NEWSLETTER E-SANTE

NUMÉRO 10 ● 2024

ÉQUIPE

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocat counsel

SOMMAIRE

EST-IL POSSIBLE DE RECOURIR A UNE PLATEFORME DE MISE EN RELATION POUR VENDRE EN LIGNE DES MEDICAMENTS ?

Alors que les plateformes de mise en relation ne cessent de fleurir et ce, dans de nombreux domaines, le secteur pharmaceutique n'a pas échappé à cette tendance. Compte tenu de la règlementation stricte applicable à la vente de médicaments, la licéité du recours à de telles plateformes pour ce type de vente interroge. En particulier, une telle pratique est-elle compatible avec l'interdiction de la vente en ligne de médicaments non soumis à prescription médicale par une personne n'ayant pas la qualité de pharmacien ?

La Cour de Justice de l'Union européenne (CJUE) a récemment jugé que la licéité d'une telle pratique dépend du degré d'implication de la plateforme de mise en relation dans le processus de vente des médicaments (arrêt du 29 février 2024, affaire C-606/21).

En l'occurrence, l'affaire concernait le site internet Doctipharma (devenue DocMorris) qui mettait en relation des pharmaciens et des patients potentiels pour l'achat de médicaments non soumis à prescription médicale. La particularité de Doctipharma résidait dans le fait que l'achat des médicaments était réalisé à partir des sites internet des pharmacies partenaires, créés et hébergés via Doctipharma.

Considérant que le site litigieux reviendrait à faire participer Doctipharma au commerce électronique de médicaments, sans avoir la qualité de pharmacien, et donc en violation des dispositions du Code de la santé publique (article L.5125-25 et -26), l'Union des groupements de pharmaciens d'officine a porté l'affaire en justice.

Que retenir de la position de la CJUE ?

La CJUE a d'abord qualifié la plateforme de Doctipharma de « service de la société de l'information » au sens du droit de l'Union, c'est-à-dire un « *service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* ». A cet égard, les juges européens ont notamment relevé que « ce service est presté, d'une part, à la demande individuelle des pharmaciens, ceux-ci devant souscrire au site Internet de Doctipharma pour pouvoir bénéficier dudit service, et, d'autre part, à la demande individuelle des clients, ceux-ci devant créer un compte client pour pouvoir accéder aux sites des pharmaciens de leur choix en vue d'acheter, sur commande, des médicaments non soumis à prescription médicale ». Aussi, pour la CJUE, la vente à distance de tels médicaments via un service de la société de l'information doit pouvoir, par principe, être autorisée. La CJUE a ensuite indiqué qu'il fallait s'intéresser au rôle joué par la plateforme dans le cadre de la vente de médicaments non soumis à prescription médicale.

De deux choses l'une :

- Soit la plateforme (ne possédant pas la qualité de pharmacien) procède elle-même à la vente des médicaments non soumis à prescription, ce qui peut justifier l'interdiction d'une telle pratique ;

- Soit la plateforme se borne, par une prestation propre et distincte de la vente, à mettre en relation des pharmaciens et des patients potentiels, pratique qui ne peut être interdite « *au motif [que la plateforme participe] au commerce électronique de vente de médicaments sans avoir la qualité de pharmacien* ».

Cette solution nous donne ainsi des éclairages précieux pour apprécier la licéité du recours à une plateforme de mise en relation pour la vente en ligne de médicaments non soumis à prescription médicale : (i) le recours à des plateformes agissant comme simples intermédiaires, ne procédant pas elles-mêmes à la vente serait licite, (ii) tandis que le recours à des plateformes effectuant elles-mêmes la vente en ligne serait illicite. La décision de la Cour d'appel de Paris permettra d'aller encore plus loin en appréhendant, factuellement, les critères qui pourront justifier précisément ce rôle joué par la plateforme, de simple intermédiaire versus celui de vendeur (par exemple : l'existence ou non de moyens de contrôle des ventes par la plateforme, la mise à disposition d'une solution de paiement, etc.). A suivre…

Source : ici

LES ETABLISSEMENTS DE SANTE DANS LE COLLIMATEUR DE LA CNIL

VU DANS LA PRESSE

« DSIH » 14 FEVRIER 2024

La CNIL a diligenté treize contrôles entre 2020 et 2024 auprès d'établissements de santé. Résultat : les mesures mises en œuvre par ces derniers pour garantir la sécurité du dossier patient informatisé (DPI) sont insuffisantes. Plusieurs d'entre eux ont fait l'objet de mise en demeure de prendre des mesures adaptées. La CNIL prévoit des mesures correctrices contre d'autres établissements en 2024. Nos avocats en droit des données personnelles vous éclairent.

