NEWSLETTER E-SANTE

NUMÉRO 11 ● 2024

ÉQUIPE

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocat counsel

SOMMAIRE

L'ENVOI D'UN COURRIEL, À UNE LISTE DE DESTINATAIRES ATTEINTS DU VIH, SANS UTILISER LA FONCTION COPIE CACHÉE EST CONTRAIRE AU RGPD

ACTUALITES

L'autorité de contrôle anglaise a infligé une amende à un organisme éducatif qui, en transmettant un courriel aux membres d'un programme d'accompagnement des personnes atteintes du VIH sans utiliser la fonction copie cachée, a dévoilé des informations sur l'infection des destinataires.

ICO (Royaume-Uni), 6 mars 2024

Le 6 octobre 2022, un organisme caritatif d'éducation a transmis à 270 destinataires un courrier électronique les invitant à une conférence sur la nutrition.

L'invitation s'inscrivait dans le cadre du « *programme de santé* positive », un programme destiné aux personnes atteintes du VIH.

Problème : le courriel a été envoyé, par erreur, en utilisant la fonction « copie » et non la fonction « copie cachée ». En conséquence, des informations relatives à l'état de santé des 270 destinataires ont été transmises.

Saisie de plusieurs plaintes, l'autorité de contrôle anglaise a considéré, outre que les données traitées par l'organisme caritatif sont des données de santé, que le responsable du traitement avait enfreint les principes de sécurité posé aux articles 5.1.f et 32 du RGPD du Royaume-Uni.

Compte tenu de ce qui précède, l'autorité de contrôle a infligé une amende de 7500 livres à l'encontre de l'organisme pour manquement aux obligations de sécurité qui pèsent sur les responsables du traitement.

Source : ici

LA TEMPÉRATURE CORPORELLE EST UNE DONNÉE DE SANTE QUI DOIT ÊTRE PROTÉGÉE COMME UNE AUTRE

L'autorité de contrôle espagnole a infligé une amende à une clinique qui, pendant la crise du Covid, obligeait les patients à mesurer leur température corporelle au vu et au su de tous.

AEPD (Espagne), 8 février 2024

Pendant la crise du covid, les patients se présentant à la réception d'une clinique étaient sommés, conformément à la législation locale, de prendre leur température à l'aide d'un thermomètre fixé au mur situé entre la salle d'attente et la réception.

Un patient, constatant que le thermomètre affichait la mesure de la température sur un écran visible par les autres personnes présentes dans la salle d'attente, a refusé de prendre sa température. N'ayant pas été autorisé à réaliser sa prise de sang, il a déposé une plainte devant l'autorité de contrôle espagnole.

Pour sa défense, la clinique indiquait :

- Que la température d'une personne n'est pas une donnée personnelle ;
- Qu'en tout état de cause, la clinique n'est pas responsable du traitement car les relevés de température étaient effectués par les patients eux-mêmes ;
- Qu'il n'est pas démontré que, le jour où le patient s'est présenté, il y avait effectivement d'autres personnes dans la salle d'attente qui auraient pu voir sa température ;
- Que, compte tenu de l'emplacement du thermomètre et d'un dispositif d'obstruction visuelle, il était presque impossible que la température soit visible par d'autres personnes ;
- Qu'en ce qui concerne le cas d'espèce, le patient n'a pas pris sa température, et donc qu'en tout état de cause aucun traitement de ses données à caractère personnel n'a été effectué.

L'autorité de contrôle a considéré, au contraire :

- Que la température corporelle est une donnée de santé et qu'ainsi les contrôles de température peuvent constituer un traitement au sens du RGPD ;
- Que ce traitement, réalisé pendant la crise du Covid, était autorisé par la législation locale et donc reposait sur une base légale valable ;
- Que le résultat de la mesure de la température s'affichait pendant plusieurs secondes sur l'écran de l'appareil, le rendant visible des autres personnes présentes dans la salle d'attente. Qu'en conséquence, cela permet aux autres personnes de déduire l'état de santé de la personne.
- Compte tenu de ce qui précède, l'autorité de contrôle a (i) considéré que la clinique n'avait pas mis en œuvre les mesures de sécurité nécessaires pour éviter que les autres personnes puissent voir la température du patient conformément aux articles 5.1.f et 32 du RGPD et a (ii), en conséquence, infligé une amende de 20.000 euros à la clinique.

