NEWSLETTER E-SANTE

NUMÉRO 6 ● 2023

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocat counsel

SOMMAIRE

L'E-SANTÉ EN BREF

DONNÉES DE SANTÉ

- « Le Conseil national de l'Ordre des médecins et la CNIL ont annoncé, le 3 février dernier, la signature d'une convention de partenariat pour la protection des données de santé. La convention est basée sur une réciprocité de partage.» (DSIH, 14 février 2023)
- L'accès au dossier patient informatisé au sein des établissements de santé a été annoncé le 15 mars dernier par la CNIL, comme étant l'un de ses thème prioritaires de contrôle pour l'année 2023 (CNIL, 15 mars 2023).

SANTÉ CONNECTÉE

- 76% des personnes interrogées se disent prêtes à utiliser les outils de santé connectée, mais 46% ne le feraient que sous certaines conditions. Les principales craintes exprimées concernent la sécurité et le risque de détournement des données, mais aussi la diminution des interactions humaines (DSIH, 3 février 2023).

CHATGPT

- « ChatGPT a presque le niveau requis pour exercer la médecine aux Etats-Unis » (TicPharma 20 février 2023).

ARGENT

- « 1,79 milliard d'euros levés en France en 2022, trois fois plus qu'en 2021 (Karista) » (TicPharma 20 mars 2023).

EHDS

- Le 13 avril dernier, le Health Data Hub a publié 12 recommandations du groupe de travail qu'il pilote (impliquant aussi Sciensano et la NHSConfederation) sur l'implication des citoyens européens dans le futur espace européen des données de santé. Ces recommandations visant, en particulier, à sensibiliser les citoyens aux données de santé et à leur utilisation secondaire ont été partagées à la Commission européenne (Health Data Hub, 13 avril 2023 https://www.health-data-hub.fr/actualites/projet-europeen-tehdas-publication-des-recommandations-finales-pour-impliquer-les).

DISPOSITIFS MEDICAUX : LA PRISE EN CHARGE ANTICIPEE PEUT DEMARRER !

Un décret publié le 31 mars dernier précise les modalités d'application de la prise en charge anticipée par l'assurance maladie des dispositifs médicaux numériques à visée thérapeutique et des activités de télésurveillance.

Ce décret n°2023-232 du 30 mars 2023 a été pris en application de la loi de financement pour la sécurité sociale de 2022 et, plus précisément, son article 58, prévoyant une prise en charge anticipée de deux types de dispositifs médicaux :

1. Des dispositifs médicaux numériques à visée thérapeutique qui seront inscrits sur la LPPR (Liste des Produits et des Prestations Remboursables) ;

2. Des dispositifs médicaux numériques permettant une télésurveillance qui seront inscrits sur la LATM (Liste des Activités de Télésurveillance Médicale – à venir).

Avec ce système, le patient pourra bénéficier d'un remboursement pour ce type de dispositifs, prescrit par un médecin, pendant une durée d'un an avant son entrée dans le droit commun de la prise en charge.

Pour ce faire, les exploitants de tels dispositifs devront déposer un dossier dont les modalités de dépôt et de traitement sont précisées par le décret.

Ces dispositifs doivent, pour mémoire, remplir les conditions suivantes (article L.162-1-3 du Code de la sécurité sociale) :

- Être présumés innovants, « *notamment en termes de bénéfice clinique ou de progrès dans l'organisation des soins, d'après les premières données disponibles et compte tenu d'éventuels comparateurs pertinents* » ;

- Bénéficier d'un marquage CE dans l'indication considérée ;

- Garantir leur conformité aux règles de protection des données personnelles et aux référentiels d'interopérabilité et de sécurité applicables (sur le fondement de l'article L.1470-5 du code de la santé publique) ;

- Permettre « *d'exporter les données traitées, dans des formats et dans une nomenclature interopérables, appropriés et garantissant l'accès direct aux données, et comporte, le cas échéant, des interfaces permettant l'échange de données avec des dispositifs ou accessoires de collecte des paramètres vitaux du patient* ».