La sensibilité du dossier patient informatisé (DPI)

Le dossier patient informatisé (DPI) est le fichier dans lequel est centralisé l'ensemble des données de santé des patients pris en charge au sein d'un établissement de santé. Il permet aux professionnels de santé de cet établissement d'accéder facilement à leurs informations médicales.

Compte tenu du volume et de la sensibilité des données qu'il contient, le DPI doit, selon la CNIL, faire l'objet de « mesures de sécurité renforcées ».

Des mesures de sécurité souvent inadaptées

Les mesures prises par les établissements de santé concernés ne sont pas satisfaisantes car la politique de gestion des habilitations est trop souvent inadaptée, en ce qu'elle permet notamment à des catégories de personnel desdits établissements de santé d'accéder à des données dont elles n'ont pas besoin de connaître.

Les mesures de sécurité préconisées par la CNIL

Les établissements de santé devraient, selon la CNIL, mettre en place les trois mesures suivantes :

- Sécuriser les accès au DPI grâce à une politique d'authentification robuste, qui devrait prévoir a minima (i) un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs et (ii) le recours à des mots de passe suffisamment complexes.

- Implémenter des règles d'habilitation répondant à l'exigence selon laquelle un professionnel de santé ou un agent ne peut accéder qu'aux données dont il a besoin de connaître.
  Selon la CNIL, cette deuxième mesure passe par le respect des deux critères suivants :

  - 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* » ;

  - Le critère de l'« équipe de soins » (telle que définie par la loi (art. 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* ».

- Implémenter un dispositif de journalisation permettant de tracer les accès au DPI : « *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.* »

La CNIL prévoit de poursuivre ses contrôles en 2024.

A suivre…

Source : ici

EHDS, OÙ EN EST-ON ? RETOUR SUR LES DERNIERS AMENDEMENTS PROPOSES PAR LE PARLEMENT EUROPEEN

VU DANS LA PRESSE

« DSIH » 6 FEVRIER 2024

Pour mémoire, la Commission européenne avait présenté le 3 mai 2022 une proposition de règlement européen sur l'espace européen des données de santé (European Health Data Space ou « EHDS »). Le 13 décembre dernier, le Parlement européen a pris position sur ce texte novateur, considéré comme une « pierre angulaire » dans la construction d'une Union européenne de la santé forte. Nos avocats en droit des données personnelles vous offrent leur expertise.

Ce texte prévoit la mise en place de mesures propres au secteur de la santé afin de permettre le déploiement d'un espace européen commun des données dans ce domaine. La proposition de règlement sur l'EHDS a principalement pour objectif de répondre au challenge de l'accès et du partage des données de santé dans toute l'UE. Plus précisément, l 'EHDS vise à répondre à un constat global de difficultés rencontrées tant par les citoyens/patients que par les professionnels de santé, les autorités ainsi que les chercheurs, les organismes et les entreprises de l'UE, en termes de soins et d'innovations sanitaires.

Cette proposition contient notamment deux grandes séries de règles : (i) l'une portant sur l'utilisation dite primaire des données de santé électroniques et (ii) l'autre concernant l'utilisation dite secondaire des données de santé électroniques

L'utilisation primaire des données de santé électroniques

Concrètement, il s'agit pour les patients européens de bénéficier d'un droit d'accès à leurs données de santé électroniques dans les différents services de santé de l'UE et ce, de façon simplifiée, immédiate et gratuite dans un format facilement lisible, consolidé et accessible.

Parallèlement les professionnels de santé auront le droit d'accéder aux données de santé électroniques de leurs patients lorsqu'ils sont nécessaires à un traitement spécifique. Dans ce cadre, « *l'accès aux dossiers des patients, aux ordonnances électroniques, aux images médicales et aux résultats de laboratoire sera possible* ».

Des règles « techniques » sont prévues à cette fin, notamment en termes de qualité et de sécurité des données de santé électroniques avec contrôle par des autorités nationales.

Des services d'accès aux données de santé électronique seront mis en place, par Etat membre, sur une plateforme dédiée « MyHealth@EU ».

Le Parlement européen a notamment proposé que les patients puissent savoir quels professionnels de santé ont accédé à leurs données de santé électroniques et à quel moment, par le biais d'un système de notification automatique (pouvant être désactivé). Le Parlement a également suggéré la possibilité pour le patient concerné d'empêcher l'accès à ses données de santé électroniques « *à toute personne autre que le professionnel de la santé qui a inséré les données électroniques de santé* »

L'utilisation secondaire des données de santé électroniques

Il s'agit pour les chercheurs, les innovateurs, les autorités publiques de pouvoir utiliser certaines données de santé électroniques, dans certaines conditions strictes, « *pour des raisons d'intérêt commun comme la recherche, l'innovation, l'élaboration des politiques, l'éducation, et la sécurité des patients* ». Cela concernera, en particulier, les données agrégées « *sur les agents pathogènes, les allégations de santé et les remboursements, les données génétiques et les informations du registre de santé publique* ».

