Santé), les premiers éléments d'une "Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) " ont été publiés dès 2013 et un ensemble de référentiels et de guides ont été régulièrement produits depuis. La PGSSI-S s'applique à l'ensemble des acteurs de santé, établissements et professionnels, quels que soient les modes d'organisation et les lieux d'exercice. Le dispositif d'agrément des hébergeurs de données de santé mis en œuvre sur la base des dispositions du décret du 4 janvier 2006 s'est fortement développé. Depuis la mise en place du comité d'agrément des hébergeurs, début 2009, 292 dossiers ont été réceptionnés, 138 dossiers ont été agréés, 69 ont été refusés et 57 sont en cours de procédure. Afin de rendre les systèmes d'information plus performants, en particulier en termes de qualité et de sécurité des soins, le ministère a lancé, en novembre 2011, le programme « Hôpital numérique ». Dans ce cadre, un guide pour les directeurs d'établissement de santé « Introduction à la sécurité des systèmes d'information », a été publié en novembre 2013. Il est en cours d'actualisation. Au niveau des régions, il revient aux agences régionales de santé d'assurer le pilotage de l'e-santé et de veiller à la mise en œuvre des mesures de sécurisation des systèmes d'information de santé. La loi de modernisation de notre système de santé (LMSS) comprend un ensemble de dispositions faisant évoluer sensiblement le cadre de l'e-santé dans le sens de la simplification et de la sécurisation de l'utilisation des données de santé. Il convient de citer notamment : - l'obligation de signalement aux ARS et aux autorités compétentes de l'Etat, les incidents graves de sécurité des systèmes d'information prévue par l'article 110 (art. L.1111-8-2 du CSP) ; - 'opposabilité de référentiels d'interopérabilité et de sécurité par voie d'arrêté ministériel (art. 96 de la LMSS et art. L.1110-4-1 du CSP) ; ainsi, il est prévu que les référentiels publiés de la PGSSI-S sur l'authentification et l'identification des acteurs de santé soient rendus opposables par arrêté en 2017 ; - l'article 107 (art. 6132-1 et suivants du CSP) relatif aux groupements hospitaliers de territoires (GHT), confère à ceux-ci une responsabilité en matière de systèmes d'information qui comprend la dimension sécurité des systèmes d'information (le ministère prépare actuellement à l'attention des GHT un guide qui comportera un chapitre sur ce thème) ; - l'article 204-I-5 prévoit que soit définie par ordonnance la réforme du dispositif d'agrément des hébergeurs de données de santé dans le sens d'une certification sur vérification de conformité technique à un référentiel défini par les pouvoirs publics. La Commission européenne mène également une action dynamique en matière de protection des données sensibles et de sécurité du numérique et contribue à construire un cadre juridique adapté avec plusieurs règlements et directives adoptés récemment : - règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (dit « règlement eIDAS) ; -Règlement (UE) no 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; - projet de Directive (EU) du parlement européen et du conseil on Security of Network and Information Systems (dite Directive « NIS ») adoptée le 6 juillet par le Parlement européen. Ce texte qui doit participer à la construction d'un marché unique du numérique dans l'UE, a pour objectif de renforcer la réactivité des 28 États membres et de stimuler la coopération entre les autorités de lutte contre la cybercriminalité, tout en leur donnant des moyens techniques et légaux appropriés. Lors de la présentation des orientations de la stratégie nationale pour l'e-santé, le 4 juillet 2016, la ministre des affaires sociales et de la santé a notamment insisté sur la nécessaire confiance qui doit accompagner le développement du numérique en santé et a annoncé un plan d'action sur la sécurisation des systèmes d'information.