https://affairesjuridiques.aphp.fr/textes/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au-dossier-patient-informatise-dpi/
Données de santé : la CNIL rappelle les mesures de sécurité et de confidentialité pour l’accès au dossier patient informatisé (DPI)
09/02/2024
En réaction à plusieurs alertes d’accès illégitimes aux données de patients contenues dans le dossier patient dématérialisé (DPI), la Commission nationale de l’informatique et des libertés (CNIL) a procédé, entre 2020 et 2024, à treize contrôles auprès d’établissements de santé.
Selon la CNIL, ces contrôles « ont permis de constater que les mesures de sécurité informatique et la politique de gestion des habilitations étaient parfois inadaptées aux besoins des établissements, en permettant notamment à des professionnels de santé ne participant pas à la prise en charge du patient d’accéder à des informations relatives à ce dernier ». Toutefois, la CNIL ne précise pas le nombre, ni l’identité des établissements concernés.
La CNIL prévoit de prendre « des mesures correctrices contre d’autres établissements en 2024 » et a mis en demeure plusieurs établissements de mettre en œuvre des mesures de sécurité permettant de préserver la sécurité et la confidentialité des données du DPI. Ces mesures sont de trois types.
Tout d’abord, « sécuriser les accès au système grâce à une politique d’authentification robuste », notamment en créant des mots de passe suffisamment complexes.
Ensuite, prévoir des « habilitations spécifiques pour chaque professionnel de santé ou agent de l’établissement n’accède qu’aux dossiers dont il a à connaître ». Cette politique doit prendre en compte le métier exercé (un agent responsable de l’accueil des patients dans la structure ne doit accéder qu’au dossier administratif du patient et non aux données médicales, alors qu’un médecin accèdera également aux données médicales) et la notion d’équipe de soins, telle que définie par la loi (article L. 1110-12 du Code de la santé publique), afin que seuls les professionnels impliqués dans la prise en charge d'un patient puissent avoir accès aux informations couvertes par le secret médical. Des mesures de confidentialité doivent également être prévues pour certains dossiers particuliers, comme ceux de patients provenant d’un établissement pénitentiaire.
A noter qu’un mode « bris de glace » peut être mis en place en cas d’urgence afin de permettre aux agents administratifs et professionnels de santé d’avoir accès à d’autres données pour tout patient, sous réserve de tracer et surveiller de tel sorte que toute personne y ayant recours puisse être identifiée et justifier des conditions de son utilisation.
Enfin, il est nécessaire de tracer les accès au DPI pour savoir « qui a accédé à quoi ». « Des contrôles réguliers de ces accès doivent être opérés, afin d’identifier ceux susceptibles d’être frauduleux ou illégitimes. ». La CNIL recommande pour cela de disposer d’un « système d’analyse automatique des journaux de connexion afin de repérer les accès qui semblent anomaux » (exemple : un usage fréquent du mode « bris de glace »).