Source : ici

LA VIDÉOSURVEILLANCE DANS LES CHAMBRES DES EHPAD : EST-CE LICITE ?

Par une délibération du 29 février 2024, la CNIL a adopté ses recommandations relatives à la mise en place de dispositifs de vidéosurveillance au sein des chambres des établissements accueillant des personnes âgées.

En février 2023, la CNIL annonçait lancer une consultation publique relative à la vidéosurveillance dans les chambres d'EHPAD. Un an plus tard, la CNIL a publié ses recommandations et encadré l'utilisation de cet outil.

Le principe : l'interdiction

La CNIL considère que, par principe, l'installation d'un dispositif de vidéosurveillance dans la chambre d'un résident est disproportionnée.

Plus précisément, et même si la personne concernée y consent, l'installation des caméras est interdite, y compris pour les finalités suivantes :

- Améliorer le service offert ;
- Assurer la sécurité des personnes concernées en cas de chute ou d'accident.

La CNIL justifie ces interdictions par le fait que d'autres dispositifs moins attentatoires à la vie privée existent et devraient être privilégiés.

L'exception : les suspicions fortes de maltraitance

Par exception, la CNIL considère que l'installation d'un tel dispositif est possible à deux conditions.

Premièrement, il doit y avoir une « *suspicion de maltraitance basée sur un faisceau d'indices concordants (hématomes, changements comportementaux…) malgré l'existence de dispositifs alternatifs déjà mis en place* ».

Deuxièmement, une enquête interne doit, préalablement, avoir été initiée et ne doit pas avoir permis de détecter des actes de maltraitance avec certitude, mais doit établir que de fortes suspicions subsistent quant à l'existence de tels actes.

C'est seulement à ces conditions qu'un dispositif de vidéosurveillance pourra être installé dans la chambre et, s'il existe toujours des doutes par la suite, dans les lieux d'intimité (douche, toilettes…).

Les garanties appropriées

Bien qu'exceptionnellement autorisé, l'installation d'un tel dispositif suppose la mise en œuvre des garanties appropriées suivantes : (i) limiter l'activation dans le temps, (ii) désactiver le dispositif lors des visites de proches, (iii) déterminer les conditions justifiant l'installation d'un tel dispositif, (iv) informer les personnes concernées, (v) flouter les parties intimes, (vi) indiquer dans le règlement intérieur qu'un tel dispositif peut être mis en place, (vii) installer le dispositif de manière concertée et, enfin, (viii) sensibiliser et former le personnel.

L'obligation d'effectuer une analyse d'impact

Pour finir, au regard des risques élevés qu'est susceptible d'engendrer ce traitement pour les droits et libertés des personnes concernées, la CNIL a indiqué qu'une analyse d'impact (AIPD) est obligatoire.

Source : ici

PREMIÈRES RECOMMANDATIONS DE LA CNIL EN MATIÈRE D'IA : QUELS EXEMPLES APPLIQUÉS AU SECTEUR DE LA SANTÉ ?

VU DANS LA PRESSE

DSIH, mai 2024

La CNIL a émis, ce mois-ci, ses premières recommandations en matière de développement de systèmes d'intelligence artificielle. Avec pour objectif « d'aider les professionnels à concilier innovation et respect des droits des personnes », ces recommandations s'appliquent pleinement au secteur de la santé, comme en témoignent plusieurs exemples donnés par l'autorité de contrôle.