Le projet de texte liste les finalités pouvant être poursuivies pour l'utilisation secondaire, parmi lesquelles, souligne le Parlement européen, la mise au point de nouveaux médicaments et d'autres produits et services de santé. Des finalités interdites pour l'utilisation secondaire des données de santé sont également indiquées telles que la publicité ou encore l'évaluation des demandes d'assurance, mais également, ainsi que le suggère le Parlement européen, sur le marché du travail ou dans les secteurs financiers.

Les parlementaires européens souhaitent, par ailleurs, que les patients aient davantage de contrôle sur leurs données de santé électroniques, objet de l'utilisation secondaire. Leur proposition est (i) la mise en place d'un mécanisme d'opposition facilement accessible et compréhensible (« opt-out ») pour l'utilisation secondaire de la majorité de leurs données de santé électroniques et (ii) le recueil du consentement explicite (« opt-in ») du patient concerné pour l'utilisation secondaire de certaines données de santé électroniques dites sensibles (informations génétiques et génomiques, etc.).

Enfin, le Parlement a insisté sur la nécessité d'une mise en place de mesures nécessaires pour assurer la confidentialité des droits de propriété intellectuelle et la protection des secrets d'affaires dans le cadre d'une telle utilisation secondaire.

A suivre…

Source : ici

QUAND L'ETHIQUE S'INVITE DANS LES SERVICES NUMERIQUES DE SANTE INTEGRANT L'IA

VU DANS LA PRESSE
« DSIH » 4 MARS 2024

L'Agence du Numérique en Santé (ANS) vient de publier un référentiel éthique pour les services numériques de santé intégrant l'IA. Ce référentiel s'adresse aux éditeurs-fournisseurs d'un SI embarquant un module d'IA, mais aussi aux professionnels de santé et aux patients utilisateurs.

Ce référentiel s'inscrit dans le « Cadre de l'Ethique en Santé » (« CENS »), qui un corpus documentaire lancé en 2023 par la DNS et l'ANS, avec pour objectif de promouvoir et d'encadrer l'éthique des solutions et services numériques en santé. Nos avocats en droit des données personnelles vous éclairent.

Ce référentiel repose sur les 5 principes suivants :

- La bienfaisance où la garantie de transparence donnée aux utilisateurs quant à l'utilisation d'une solution IA ;
- La non-malfaisance ou la garantie à un traitement approprié et pertinent des données ;
- L'autonomie ou la garantie donnée aux utilisateurs quant au recours à une solution IA et à leur pouvoir décision sur sa désactivation ;
- La justice et l'équité ou la garantie donnée pour une performance identique de l'IA pour tous les publics (en évitant les biais algorithmiques) ;
- Le développement durable ou l'engagement des éditeurs dans une démarche (i) d'évaluation de l'impact environnemental de leurs solutions et (ii) d'amélioration continue.

32 critères, élaborés à partir de ces principes, composent ce référentiel.

Parmi ces critères, on peut noter :

- Les professionnels de santé utilisateurs d'un SI de santé doivent bénéficier d'une formation à l'utilisation de l'IA en amont de son introduction ;

- Les utilisateurs – professionnels de santé et patients – d'une solution d'IA sont informés qu'ils interagissent avec une IA et le fournisseur met en œuvre des mécanismes permettant de s'assurer de leur bonne compréhension ;

- Lorsqu'un professionnel de santé construit sa décision (diagnostique/thérapeutique) en suivant les propositions d'une IA, il doit informer les patients de l'usage de l'IA et du fait qu'il a suivi les propositions faites par l'IA ;

- Lorsqu'un professionnel de santé construit sa décision (diagnostique/thérapeutique) en utilisant une IA, mais sans suivre les propositions d'une IA, il doit informer les patients de l'usage de l'IA et du fait qu'il n'a pas suivi les propositions faites par l'IA ;

- Tout module d'IA doit proposer une interface intuitive permettant à l'utilisateur -professionnel de santé ou patient – de comprendre l'origine de la proposition de l'IA ;

- Les interfaces d'un SI de santé intégrant un module d'IA doivent mettre en évidence les résultats qui ont été produits par l'IA ;

- Le fournisseur d'un module d'IA utilise des données anonymisées comme données d'apprentissage. Si l'anonymisation n'a pas été possible, et qu'il dispose de données pseudonymisées, il doit s'assurer que les patients ont consenti à la réutilisation secondaire de leurs données de santé à des fins d'apprentissage pour des solutions d'IA ;
- Le fournisseur d'un module d'IA met en œuvre des mécanismes lui permettant de minimiser le recueil des données utilisées pour l'entraînement de l'algorithme, la protection et l'exploitation du module d'IA, aux seules données nécessaires et suffisantes pour tenir compte de la singularité des patients qui constituent la cible d'usage du module d'IA.

