RGPD

Sécurité : empêcher les accès inappropriés au dossier médical

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 différentes autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question des règles d'habilitation qui font souvent défaut dans les établissements de santé, et ce en violation du principe de sécurité.

Il ressort des termes de l'article 5.1.f du RGPD que les données doivent être traitées « *de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* ». L'article 32 du même texte ajoute que le responsable du traitement est tenu de mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». En d'autres termes, le responsable du traitement est le garant de la sécurité des données personnelles qu'il traite dans le cadre de l'exercice de son activité. À ce titre, il lui appartient notamment de s'assurer que seules les personnes autorisées ont accès aux données personnelles, à savoir uniquement les personnes ayant besoin d'en connaître dans le cadre de l'exercice de leur fonction au sein de l'organisme.

Entre 2020 et 2024, la Cnil s'est intéressée à la situation des établissements de santé. Au terme de treize contrôles, l'autorité française de protection des données a pu constater que les mesures mises en œuvre par ces établissements concernant la sécurité du dossier patient informatisé (DPI) sont insuffisantes notamment en raison d'une politique de gestion des habilitations trop souvent inadaptée, en ce qu'elle permet à des catégories de personnel d'accéder à des données de santé de patients dont elles n'ont pas la charge. L'affaire commentée illustre l'insuffisance des moyens mis en œuvre par les établissements de santé.

L'affaire[3]

L'autorité italienne de protection des données (ou « *GPDP* ») a reçu plusieurs plaintes concernant des accès suspects, au sein d'un établissement de santé, aux dossiers médicaux de patients. L'enquête a montré que ces accès étaient, en effet, inappropriés dans la mesure où ils ont été effectués par des professionnels de santé qui n'étaient pas en charge des patients concernés par les dossiers médicaux consultés. La GPDP a, après avoir analysé les mesures en place au sein de l'établissement, sanctionné ce dernier pour avoir traité des données à caractère personnel en violation notamment des article 5.1.f et 32 du RGPD, la configuration du système permettant à tout personnel de santé de l'organisme d'accéder, sans restriction, aux dossiers médicaux des patients.

Selon l'autorité, « *les mesures mises en place n'apparaissaient pas pleinement adéquates pour garantir que seul le personnel de santé traitant un patient puisse accéder au dossier de santé de ce dernier* », tout en rappelant que « *le responsable du traitement doit identifier, par rapport aux différentes fonctions auxquelles le personnel est affecté, des profils spécifiques pour l'accès au dossier, y compris en ce qui concerne les organes administratifs de la direction médicale* ». Par ailleurs, la GPDP a relevé que l'établissement n'avait

prévu aucun système de détection des anomalies visant à identifier les comportements anormaux (ou à risque) relatifs aux opérations effectuées par le personnel de l'organisme.

Quelles recommandations ?

Les établissements de santé devraient, selon la Cnil, mettre en place des mesures visant à sécuriser les accès au dossier médical, grâce notamment à une politique d'authentification robuste, qui devrait prévoir a minima (i) un identifiant unique par utilisateur,interdire les comptes partagés entre plusieurs utilisateurs et (ii) imposer le recours à des mots de passe suffisamment complexes.

Par ailleurs, ils devraient implémenter des règles d'habilitation répondant à l'exigence selon laquelle un professionnel de santé ou un agent ne peut accéder qu'aux seules données dont il a besoin de connaître.

Selon la Cnil, cette deuxième mesure passe par le respect des deux critères suivants : (i) le critère du « *métier exercé* » : un agent responsable de l'accueil des patients dans la structure de soins ne doit accéder « *qu'au dossier administratif du patient et non aux données médicales* », alors qu'un médecin accèdera « *également aux données médicales* » ; (ii) le critère de l'« *équipe de soins* » (tel que défini à l'article L.1110-12 du code de la santé publique) : seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués doivent pouvoir avoir accès aux données couvertes par le secret médical.

La Cnil précise, toutefois, consciente des enjeux et des nécessités du métier, que « *les habilitations accordées peuvent être complétées d'un mode "bris de glace", qui permet aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient* ». Enfin, la Cnil recommande l'implémentation d'un dispositif de journalisation permettant de tracer les accès au dossier : « *cette traçabilité doit non seulement permettre d'indiquer qui s'est connecté à la base de données à quel moment, mais, plus précisément, qui a accédé à quoi. Des contrôles réguliers de ces accès doivent être opérés, afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes. Il est vivement recommandé de disposer d'un système d'analyse automatique des journaux de connexion afin de repérer les accès qui semblent anormaux.* »

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au#:~:text=La%20CNIL%20a%20mis%20en,du%20besoin%20d'en%20conna%C3%AEtre.

(2) GPDP, 22 février 2024.

(3) https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au#:~:text=La%20CNIL%20a%20mis%20en,du%20besoin%20d'en%20conna%C3%AEtre