1. Une première série de recommandations en matière d'IA attendues et circonscrites

La CNIL a été interrogée par plusieurs acteurs sur l'application du RGPD à l'IA et, plus particulièrement, aux systèmes d'IA génératives. Dans ce cadre, la CNIL a émis des premières recommandations sur le développement des systèmes d'IA, présentées sous forme de 7 fiches pratiques (lesquelles seront complétées après consultation publique).

Le périmètre de ces recommandations est donc limité à la phase de développement des systèmes d'IA, sous réserve qu'elle « implique » le traitement de données personnelles soumis au RGPD. Cette phase de développement du système d'IA comprend la conception du système, la constitution de la base de données, l'apprentissage et, parfois, l'intégration, indique la CNIL.

Sans rentrer dans la description et l'analyse de chacune de ces fiches qui s'appliquent, de façon générale, à tous les secteurs dont le secteur de la santé, certaines d'entre elles nous livrent des précisions et/ou des exemples concrets, particulièrement instructifs en santé.

2. Quelques cas concrets appliqués au secteur de la santé

2.1 Développement d'un système d'IA et recherche scientifique

Parce qu'il n'est pas toujours évident de déterminer si le développement d'un système d'IA poursuit un objectif de recherche scientifique, la CNIL rappelle, de façon générale, ce qu'on entend par traitement de données relevant de la « recherche scientifique ». La CNIL propose ainsi « *un faisceau de critères* » permettant de déterminer si un traitement de données ayant pour objectif la recherche, relève bien de la recherche scientifique.

Ces critères sont notamment (i) le mode de financement du programme de recherche (par exemple, un financement par l'Agence Nationale de la Recherche), ou, en particulier pour la recherche scientifique privée, (ii) l'analyse et la réunion de cinq critères que sont la nouveauté, la créativité, l'incertitude, la systématicité (« *C'est par exemple le cas des exigences méthodologiques particulières pour les traitements mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* ») et la transférabilité/la reproductibilité.

En matière de recherche scientifique, la CNIL montre une certaine souplesse quant aux objectifs (finalités) d'un traitement à déterminer au stade du développement d'un système d'IA, « *compte tenu des difficultés que les chercheurs peuvent avoir à cerner [toutes les finalités] dès le début de leurs travaux* ». La CNIL admet effectivement que le responsable de traitement puisse ne pas indiquer l'ensemble du ou des objectif(s) poursuivi(s), et apporter, au fur et à mesure de l'avancement du projet concerné, des informations plus précises sur ces objectifs.

Par ailleurs, la CNIL revient sur les conditions de réutilisation d'un jeu de données, initialement constitué à des fins recherche scientifique, à d'autres fins dans le cadre du développement d'un système d'IA :

- L'anonymisation préalable des données ;
- Le respect de l'exigence de la compatibilité entre la finalité initiale du jeu de données et la nouvelle et ce, dans le respect du RGPD (information des personnes sur la nouvelle finalité, identification d'une base légale…).

2.2. Développement d'un système d'IA en santé et responsabilité des parties prenantes

Dans le cadre du développement d'un système d'IA, plusieurs acteurs peuvent influer sur le pourquoi (objectif/finalités) et le comment (moyens mis en œuvre) d'un traitement de données personnelles.

A cet égard, la CNIL prend l'exemple de centres hospitaliers universitaires qui développent un système d'IA pour l'analyse de données d'imagerie médicale et qui, dans ce cadre, décident d'utiliser un protocole identique d'apprentissage fédéré (dont l'objectif est d'exploiter des données pour lesquels chaque centre est « *responsable de traitement* » distinct, sans que chaque centre ne s'en rende mutuellement destinataire). Dans un tel cas, les centres hospitaliers sont considérés par la CNIL comme « *responsables conjoints du traitement* » d'apprentissage fédéré dans la mesure où ils déterminent ensemble (i) l'objectif du traitement, à savoir l'entrainement d'un système d'IA médicale et également (ii) les moyens de ce traitement, consistant en la mise en place d'un protocole et la détermination des données exploitées.