Ce corpus documentaire a vocation à être opposable. En effet, l'article L.1470-5 du Code de la santé publique consacre l'opposabilité des référentiels éthiques du CENS au même titre que les référentiels de sécurité (PGSSI-S) et d'interopérabilité (CI-SIS). A suivre…

Source : ici

SECURITE DES DOSSIERS PATIENT INFORMATISES : LA CNIL MET LA PRESSION SUR LES ETABLISSEMENTS DE SANTE

VU DANS LA PRESSE

LA VEILLE ACTEURS DE SANTE
4 MARS 2024

Dans une communication récente, la CNIL a mis en avant l'insuffisance des mesures mises en œuvre par les établissements de santé visant à garantir la sécurité de leurs dossiers patients informatisés (DPI). Le grief principal est le suivant : trop de personnel au sein de ces organismes aurait accès aux données de santé des patients. Les enjeux éthiques et juridiques sont énormes. Des mesures d'amélioration sont proposées par la CNIL, valables pour toutes les structures de soins où de nombreuses personnes ont accès aux dossiers des patients. Nos avocats en droit de la e-santé vous éclairent.

La sensibilité du dossier patient informatisé (DPI)

Le dossier patient informatisé (DPI), fichier dans lequel est centralisé l'ensemble des données de santé des patients pris en charge par l'établissement de santé ou toute structure de soins, permet aux professionnels de santé de ce lieu d'exercice d'accéder facilement à leurs informations médicales.

Compte tenu du volume et de la sensibilité des données qu'il contient, le DPI doit, selon la CNIL, faire l'objet de *« mesures de sécurité renforcées* » . Mais, force est de constater que ces mesures sont bien souvent insuffisantes, ne serait-ce qu'en raison de l'application d'une politique de gestion des habilitations inadaptée, permettant notamment à des catégories de personnels d'accéder à des données qu'elles n'ont pas besoin de connaître.

Les mesures de sécurité préconisées par la CNIL

Afin de renforcer la sécurité du dossier patient informatisé, la CNIL préconise le choix de règles répondant à l'exigence selon laquelle un professionnel de santé ou un agent/personnel ne peut accéder qu'aux données qu'il a strictement besoin de connaître.

Dans la définition de ces règles, deux critères peuvent être retenus :

- Le critère du « métier exercé », qui signifie qu'un agent/personnel 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 ou un professionnel de santé pourra, bien entendu, accéder au dossier administratif mais « également aux données médicales » ;

- Le critère de l'équipe de soins [telle que définie par la loi (art. L.1110-12 du Code de la santé publique)], qui signifie que 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.

Consciente des enjeux et des nécessités du métier et des situations d'urgence dans lesquelles se trouve confronté le personnel de ces établissements, la CNIL précise toutefois que les habilitations accordées peuvent être complétées d'un « mode bris de glace », afin de permettre aux agents/personnels administratifs et professionnels de santé d'avoir accès à d'autres données pour tout patient.

D'autres mesures peuvent venir compléter cet arsenal, comme la mise en place d'une politique d'authentification robuste, qui devrait prévoir a minima :

- un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs
- le recours à des mots de passe suffisamment complexes.

L'implémentation d'un dispositif de journalisation permettant de tracer les accès au DPI est également recommandée par la CNIL : « *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.* »

Les enjeux

D'un point de vue éthique, les enjeux sont tout aussi importants. Le respect de la sécurité (et notamment de la confidentialité des données de santé) doit être au centre des préoccupations des professionnels de santé, en vue notamment de garder un haut niveau de confiance entre eux et leurs patients.

D'un point de vue juridique, les enjeux sont énormes. En application du RGPD, la sanction encourue, en cas de manquement à l'obligation de sécurité, est de 2% du chiffre d'affaires annuel mondial. D'ailleurs, dans une affaire récente, l'autorité espagnole de protection des données n'a pas hésité à sanctionner un hôpital qui n'avait pas mis en place les mesures permettant de limiter l'accès au dossier clinique aux seuls professionnels de santé ayant besoin d'en connaître (AEPD, décision n°PS/00587/2021).

En France, à la suite des contrôles réalisés depuis 2020, plusieurs établissements de santé ont fait l'objet de mise en demeure de prendre des mesures adaptées. La CNIL prévoit, pour 2024, des mesures correctrices contre d'autres établissements disposant de DPI.

A suivre…

Source : ici

IA ET SANTE : VERS UNE REFORME DE LA LOI « INFORMATIQUE ET LIBERTES » POUR FACILITER L'INNOVATION ET LA RECHERCHE ?

