RGPD

Sécuriser les données de santé, c'est déjà sécuriser leur envoi…

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la problématique de la sécurité des communications dans le cadre des envois électroniques et postaux contenant des données de santé à caractère personnel.

Selon la Cnil, la notion de données de santé à caractère personnel doit être entendue très largement. Il s'agit de toutes les données « *relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne* »[1].

Entrent donc dans cette catégorie de données sensibles : (i) celles qui sont des données de santé par nature (antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap(s), etc.) ; (ii) celles, qui, du fait de leur croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne ; et (iii) celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Compte tenu de leur sensibilité, les données de santé à caractère personnel bénéficient d'un régime juridique très protecteur (RGPD, article 9). L'organisme qui les traite et qui, comme tout responsable du traitement, est tenu à une obligation de sécurité, doit mettre en œuvre toutes les mesures techniques et organisationnelles qui s'imposent pour préserver leur intégrité, leur disponibilité et leur confidentialité.

Il doit ainsi prendre toutes les précautions utiles, au regard des risques présentés, pour empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès, et ce notamment au moment de leur collecte, lors de leur conservation, mais aussi durant leur transmission (RGPD, articles 5 et 32).

Les affaires

Dans deux affaires récentes – l'une qui se déroule en Italie l'autre en Suède – le responsable du traitement a fait l'objet d'une sanction pour ne pas avoir suffisamment protégé les données de santé contenues dans les correspondances adressées aux patients destinataires.

Dans la première affaire[2], il était reproché à un organisme d'avoir, dans le cadre d'une campagne d'information concernant la distribution en Italie d'Eversense XL - « *un système de surveillance continue du glucose pour les personnes souffrant de diabète* » -, saisi, dans le champ « *cc* », les adresses électroniques de tous les patients concernés par le dispositif, permettant ainsi à tous les destinataires de connaître l'identité des autres patients. Le courriel litigieux n'ayant été adressé qu'aux seuls utilisateurs du système de surveillance susvisé, l'autorité italienne de protection des données en a conclu que les informations contenues dans ce courriel devaient de facto s'analyser comme des données à caractère personnel relatives à la santé. Dans ce contexte, elle a estimé que les mesures techniques et organisationnelles mises en œuvre étaient insuffisantes et que l'organisme avait, par une telle communication, « *divulgué aux destinataires des données relatives à l'état de santé des autres patients* » caractérisant ainsi un manquement aux dispositions des articles 5 paragraphe 1, point a) et f), et 9 du RGPD.

Dans la seconde affaire[3], un organisme a été épinglé pour avoir envoyé par voie postale à des patients des convocations à des visites de soins, en utilisant des enveloppes à fenêtre laissant apparaître, outre le nom et

l'adresse des patients, le nom des établissements de soins concernés. Selon l'autorité de contrôle suédoise, « *les données relatives à ces établissements de santé (...) constituent des données de santé au sens de l'article 4(15) du RGPD* ». Par conséquent, et dans la mesure où, du fait de l'utilisation des enveloppes à fenêtre, des données personnelles sensibles étaient « *entièrement visibles* » par tous ceux qui ont été en contact avec les lettres litigieuses, l'autorité de contrôle a prononcé une amende administrative à l'encontre de l'organisme pour manquement caractérisé à l'obligation de sécurité.

Quelles recommandations ?

Pour rappel et au risque de se répéter, le professionnel de santé est tenu de prendre toutes les précautions utiles - au regard des risques présentés par son traitement - pour préserver la sécurité des données. Cela passe notamment par : la sensibilisation du personnel accédant aux données, la gestion des habilitations et des authentifications, la sécurisation des postes de travail, la protection du réseau informatique interne, la sécurisation des serveurs, ou encore la protection des locaux

Il ne faut pas oublier la sécurisation des échanges, qui est tout aussi indispensable que les mesures précédemment citées, et ce qu'il s'agisse d'échanges entre professionnels intervenant dans la prise en charge du patient ou entre un professionnel et un patient. Dans ce cadre, plusieurs mesures sont recommandées par la Cnil : (i) procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard et transmettre le secret par un envoi distinct et via un canal différent ; (ii) utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ; (iii) choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes. N'oublions pas l'essentiel : pour les envois postaux, protéger les données par l'utilisation d'une enveloppe adaptée (qui ne rend pas visible le contenu du courrier) et, pour les envois électroniques, vérifier la liste des destinataires en copie afin de ne pas porter atteinte à la confidentialité des données. Sécuriser les données de santé, c'est aussi sécuriser leur envoi...

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

(2) GPDP, 7 juillet 2022, n° 9809998

(3) IMY, 17 janvier 2023, 2022-695.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info