2.3. Développement d'un système d'IA en santé et mesures de protection des données personnelles dès la conception

La CNIL détaille la façon dont les mesures de protection des données personnelles pourraient être mises en place « *au regard de leur influence sur les performances techniques – théoriques et opérationnelles* » du système d'IA en développement. Pour la CNIL, ces mesures seront considérées comme « bénéfiques » en raison (i) de « *leur capacité à réduire les conséquences d'une éventuelle perte de confidentialité des données* » et (ii) de « *la possibilité éventuelle d'utiliser le modèle entrainé en phase opérationnelle sur des données ayant fait l'objet de mesures de protection identique* ».

La CNIL nous livre un exemple en santé concernant le développement d'un système d'IA d'aide au diagnostic. Selon l'autorité de contrôle, le risque de perte de confidentialité de données, en l'occurrence sur l'âge des patients, peut être « *réduit drastiquement* » en jouant simplement sur la définition des types de données à traiter (choisir un champ [mois- année] ou [année] au lieu de [jour-mois-année]) et, « *cela sans préjudice sur la capacité de généralisation de son système* ».

Ces premiers éclairages vont être prochainement enrichis par la CNIL. A suivre…

Source : ici

AGRESSION DES PROFESSIONNELS DE SANTÉ : QUELLE RESPONSABILITÉ POUR L'ÉTABLISSEMENT DE SANTÉ EMPLOYEUR ?

VU DANS LA PRESSE

La Veille Acteurs de Santé, mai 2024

La sécurité des professionnels de santé est au cœur de l'actualité, en particulier face à l'augmentation des agressions dont ils sont victimes. Le Gouvernement a ainsi présenté, il y a quelques mois, un plan national sur ce sujet. Concernant le volet pénal de ce plan, une proposition de loi visant à renforcer la sécurité des professionnels de santé a été ainsi adoptée, en mars dernier. Cette problématique de sécurité intéresse également les établissements de santé, en qualité d'employeur, comme l'illustre une récente décision de la Cour de cassation.

Quand la Cour de cassation s'en mêle

Tel était le cas dans l'affaire soumise à la Cour de cassation. Une médecin urgentiste a été victime d'une agression physique violente commise par une patiente qui, après s'être introduite dans l'espace ambulatoire, s'était jetée sur la médecin urgentiste, au motif qu'elle ne prêtait pas attention à elle. Elle l'aurait alors agrippée par les cheveux avant de la frapper, une fois au sol, à coups de poings et de pied. Fort heureusement, l'équipe de soins est intervenue pour les séparer.

C'est dans ce contexte que l'établissement de santé s'est retrouvé devant les tribunaux judiciaires : la médecin urgentiste, qui invoquait la « *faute inexcusable* » de l'employeur, réclamait l'indemnisation de nombreux préjudices, tels que les souffrances endurées, le préjudice esthétique et le déficit fonctionnel.

En défense, l'établissement de santé soutenait ne pas pouvoir prévoir ni empêcher l'agression commise par une patiente. La médecin urgentiste a vu sa demande rejetée devant la juridiction du premier degré, puis a finalement obtenu gain de cause devant la juridiction du second degré (Cour d'appel de Versailles). Un pourvoi a été formé devant la Cour de cassation par l'établissement de santé.

La Cour de cassation a confirmé la décision de la juridiction du second degré en relevant notamment que « *l'employeur ne pouvait ignorer le risque d'agression encouru par son personnel soignant, médecins compris* », compte tenu de « *la recrudescence d'actes violents au sein du service des urgences de l'hôpital […] évoquée dès 2015* ».