VU DANS LA PRESSE
DSIH

18 MARS 2024

La Commission de l'IA (Intelligence artificielle) préconise la suppression des procédures d'autorisation préalable d'accès aux données de santé et la réduction des délais de réponse de la CNIL. Retour sur ce rapport tant attendu, qui a été présenté mercredi dernier au Président Emmanuel Macron.

Le rapport de la Commission de l'intelligence artificielle, en quelques mots

En septembre dernier, le Gouvernement a installé la Commission de l'intelligence artificielle pour « contribuer à faire de la France un pays à la pointe de la révolution de l'IA ». La Commission a remis, mercredi 13 mars 2024, son rapport au Président Emmanuel Macron. Ce rapport contient 25 recommandations pour que la France puisse tirer partie de la révolution technologique de l'IA. La recherche dans le secteur de la santé est au cœur des réflexions. La question de la protection des données personnelles l'est également.

En synthèse, il ressort du rapport que :

- L'IA est une révolution technologique incontournable ;
- Cette révolution technologique affecte tous les domaines d'activité ;
- 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 ») ;
- L'Europe et la France ont des atouts pour être des acteurs de cette révolution ;
- L'Europe et la France doivent relever le défi de l'IA, « *faute de quoi nous n'aurons pas la maîtrise de notre avenir* »

Afin de gagner le défi de l'IA, la Commission propose six grandes lignes d'actions :

- Lancer immédiatement un plan de sensibilisation et de formation de la nation ;
- Réorienter structurellement l'épargne vers l'innovation et créer, à court terme, un fonds « France & IA » de 10 Md euros ;
- Faire de la France un pôle majeur de la puissance de calcul ;
- Faciliter l'accès aux données ;
- Assumer le principe d'une « exception IA » dans la recherche publique ; et
- Promouvoir une gouvernance mondiale de l'IA.

L'accès aux données, le défi 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).

Les contraintes règlementaires

Les contraintes sont de deux ordres.

Tout d'abord, la Commission considère que 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 de 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 estime qu'il existe « *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* ».

Quelles solutions ?

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*. »

Affaire à suivre…

Source : ici

ENTREPOTS DE DONNEES DE SANTE ET CLOUD NON-SOUVERAIN SONT-ILS COMPATIBLES ?

Le Health Data Hub, « chargé par la loi de recueillir les bases de données de santé les plus importants du pays , a conclu un contrat de services avec l'Agence européenne des médicaments (EMA). C'est dans ce cadre qu'intervient le projet EMC2" afin, en particulier, d'observer et évaluer la prise en charge des patients , d' évaluer l'utilisation et/ou les pratiques, l'efficacité et la sécurité en vie réelle des produits de santé, en particulier les médicaments et les dispositifs médicaux inscrits au remboursement ou en accès précoce .

Aussi, ce projet porte sur la création d'un entrepôt de données de santé pour des analyses pharmatico-épidémiologiques. « *Un appariement entre les données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par les établissements de santé partenaires* » y est prévu.

Le Health Data Hub a saisi la CNIL d'une demande d'autorisation pour mettre en œuvre cet entrepôt de données de santé. A noter, effectivement, qu'un entrepôt de données de santé « *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* », tel que le projet « EMC2 », doit être conforme au référentiel CNIL relatif « *aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé* » , pour pouvoir être mis en œuvre par l'organisme, responsable de traitement, concerné.

En cas de conformité, une déclaration de conformité auprès de la CNIL suffit. A défaut, une autorisation spécifique préalable de la CNIL doit être obtenue.

En l'occurrence, le projet « EMC2 » ne répondait pas à toutes les exigences prévues dans ledit référentiel et nécessitait donc une autorisation.

La possibilité d'hébergement temporaire sur un cloud non-souverain, faute de mieux

Le projet « EMC2 » prévoyait de recourir à l'hébergeur Microsoft Ireland Ltd (avec la solution Microsoft Azure), dont la maison mère est située au Etats-Unis. La question des ingérences extraterritoriales se pose.

Certes, la Commission européenne a reconnu que le cadre de transfert des données « Etats-Unis/UE » assure un niveau de protection adéquat (décision d'adéquation du 10 juillet 2023). Pour autant, selon la CNIL, le risque d'accès aux données hébergées chez Microsoft par les autorités américaines demeure.

Ainsi, « *pour les bases de données les plus sensibles* », telles que les bases de données de santé, la CNIL recommande de recourir à un hébergeur exclusivement soumis droit européen et certifié « SecNumClou ». Les entrepôts de données de santé appariées avec le SNDS font d'autant plus l'objet d'une vigilance particulière, « *malgré le fait que le ces données soient pseudonymisées* », dans la mesure où « *la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ».