Le décret précise que ces conditions sont appréciées au regard :

- Des « *progrès dans l'organisation des soins* » qui « *ne doivent pas altérer la qualité des soins* » ;

- Du fait que le dispositif « *fait l'objet d'études en cours de nature à apporter* (…) *des données suffisantes pour que* [la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé] *puisse rendre un avis* ».

Les dossiers doivent être déposés auprès des ministères chargés de la santé et de la sécurité sociale et une copie doit être simultanément adressée pour avis à la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (via la plateforme EVATECH).

Aussi, la liste des critères d'évaluation doit parallèlement être envoyée à l'Agence du numérique en santé (via la plateforme « Convergence ») qui doit rendre un autre avis dans les 60 jours.

Après réception de ces avis, les ministres chargés de la santé et de la sécurité sociale doivent rendre leur décision dans les 30 jours.

Source : ici

L'UTILISATION ILLEGALE DE DONNEES DE SANTE DANS UN ARTICLE DE BLOG SPECIALISE

ANSPDCP (Roumanie), 31 janvier 2023

L'autorité de contrôle roumaine a condamné un cabinet dentaire pour avoir publié, dans un article de blog spécialisé, les données de santé de l'un de ses patients sans son consentement.

Le patient d'un cabinet dentaire a constaté que ses données de santé relatives à son traitement orthodontique (à savoir un ensemble de radiographies et de photographies), avaient été publiées sur un article de blog spécialisé sans son consentement.

Le patient a alerté le cabinet dentaire, qui, bien qu'ayant connaissance de l'existence d'une violation de données de santé, ne l'a pas notifié à l'autorité de contrôle compétente.

Face à l'inaction du cabinet dentaire, le patient a déposé une plainte.

Au cours de son enquête, l'autorité de contrôle a considéré, d'une part, que faute de pouvoir apporter la preuve de l'obtention du consentement du patient, le traitement opéré par le cabinet dentaire n'était fondé sur aucune base légale, méconnaissant ainsi les articles 6 et 9 du RGPD.

L'autorité a constaté, d'autre part, que le cabinet médical, pourtant alerté, n'avait pas notifié la violation de données à l'autorité de contrôle dans les 72 heures, manquant ainsi aux dispositions de l'article 33 du RGPD.

Elle a rappelé, enfin, que dès lors qu'un cabinet dentaire traite des données de santé dans le cadre de la fourniture de soins, l'utilisation de telles données à d'autres fins nécessite (i) de se fonder sur une base légale valide, (ii) d'informer la personne concernée et, (iii) selon les circonstances, de prendre les mesures techniques et organisationnelles adaptées, en particulier d'anonymisation ou de pseudonymisation, ce que le cabinet dentaire n'avait pas fait en l'espèce.

Compte tenu de ces manquements, l'autorité de contrôle a infligé au cabinet médical une amende d'environ 1.000 €.

Source : ici

DOUBLE PEINE POUR UN HOPITAL : RANSOMWARE ET SANCTION DE L'AUTORITE DE CONTROLE

CDP (Irlande), 23 janvier 2023

L'autorité de contrôle irlandaise a sanctionné un hôpital qui avait subi une attaque par ransomware, pour n'avoir pas mis en œuvre les mesures techniques et organisationnelles adéquates.

Un hôpital irlandais a subi une attaque informatique par ransomware qui a entraîné l'accès non autorisé, la modification et la destruction de données personnelles de 70 000 patients, incluant des données de santé. Malgré des sauvegardes quotidiennes, certaines de ces données personnelles n'ont pas pu être récupérées.

L'autorité de contrôle irlandaise, après avoir reçu la notification de la violation de données personnelles, a ouvert une enquête et a sollicité de l'hôpital la fourniture d'informations relatives aux mesures de sécurité mises en œuvre.