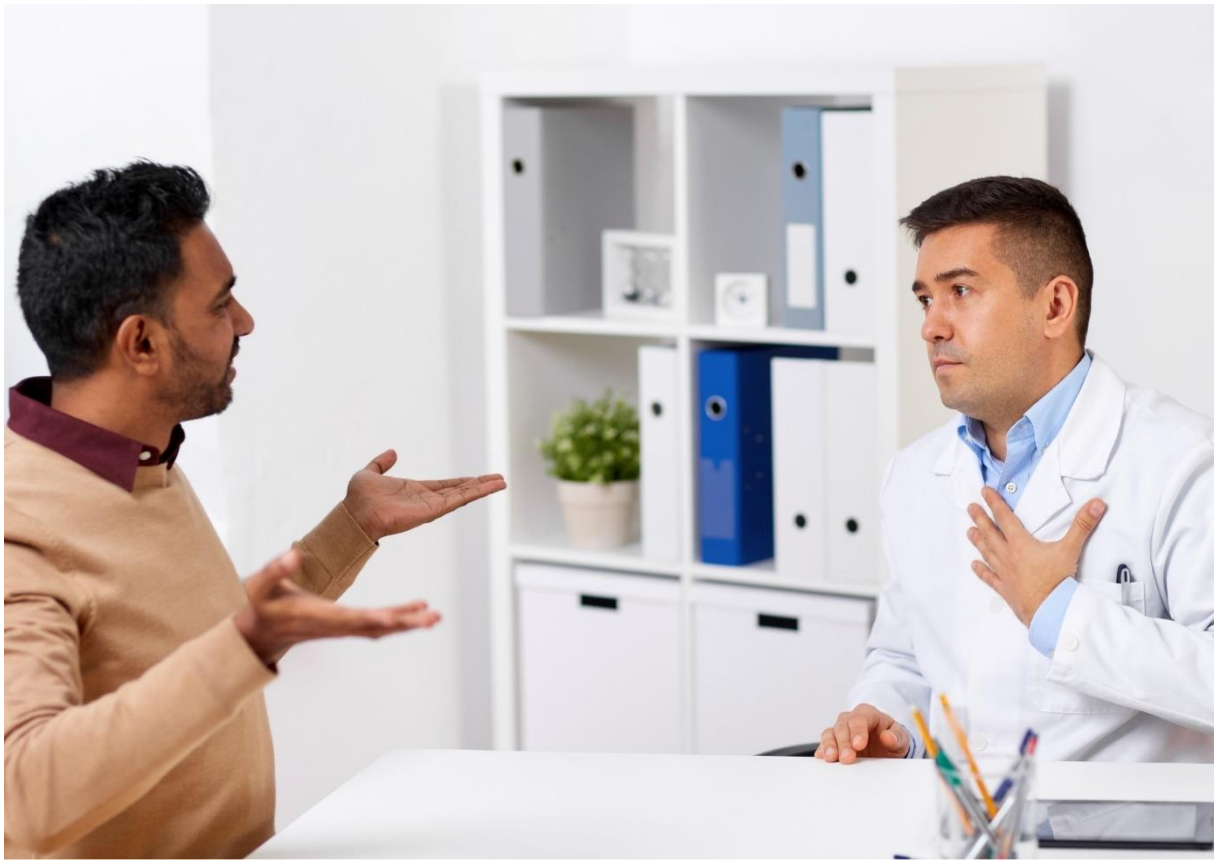
L'établissement jugé responsable

Aussi, les Juges ont estimé que l'établissement de santé n'avait pas mis en œuvre des mesures de protection suffisantes et efficaces pour prévenir ce risque. En particulier, un contrat de sécurité cynophile a été jugé « *insuffisan[t]* » et l'organisation de formation sur la gestion de la violence qualifiée de « *réponse sous-dimensionnée* ». Les juges ont également reproché à l'établissement de santé de ne pas avoir mis en place, avant l'agression, un agent de sécurité et de ne pas avoir fermé le service concerné par des portes coulissantes – et ce, indépendamment du point de savoir si ces éléments auraient, en réalité, empêché l'agression.

L'établissement de santé a ainsi été condamné à supporter le montant des préjudices effectivement subis par la médecin urgentiste.