La circulaire de la Première Ministre du 31 mars 2023 demande effectivement, rappelle la CNIL, que les autorités publiques s'assurent que « *les données 'd'une sensibilité particulière' hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». Ainsi, le choix du Health Data Hub « *apparaît en très nette contradiction avec [ces] éléments* » .

On aurait alors pu s'attendre à un refus de la CNIL d'autoriser l'entrepôt de données de santé « EMC2 », hébergé chez Microsoft.

Mais, après avoir notamment déplor[é] qu'aucun prestataire susceptible de répondre actuellement aux besoins exprimés par le [Health Data Hub] ne protège les données contre l'application de lois extraterritoriales de pays tiers « , *la CNIL a décidé d'autoriser la mise en œuvre de l'entrepôt de données de santé « EMC2* » avec un hébergement chez Microsoft pour une durée de 3 ans.

Il faut savoir que, pour répondre aux demandes de la CNIL, une expertise, pilotée par la délégation numérique en santé (DNS), la direction interministérielle du numérique (DINUM) et l'Agence Numérique en santé, avait été réalisée « *aux fins de déterminer si le projet EMC2 pouvait, sans compromettre le projet vis-à-vis des conditions fixées par [l'Agence européenne du médicament], être mis en œuvre via un prestataire soumis uniquement aux lois de l'Union européenne* » .

Le rapport d'expertise, établi dans des délais relativement courts, avait répondu par la négative.

Un sujet au cœur des débats et une position du Conseil d'Etat à venir

Cette position de la CNIL donne lieu à d'importants débats.

En particulier, cette décision interroge compte tenu

- d'un côté, de la récente décision de la Commission européenne considérant que le niveau de protection de données personnelles du cadre de transfert de données UE/Etats-Unis est équivalent à celui de l'Union européenne et

- de l'autre côté, des exigences nationales en termes de souveraineté.

Des critiques se sont également élevées contre la CNIL dans la mesure où elle reconnaît le non-respect du projet « EMC2 » aux exigences nationales de souveraineté tout en validant ce projet, tandis que d'autres projets similaires hébergés par Microsoft auraient déjà été refusés par la CNIL.

La position du Conseil d'Etat, saisi dans le cadre d'un recours en annulation initié par l'Internet Society France, est ainsi particulièrement attendue. A suivre…

Source : ici

UN ENTREPOT DE DONNEES DE SANTE PEUT-IL ETRE HEBERGE PAR MICROSOFT ?

VU DANS LA PRESSE

DSIH
26 FEVRIER 2024

Rappel du cadre légal des entrepôts de données de santé

Pour mémoire, la CNIL a publié un référentiel relatif « aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé » (le « Référentiel »). Ce Référentiel concerne uniquement les entrepôts de données de santé « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ». Nos avocats en droit des données personnelles mettent leur expertise à votre service.

Ainsi, un organisme, responsable de traitement, souhaitant mettre en œuvre un entrepôt de données de santé ayant une telle finalité d'intérêt public doit, par principe, s'assurer de la conformité de son projet au Référentiel.

Dans le cas où l'organisme considère que son projet est en stricte conformité avec le Référentiel, il peut alors se contenter d'une déclaration de conformité auprès de la CNIL (Cas n°1). Dans l'hypothèse où il y aurait des écarts avec les exigences prévues au Référentiel, l'organisme doit saisir la CNIL d'une demande d'autorisation spécifique préalable (Cas n°2).

La demande d'autorisation du Health Data Hub pour « EMC2 »

Le Health Data Hub s'est trouvé dans le Cas n°2 concernant son projet d'entrepôt de données de santé « EMC2 ». Il a donc saisi la CNIL d'une demande d'autorisation.

Pour information, le projet « EMC2 », qui s'inscrit dans le cadre d'une convention de services liant le Health Data Hub à l'Agence européenne des médicaments (EMA), a pour objet la création d'une base de données afin de réaliser des études en pharmaco-épidémiologie.

Le projet « EMC2 » a, plus précisément, notamment pour objectif d'«*observer et évaluer la prise en charge des patients (…)* », d'« *évaluer l'utilisation et/ou les pratiques, l'efficacité et la sécurité en vie réelle des produits de santé, en particulier les médicaments et les dispositifs médicaux inscrits au remboursement ou en accès précoce (…)* ».

A noter que « la constitution de l'entrepôt nécessite un appariement entre les données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par les établissements de santé partenaires ».

La position de la CNIL

Dans le cadre de l'analyse du projet « EMC2 », la CNIL s'est notamment penchée sur la question du recours à la société Microsoft Ireland Operations Ltd en tant qu'hébergeur des données.