Elle a, dans un premier temps, considéré que « *le traitement des données à caractère personnel par l'hôpital présentait un risque élevé, tant en termes de probabilité que de gravité, pour les droits et libertés des personnes concernées* », en raison notamment de « *la quantité importante de données* », relevant de « *catégories particulières* » et des « *risques d'entrave à la fourniture de soins médicaux aux personnes concernées* ».

Elle a, dans un second temps, analysé en détail les « *mesures mises en œuvre par l'hôpital pour faire face aux risques* » et considéré ces dernières insuffisantes, dès lors que l'hôpital :

Dans ce contexte, l'autorité de contrôle irlandaise a infligé à l'hôpital une amende de 460.000 €.

Source : ici

PAS DE DONNEES PERSONNELLES DANS UNE THESE DE MEDECINE

GDPD (Italie), 24 novembre 2022

Un médecin a été sanctionné par l'autorité de contrôle italienne pour avoir publié dans sa thèse, accessible sur internet, des données non anonymisées.

Sous la supervision d'un psychiatre référent, un couple a réalisé une consultation auprès d'un interne en médecine se spécialisant en psychiatrie.

Le couple a, par la suite, appris de manière fortuite que ladite consultation, qui avait été relatée dans la thèse de l'interne, avait été publiée sur un site internet dédié aux publications scientifiques. Par ailleurs, la thèse comportait de nombreuses données personnelles les concernant, et notamment leur âge (ainsi que celui de leurs enfants), mais également leur profession, leurs histoires familiales respectives et de nombreux autres éléments d'ordre personnel. Seuls les noms avaient été pseudonymisés.

Le couple a déposé une plainte auprès de l'autorité de contrôle italienne qui a constaté que la thèse « *contenait les données personnelles (y compris des données de santé)* » du couple, et que le médecin « *avait effectué un traitement de données personnelles en violation [du RGPD]* ».

Pour sa défense, le médecin se prévalait de l'anonymisation des noms de famille. Mais l'autorité de contrôle a rappelé que le simple remplacement du nom de famille par un pseudonyme n'est pas une mesure appropriée pour garantir l'anonymisation des données à caractère personnel et, en tout état de cause, que le seul fait d'avoir eu recours à un psychiatre est déjà une donnée de santé.

Constatant (i) l'absence de base légale, conformément aux articles 6 et 9 du RGPD, et, à défaut (ii) l'absence d'anonymisation en bonne et due forme, l'autorité de contrôle italienne a infligé au médecin une amende de 1.000 euros.

Source : ici

PROFILER UNE PERSONNE POUR DETERMINER SON RISQUE DE COMPLICATION EN CAS DE COVID EST ILLICITE

ACTUALITES

GDPD (Italie), 15 décembre 2022

L'autorité de contrôle italienne a sanctionné une agence sanitaire italienne pour avoir établi un profil de risque de patients en cas de contraction de la covid-19 en méconnaissance de nombreux principes du RGPD.

Dans le but de mettre en œuvre *« des interventions préventives de prise en charge du patient », une* agence sanitaire italienne a créé des *« profils de risques sanitaires » afin de « classer les patients considérés comme étant à risque ».*

Plus précisément, l'agence sanitaire a accédé à une base de données comportant les données de santé de près de 40 000 personnes et a effectué sur cette base un traitement algorithmique.

L'algorithme profilait les personnes et dressait une liste des patients les plus à risques en cas d'infection à la covid-19.

Alerté par l'existence de ce traitement, l'autorité de contrôle italienne a ouvert une enquête et considéré que le traitement était illégal car (i) violait le principe de licéité (article 5§1a du RGPD) et (ii) était réalisé en violation de l'interdiction de traiter des données de santé (article 9 du RGPD).