Cette décision de justice, au-delà de l'actualité, invite les établissements de santé, employant des professionnels de santé, à redoubler de vigilance dans la prévention de la sécurité de ces derniers. Un audit de la politique de sécurité, au regard de la situation propre à chaque établissement de santé, s'impose donc…

Source : ici



IA ET SANTÉ : VERS UNE LIBÉRATION DES DONNÉES POUR FACILITER L'INNOVATION ET LA RECHERCHE

VU DANS LA PRESSE

La Veille Acteurs de Santé, avril 2024

La Commission de l'intelligence artificielle pour « contribuer à faire de la France un pays à la pointe de la révolution de l'IA » a remis son rapport le 13 mars dernier. Elle formule 25 recommandations pour que la France puisse tirer parti de la révolution technologique de l'IA. La recherche dans le secteur de la santé est ciblée, avec un enjeu majeur : les données de santé. La question de l'équilibre entre protection des données personnelles et libération au profit de l'innovation revient une nouvelle fois au cœur du débat. Retour sur ce rapport tant attendu dont on attend désormais les suites.

La Commission de l'intelligence artificielle pour « *contribuer à faire de la France un pays à la pointe de la révolution de l'IA* » a été installé en septembre 2023 par le Gouvernement. Son rapport part d'un constat largement partagé et aujourd'hui devenu banal à savoir que l'IA est un défi majeur pour l'avenir de l'Europe et la France. Il rappelle que l'IA est une révolution technologique incontournable qui affecte absolument tous les domaines d'activité. Il adopte un scénario raisonnable sur l'impact attendu, en soulignant que l'IA ne doit susciter ni excès de pessimisme, ni excès d'optimisme (« *Nous n'anticipons ni chômage de masse, ni accélération automatique de la croissance* »).

Toutefois, la Commission estime que la France comme l'Europe doivent relever le défi de l'IA, « *faute de quoi nous n'aurons pas la maîtrise de notre avenir* ». Un défi que la France tout comme l'Europe peuvent relever, la Commission estimant que nous disposons des atouts pour le faire. Mais il n'y a pas de temps à perdre.

Pour cela, le rapport dégage six grandes lignes d'actions :

1) Lancer immédiatement un plan de sensibilisation et de formation de la nation ;

2) Réorienter structurellement l'épargne vers l'innovation et créer, à court terme, un fonds « France & IA » de 10 Md euros ;

3) Faire de la France un pôle majeur de la puissance de calcul ;

4) Faciliter l'accès aux données ;

5) Assumer le principe d'une « exception IA » dans la recherche publique ; et

6) Promouvoir une gouvernance mondiale de l'IA.

Le développement de l'IA dans la santé passe par la libération des données

Le rapport identifie clairement la **Santé** comme l'un des domaines d'avenir clé pour le développement de l'IA.

Premier constat : l'IA permet d'appréhender un volume considérable de données disponibles, que l'intelligence humaine ne peut pas traiter. « *Plus de 5 millions d'articles scientifiques sont publiés chaque année, dont la moitié dans le seul domaine de la recherche médicale, indique la Commission. Il est évidemment impossible qu'un chercheur ou une équipe de chercheurs, même de haute volée, puisse les lire, et encore moins les évaluer et les analyser.* »

Deuxième constat : les données constituent un ingrédient indispensable aux développements récents de l'intelligence artificielle. Et si ces données ne sont pas nécessairement personnelles, force est de constater que nombre d'entre elles ont un caractère personnel. « *Exploiter le potentiel de l'intelligence artificielle et permettre son déploiement au service de l'humain exige par conséquent que les chercheurs, les développeurs et les innovateurs disposent d'un accès à des données massives, fiables, aisément manipulables et dont la représentativité et la qualité peuvent être évaluées* » souligne la Commission.

Dans un contexte d'évolution technologique rapide et de concurrence accrue, cet accès doit en outre pouvoir leur être ouvert rapidement et les données être utilisées sans contraintes excessives, au risque de favoriser davantage encore les acteurs en place ou de voir d'autres s'approprier nos recherches et nos innovations, en nous devançant dans leur expérimentation et leur diffusion. »

Troisième constat : l'accès aux données est souvent compliqué et les contraintes sont considérées comme excessives par les acteurs de l'IA, quels qu'ils soient (entreprises, chercheurs, laboratoires, institutions publiques et privées, associations).