En premier lieu, la CNIL a relevé que :

- les données seront conservées dans des centres de données localisés en France ;

- seules les « données techniques d'usage de la plateforme (qui ne révèlent aucune information de santé) », feront, pour des raisons d'administration de ladite plateforme, l'objet de transferts aux Etats-Unis (transferts encadrés par les Clauses Contractuelles Types de la Commission européenne et nécessitant une information spécifique des personnes concernées).

Ensuite, la CNIL a estimé qu'il existe tout de même un risque d'accès aux données par les autorités américaines puisque la maison mère de la société Microsoft Ireland Ltd est située aux Etats-Unis (et donc soumise au droit de cet Etat). Un tel risque demeure, pour la CNIL, en dépit de la décision d'adéquation du 10 juillet 2023 (le « Data Privacy Framework ») reconnaissant que le cadre de transferts des données « Etats-Unis/UE » assure un niveau de protection adéquat.

« *Si ce risque est le plus souvent acceptable, notamment s'agissant des pays adéquats », la CNIL recommande « pour les bases de données les plus sensibles » de faire appel à un hébergeur exclusivement soumis droit européen et certifié « SecNumCloud* ». « *En particulier, pour les entrepôts de données de santé appariées avec le SNDS, et malgré le fait que ces données soient pseudonymisées, la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ». Pour la CNIL, « *cette politique apparaît en cohérence avec (…) la circulaire de la Première ministre du 31 mai 2023 (…) qui demande, sans sa règle n°9, aux autorités publiques de s'assurer que les données « d'une sensibilité particulière » hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». Ainsi, le choix du Health Data Hub, « *chargé par la loi de recueillir les bases de données de santé les plus importants du pays », « apparaît en très nette contradiction avec [ces]*

Pour répondre aux interrogations de la CNIL, les pouvoirs publics ont fait réaliser une expertise, pilotée par la délégation numérique en santé (DNS), la direction interministérielle du numérique (DINUM) et l'Agence Numérique en santé, « aux fins de déterminer si le projet EMC2 pouvait, sans compromettre le projet vis-à-vis des conditions fixées par [l'Agence européenne du médicament], être mis en œuvre via un prestataire soumis uniquement aux lois de l'Union européenne ». Le rapport d'expertise a conclu à l'absence d'offres d'hébergement répondant à de telles conditions dans les délais requis.

Après avoir (i) « *déplor[é] qu'aucun prestataire susceptible de répondre actuellement aux besoins exprimés par le [Health Data Hub] ne protège les données contre l'application de lois extraterritoriales de pays tiers* » et (ii) considéré que « le projet EMC2 aurait pu être retenu par le [Health Data Hub] pour préfigurer la solution souveraine vers laquelle il doit migrer », la CNIL a tout de même autorisé l'entrepôt de données de santé « EMC2 » pour une durée de 3 ans (durée de la migration de la plateforme). A cet égard, la CNIL a souligné « *qu'il est nécessaire que les engagements pris vis-à-vis de [l'Agence européenne du médicament] puissent être honorés* ».

En conséquence, la CNIL a validé l'hébergement de l'entrepôt de données de santé « EMC2 » par Microsoft.

Cette décision ouvre-t-elle alors la possibilité à certains entrepôts de données de santé d'être hébergés par Microsoft ou d'autres hébergeurs américains ?

Les débats associés à la décision de la CNIL

Cette décision de la CNIL a suscité et suscite encore de vifs débats.

Il en ressort notamment la difficulté de concilier, d'une part, la récente décision d'adéquation de la Commission européenne qui constate que les Etats-Unis ont un niveau de protection de données personnelles équivalent à celui de l'Union européenne et, d'autre part, les exigences nationales en matière de souveraineté. Aussi, la position de la CNIL est critiquée (i) en ce qu'elle révèle une « contradiction » du projet « EMC2 » à ces exigences de souveraineté, sans pour autant conclure à une « invalidité » de ce projet, (ii) et ce, alors que d'autres projets d'entrepôts de données de santé similaires au projet « EMC2 » hébergés sur Microsoft Azure ont été refusés par la CNIL.

Il appartient désormais au Conseil d'Etat de trancher cette épineuse question. L'Internet Society France a effectivement annoncé avoir déposé un recours en annulation de la délibération de la CNIL.

A suivre…

Source : ici

LE SECRET MEDICAL PEUT-IL ETRE LEVE POUR LES BESOINS DE LA DEFENSE ?

VU DANS LA PRESSE

DSIH
25 MARS 2024

Nombre de collaborateurs, salariés notamment dans des établissements de santé, ont accès, dans le cadre leurs fonctions, à des documents contenant des données médicales de patients. Ces informations sont protégées par le secret médical. Mais, le jour où survient un litige entre l'un de ces salariés et son employeur, ce secret médical peut-il être levé ? En d'autres termes, un salarié peut-il utiliser, comme moyen de preuve, des documents couverts par le secret médical dans le cadre d'un litige prud'homal, n'intéressant donc pas le patient concerné ?