Plus encore, le responsable du traitement n'avait pas fourni aux personnes concernées les informations nécessaires (articles 12 à 14 du RGPD) et n'avait pas réalisé d'analyse d'impact relative à la protection des données personnelles, compte tenu notamment du grand nombre de personnes concernées par le traitement de données de santé (article 35 du RGPD).

En conséquence, l'autorité de contrôle a prononcé une amende de 55.000 € à l'encontre de l'agence sanitaire.

Source : ici

TRANSFERT D'UN RAPPORT MEDICAL AU MAUVAIS DESTINATAIRE

GPDP (Italie), 20 octobre 2022

L'autorité de contrôle italienne a sanctionné un hôpital pour avoir transféré un rapport médical au mauvais destinataire.

A la suite d'une erreur humaine, un hôpital a transmis par courriel un « rapport d'anatomie pathologique » en intervertissant deux patients.

L'un des patients a immédiatement signalé cette erreur et a déposé une plainte auprès de l'autorité de contrôle italienne.

L'enquête initialement dirigée contre l'hôpital a été étendue à « l'institut d'étude et de prévention du cancer », ce dernier étant, selon l'hôpital et l'autorité de contrôle, le responsable du traitement, l'hôpital n'étant que sous-traitant au sens du RGPD.

Bien que constatant l'existence d'une violation de données, l'autorité de contrôle n'a pas sanctionné le responsable du traitement, considérant que le contrat conclu et que les instructions confiées au sous-traitant étaient satisfaisantes, et surtout qu'à la suite de l'incident, « l'institut avait mis en œuvre des mesures visant à minimiser le risque de survenance d'évènements similaires ».

En revanche, l'autorité de contrôle a considéré que l'hôpital, sous-traitant, avait réalisé un traitement de données à caractère personnel en violation des obligations de sécurité imposées par le RGPD.

En conséquence, l'autorité de contrôle italienne a infligé à l'hôpital une amende de 9000 €.

Source : ici

RECHERCHES MEDICALES : RAPPEL A L'ORDRE DE LA CNIL

VU DANS LA PRESSE

« DSIH » 17 MARS 2023

La présidente de la CNIL a rappelé à deux organismes procédant à des recherches médicales leurs obligations légales.

Deux organismes procédant à des recherches médicales entre janvier et juillet 2022 ont fait l'objet d'un signalement ayant donné lieu à un contrôle de la CNIL. Cette dernière a constaté plusieurs manquements aux règles sur la protection des données, dont l'absence d'analyse d'impact et la délivrance aux patients concernés d'une information incomplète[1].

1. Sur l'obligation de réaliser une étude d'impact

A titre liminaire, la CNIL a rappelé qu' *« à l'exception des recherches internes (réalisées à partir des données collectées pendant les soins par les professionnels de santé prenant en charge les patients, et pour leur usage exclusif), les recherches en santé doivent être autorisées par la CNIL ou être conformes à une méthodologie de référence.* »

Ces méthodologies sont au nombre de six dont :

– Pour les recherches impliquant la personne humaine :

- La MR-001, pour les recherches interventionnelles et les recherches interventionnelles à risques et contraintes minimes ;
- La MR-002 ou la MR-003, pour les recherches non-interventionnelles ;

– Pour les recherches n'impliquant pas la personne humaine, la MR-004.

En application de ces méthodologies, une analyse d'impact doit être réalisée et ce, avant le démarrage de la recherche.

A titre d'illustration, la méthodologie de référence « MR-001 » indique que : « *Le responsable du traitement doit effectuer une analyse d'impact relative à la protection des données, qui doit couvrir en particulier les risques sur les droits et libertés des personnes concernées. Il met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques identifiés. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires.* »

Ce n'est qu'une fois l'analyse d'impact réalisée que le responsable du traitement est censé être en mesure de décider entre :

– Une demande d'autorisation à la CNIL (hypothèse dans laquelle l'analyse d'impact révèle que les traitements envisagés dans le cadre de la recherche ne sont pas conformes à la méthodologie de référence applicable) ; ou

– Un engagement de conformité à la méthodologie de référence applicable (hypothèse dans laquelle l'analyse d'impact révèle que les traitements envisagés dans le cadre de la recherche sont conformes à la méthodologie de référence applicable).