Des contraintes règlementaires à lever pour l'accès aux données

Selon la Commission, les contraintes sont de deux ordres. Tout d'abord, certaines règles et pratiques françaises sont plus contraignantes que le cadre européen en matière de traitement de données personnelles.

Si le RGPD a, avec les principes de liberté et de responsabilité, renversé complètement la logique du droit qui prévalait en France depuis la loi « Informatique et Libertés » du 6 janvier 1978 (en application de laquelle les traitements des données à caractère personnel reposaient sur des procédures d'autorisation ou de déclaration préalables auprès de la CNIL), les contraintes sont encore trop fortes dans le secteur dans la santé.

« Il demeure des procédures d'autorisation préalables non prévues par le droit européen », regrette la Commission. « *C'est en particulier le cas pour l'accès aux données de santé pour la recherche. Une procédure simplifiée de déclaration de conformité à des méthodologies de référence existe mais elle est loin d'être généralisée. En pratique, la procédure simplifiée reste l'exception par rapport à la procédure d'autorisation préalable car le moindre écart par rapport à ces méthodologies implique d'en passer par une autorisation préalable qui peut impliquer jusqu'à trois niveaux d'autorisation préalable*. »

Ensuite, la Commission relève « *un décalage croissant entre la logique centrée sur la protection de l'individu et l'évolution des modes d'utilisation collective des données* ». Selon la Commission, plusieurs notions clés du RGPD sont peu adaptées face au fonctionnement de l'IA :

- La notion de « responsable du traitement », « *pour laquelle la répartition des responsabilités entre le développeur qui a procédé à l'entraînement d'une IA générative et qui la met à disposition de tiers et l'utilisateur final du système pour ses propres besoins n'apparaît pas forcément aller de soi* » ;

- La notion de « finalité du traitement », « *qui conditionne la nature des données pouvant légalement être utilisées et sur laquelle porte le consentement des personnes concernées est également plus complexe à appréhender, eu égard aux nombreuses utilisations possibles d'une IA générative une fois celle-ci entraînée* » ;
- La notion même de « donnée personnelle », « *qui constitue la clé d'application du RGPD, suscite des interrogations dans un contexte croissant d'utilisation de données collectives* ».

Même l'anonymisation des données personnelles qui permet de « *sortir* » du régime de protection des données personnelles du RGPD, ne semble pas adaptée car *« la technologie ouvre de plus en plus loin des possibilités de réidentification de données anonymisées* ».

Vers une réforme de la loi « Informatique et Libertés » ?

La Commission recommande « de supprimer des procédures d'autorisation préalable d'accès aux données de santé et de réduire les délais de réponse de la CNIL ». Elle ajoute que cette évolution devrait s'accompagner d'une réforme du mandat confié à la CNIL, pour y intégrer un « objectif d'innovation ». Elle termine en suggérant l'idée d'une « gouvernance collective » de la donnée qui pourrait poser « *les jalons d'une évolution du cadre juridique qui prendrait mieux en considération l'évolution des modes d'utilisation des données.* » Reste maintenant à connaître le plan que le gouvernement souhaite mettre en place sur la base de ce rapport…

Source : ici

QUELLES DÉMARCHES CNIL POUR QUELLE MODIFICATION DU TRAITEMENT DE DONNÉES DE SANTÉ ?

VU DANS LA PRESSE

DSIH, juin 2024

Nul n'ignore que certains traitements de données de santé doivent faire l'objet, avant leur mise en œuvre, d'une formalité CNIL. Mais saviez-vous qu'une modification d'un traitement, ayant fait l'objet d'une telle formalité, peut justifier une nouvelle formalité ? C'est ce que vient de nous préciser la CNIL dans un communiqué publié le 13 juin dernier.

Quelles formalités initiales ?

Pour connaître la formalité auquel un traitement de données santé est soumis, il convient de se reporter à la loi Informatique et Libertés.