La Chambre sociale de la Cour de cassation a récemment jugé[1] que la production de documents couverts par le secret médical est possible, sous réserve du respect de certaines conditions.

L'affaire opposait une salariée, agent comptable, à son employeur, une polyclinique. La salariée contestant sa classification et sa rémunération avait entamé un procès contre la polyclinique. Dans ce cadre, la salariée avait (i) extrait, des outils mis à sa disposition par son employeur, des documents révélant notamment les noms de patients, leurs pathologies, le nom de leur médecin traitant, la date de leur intervention chirurgicale et (ii) les avait transmis à son avocat qui les avait utilisés pour la défense de sa cliente. La polyclinique a alors licencié la salariée pour faute grave, considérant que cette dernière a violé tant ses obligations contractuelles que légales en ne respectant pas ses obligations de discrétion et de confidentialité et a porté atteinte au secret médical. La salariée soutenait, quant à elle, que les documents litigieux « *étaient strictement nécessaires à sa défense* », notamment pour démontrer les tâches qu'elle accomplissait pour son employeur et justifier, ainsi, de lui voir reconnaître la qualité de technicienne comptable.

En effet, l'article L.1110-4 alinéa 2 du Code de la santé publique prévoit que le secret médical « couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé ». Comment alors articuler la protection du secret médical, dont la portée est large, avec le principe de liberté de la preuve en matière prud'homale ?

Pour la Cour de cassation, « la production en justice de documents couverts par le secret médical ne peut être justifiée que lorsqu'elle est indispensable à l'exercice des droits de la défense et proportionnée au but poursuivi ». En l'espèce, la salariée « *n'établissait pas que l'absence d'anonymisation de ces pièces et de la suppression des données permettant l'identification des patients était, dans le cadre de l'instance en cause, indispensable pour justifier des fonctions qu'elle exerçait réellement* ».

Que peut-on en retenir ?

Compte tenu de cette dernière position de la Cour de cassation, un salarié pourrait utiliser des documents soumis au secret médical pour les besoins de sa défense dans un litige prud'homal, sous réserve de les anonymiser et/ou de supprimer les données médicales permettant d'identifier les patients concernés. Aucun garde-fou n'est cependant expressément exigé par les juges de cassation, notamment, quant aux techniques d'anonymisation à mettre en œuvre à cet égard.

Par exception, la communication intégrale desdits documents, c'est-à-dire sans anonymisation et sans suppression des données médicales identifiant des patients, serait admise, sous réserve que cette communication soit (i) indispensable à l'exercice des droits de la défense et (ii) proportionnée au but poursuivi. L'on comprend ainsi que c'est seulement si un document contenant des données médicales en clair est absolument nécessaire pour rapporter la preuve d'un fait, preuve qui ne pourrait pas être apportée autrement, que le document pourrait être communiqué en intégralité et que le secret médical serait ainsi, de façon limitée, levé.

Source : ici

EN BREF

EHDS

- L'adoption du texte progresse ! Le 15 mars 2024, le Conseil de l'UE et le Parlement européen ont trouvé un accord provisoire sur la proposition de règlement relatif à un espace européen des données de santé. La prochaine étape est l'approbation de cet accord provisoire par les deux institutions. A suivre… **source**: ici

IA ACT

- Une importante étape franchie ! Le 13 mars 2024, le Parlement européen a approuvé le règlement sur l'Intelligence Artificielle. Le texte, qui doit encore être adopté par le Conseil de l'UE, devrait être définitivement adopté avant la fin de la législature. A suivre… **source**: ici

RPPS

- La bascule de nouveaux professionnels de santé. Depuis le 13 mars 2024, les techniciens de laboratoire médical, les manipulateurs d'électroradiologie médicale, les diététiciens, les psychomotriciens et les ergothérapeutes ont intégré le RPPS. Il ne restera plus que l'intégration au RPPS des professionnels de santé de l'appareillage et des usagers de titres ADELI au milieu de l'année. Le RPPS deviendra alors « l'unique référentiel national des professionnels intervenant dans le système de santé ». **source**: ici

EDS ET CLOUD NON SOUVERAIN

- Le rapport d'expertise technique concernant le projet EMC2 publié. Le 6 mars 2024, l'Agence du Numérique en Santé a publié le rapport d'expertise technique portant sur « l'étude de faisabilité d'héberger l'entrepôt de données de santé du projet EMC2 sur une plateforme souveraine ».Il s'agit du rapport sur lequel la CNIL s'est notamment fondée pour autoriser le Health Data Hub à recourir à l'hébergeur Microsoft pour l'entrepôt de données de santé dit « EMC2 ». **source**: ici