En l'espèce, les deux organismes visés par le contrôle de la CNIL n'avaient réalisé aucune analyse d'impact concernant les recherches médicales menées.

2. Sur l'obligation d'informer les personnes concernées

La CNIL a constaté que l'information délivrée par les deux organismes aux personnes participant aux recherches était incomplète. L'autorité de contrôle a notamment souligné que « les feuillets d'information remis par les deux organismes ne précisaient ni la nature des informations collectées ni leur durée de conservation ». Par ailleurs, ces supports n'indiquaient pas les coordonnées du délégué à la protection des données, ni les modalités de recours auprès de la CNIL.

Enfin, et surtout, la CNIL a relevé qu'une notice d'information affirmait que les données étaient anonymisées, ce qui n'était pas le cas, « puisque l'identité des patients était seulement remplacée par un « numéro patient » à trois chiffres et un « code patient » composé de deux lettres correspondant à la première initiale du nom et du prénom de la personne concernée ». Ainsi, et comme l'a souligné la CNIL : « Cette procédure aboutit à une pseudonymisation des données, et non à une anonymisation, dans la mesure où il demeurait possible d'isoler un individu dans le jeu de données et de le réidentifier. »

Il convient de relever, sur ce dernier point, que les méthodologies des référence susvisées n'imposent pas aux organismes une anonymisation des données de santé, mais une simple pseudonymisation. Elles prévoient d'ailleurs un régime distinct selon que les données sont « *directement identifiantes* » ou « *indirectement identifiantes* » (et donc pseudonymisées). Ainsi, seules ces dernières peuvent être communiquées au responsable du traitement (à savoir l'organisme responsable de la recherche), contrairement aux premières.

Ainsi, seules ces dernières peuvent être communiquées au responsable du traitement (à savoir l'organisme responsable de la recherche), contrairement aux premières. Les traitements de données concernés par les manquements susvisés ayant cessé après les contrôles, la présidente de la CNIL a décidé d'adresser un simple rappel aux obligations légales à chacun des deux organismes, comme prévu par la loi « Informatique et Libertés ».

3. Point d'attention

L'analyse d'impact un outil qui contribue à la construction d'un traitement conforme au RGPD et respectueux de la vie privée. Cette analyse – en partie de nature technique – permet d'identifier des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, facilitant ainsi la détermination des mesures techniques et organisationnelles nécessaires pour protéger les données. Indépendamment de son caractère obligatoire pour certains traitements tels que ceux mis en œuvre dans le cadre de la recherche médicale, cette analyse d'impact est vivement recommandée dans l'optique de sécuriser les traitements.

A cet égard, il est rappelé, à toutes fins utiles, que la sécurité des données de santé, qui avait déjà été retenue comme thématique annuelle des contrôles de la CNIL en 2020 et en 2021, est une « *question récurrente* » que la CNIL rencontre dans un grand nombre de dossiers et qui concerne l'ensemble des établissements de santé.

VU DANS LA PRESSE

« DSIH » 17 MARS 2023

En 2023, la sécurité des données sera encore au cœur des préoccupation de l'autorité de contrôle : « *Des vérifications ont déjà été engagées par la CNIL sur l'accès au dossier patient informatisé (DPI) en 2022 et se poursuivront en 2023. Ce choix fait notamment suite à des plaintes reçues par la CNIL qui dénoncent des accès par des tiers non autorisés à des DPI au sein d'établissements de santé. Les contrôles menés auront également pour objet d'examiner l'ensemble des mesures mises en place pour assurer la sécurité des données.* »

Lien vers l'article original : ici