Les formalités sont de deux ordres : soit le traitement répond aux exigences d'un référentiel établi par la CNIL, et, dans ce cas, un engagement de conformité suffit ; soit le traitement n'y répond pas ou ne peut être rattaché à aucun référentiel, et, dans ce cas, une demande d'autorisation s'impose.

Quelles modifications peuvent justifier une nouvelle formalité ?

Selon la CNIL, seule une modification « substantielle » – par opposition à la modification « non-substantielle » – du traitement doit faire l'objet d'une nouvelle démarche.

Afin de guider les responsables du traitement dans leurs démarches, la CNIL a proposé un tableau recensant les modifications les plus fréquentes.

Voici un extrait :

Thème	Modification « *substantielle* »	Modification « *non-substantielle* »
Responsable du traitement	Changement d'identité du responsable du traitement / Ajout d'un responsable conjoint du traitement	
Destinataires	Nouvelle catégorie : partenaire industriel, académique, etc.	Changement de personnes physiques accédant aux données (chez le sous-traitant, chez le promoteur, etc.)
Finalité	Nouvelle finalité	Précisions sur la finalité
Nature des données	Nouvelle catégorie de données	Nouvelles données dans des catégories existantes
Personnes concernées	Nouvelle catégorie de personnes concernées / Augmentation conséquentes du nombre	Ajustement des critères d'inclusion / Augmentation non conséquente du nombre d'inclusions
Durée (collecte, traitement, conservation, archivage)	Allongement conséquent	Mise à jour du calendrier de l'étude / Allongement négligeable
Sécurité	Modification des mesures avec un affaiblissement de la sécurité	Modification des mesures sans affaiblissement de la sécurité
Transferts de données hors UE	Encadrement du transfert autrement que par une décision d'adéquation ou des garanties appropriées	

Quelle nouvelle formalité en cas de modification substantielle ?

Si le traitement avait été mis en œuvre dans le cadre d'engagement de conformité à un référentiel et que la modification « substantielle » n'affecte pas la conformité du traitement à ce référentiel, aucune démarche CNIL n'est nécessaire. En revanche, la modification « substantielle » affecte la conformité du traitement à ce référentiel, une demande d'autorisation auprès de la CNIL s'impose.

Si le traitement avait été mis en œuvre après une autorisation de la CNIL et que la modification « substantielle » rend le traitement conforme au référentiel dédié à ce type de traitement, un engagement de conformité suffit. En revanche, la modification « substantielle » ne rend pas le traitement conforme à ce référentiel, une demande de modification de l'autorisation auprès de la CNIL s'impose.

A vous de jouer !

Source : ici

DOCTRINE

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

EN BREF

LOI SREN

Quelles implications dans le domaine de la santé ?

La loi visant à « sécuriser et réguler l'espace numérique » dite loi « SREN », du 21 mai dernier, concerne aussi le domaine de la santé.

Elle traite, en particulier, la question de la souveraineté en matière de données de santé.

En effet :

- La loi modifie la lettre de l'article L.1111-8 du Code de la santé publique, notamment pour ajouter l'obligation des hébergeurs de données de santé de stocker les données dans l'UE ou l'EEE dans des conditions décrites par décret (en l'occurrence par le « nouveau référentiel HDS » adopté par arrêté du 26 avril 2024) ;
- La loi impose, par principe, aux administrations de l'Etat, à certains de ses opérateurs et groupements d'intérêt public, de veiller à ce que les services informatiques en nuage, fournis par un prestataire privé et utilisés dans le cadre leurs systèmes ou de leurs applications informatiques, « mettent en œuvre des critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'Etats tiers non autorisé par le droit de l'Union européenne ou d'un Etat membre ».
- Une telle exigence est requise (i) en cas de traitement de données « d'une sensibilité particulière » (dont les données nécessaires à des missions essentielles de l'Etat, notamment la protection de la santé et de la vie des personnes) et (ii) si la violation de telles données est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle.