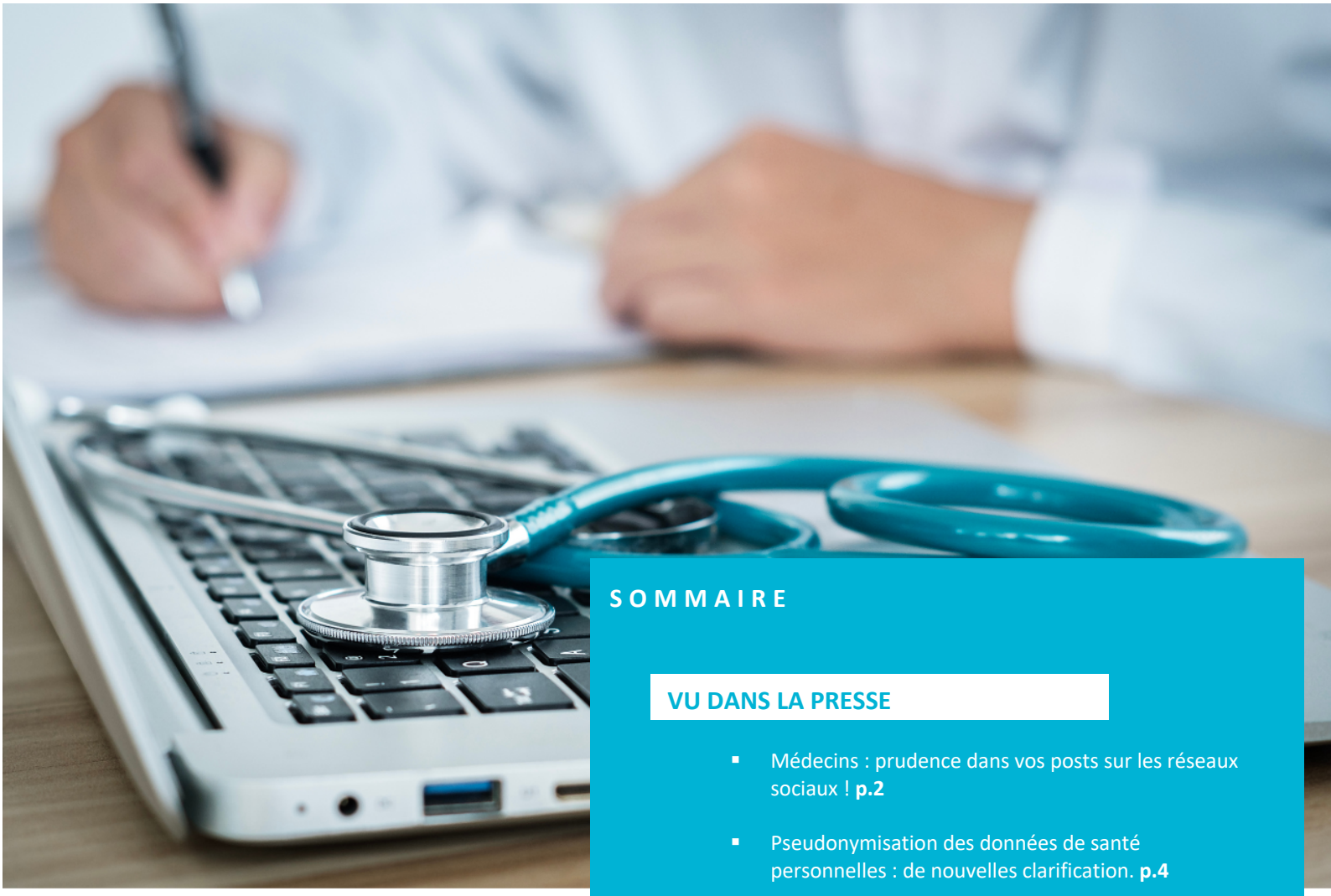
NEWSLETTER

E-Santé

NUMÉRO 15 • 2025



SOMMAIRE

VU DANS LA PRESSE

VU DANS LA PRESSE

« DSIH », JANVIER 2025

MEDECINS : PRUDENCE DANS VOS POSTS SUR LES RESEAUX SOCIAUX !

La santé et, plus particulièrement, la médecine n'échappent pas aux réseaux sociaux. Vecteurs de diffusion d'informations médicales auprès du grand public, ils présentent aussi des risques de dérives : informations partielles, erronées, dangereuses (notamment pour les « pratiques de soins non conventionnelles » et les « actes à visée esthétique »), voire désinformations. Afin de responsabiliser les médecins sur le sujet, le Conseil National de l'Ordre des médecins (« CNOM ») a récemment élaboré une charte spécifique à respecter.

L'objectif de cette charte, publiée le 16 janvier dernier, est double : favoriser une information médicale, fiable, accessible et protéger la santé collective.

Ce sont ainsi tous les médecins « *créateurs de contenus* » et ce, sur tout type de réseau social, qui sont concernés.

Cette charte, relativement brève, réalisée par le CNOM avec des médecins « *créateurs de contenus* » et la plateforme Youtube, contient 10 grands principes à respecter. Il s'agit, en réalité, de déclinaison de règles éthiques et déontologiques qui s'imposent à la profession « *dans une approche en phase avec les pratiques de création de contenus sur les réseaux sociaux* ».

Que peut-on en retenir ?

Les médecins « *créateurs de contenus* » sur les réseaux sociaux doivent :

- Publier uniquement des « *contenu*[s] *pédagogique*[s] », les « *contenu*[s] *médica*[ux] et *scientifique*[s] *vulgarisé*[s] » et « *tout autre contenu concernant des thématiques de santé* » ;
- Qualifier (en fonction des outils mis à disposition par le réseau social concerné) les publications de « *contenu de santé* » et s'identifier en tant que médecin, étant entendu que seuls les professionnels détenteurs du titre « *Dr* » doivent l'utiliser dans leur pseudonyme ;
- Mentionner leurs partenariats éventuels dans les contenus ;
- Préciser la date et la source « *explicites et détaillées* », à jour, des contenus ;
- Bannir la promotion personnelle et l'activité commerciale, mais également le recours au référencement payant ;
- Ne pas dispenser de conseil médical personnalisé et faire preuve de prudence et de modération dans les propos et les interactions avec les autres utilisateurs du réseau social en cause.

Par ailleurs et de façon générale, il convient de garder à l'esprit deux points essentiels.

D'une part, si cette charte n'est pas juridiquement contraignante, son non-respect pourrait constituer un manquement déontologique. D'autre part, respecter cette charte ne saurait pour autant assurer à tout médecin « créateur de contenu » la pleine conformité de ses publications et une absence de mise en jeu de sa responsabilité.

D’autres règles que celles édictées dans la charte s’imposent effectivement au médecin, par sa profession (respect du secret médical et, plus généralement, des dispositions du Code de la santé publique) ou, plus généralement, par sa qualité d’auteur de publications en ligne (respect des droits de tiers, de la propriété intellectuelle, du RGPD), etc.

La prudence reste donc de mise…

Alexandre Fievée
Alice Robert

VU DANS LA PRESSE

« DSIH », AVRIL 2025

PSEUDONYMISATION DES DONNEES DE SANTE PERSONNELLES : DE NOUVELLES CLARIFICATION

La pseudonymisation des données de santé personnelles est une technique requise, dans certains cas, pour assurer la conformité légale de vos traitements. Elle soulève toutefois des questions quant à sa caractérisation et sa mise en œuvre. De nouvelles lignes directrices du CEPD ont récemment été publiées sur le sujet [1].

Dans le secteur de la santé, le recours à des données pseudonymisées peut être nécessaire dans le cadre de certains traitements de données de santé à caractère personnel. Plusieurs « référentiels CNIL » imposent d'ailleurs, dans des cas spécifiques, le recours à la pseudonymisation. A titre d'exemple, le référentiel sur l'EDS impose la pseudonymisation des données de santé à caractère personnel comme une exigence de sécurité à plusieurs niveaux.

Mais qu'entend-on par pseudonymisation ? Quel est l'intérêt de recourir à une telle technique et comment la mettre en œuvre ?

Le Comité Européen à la Protection des Données (CEPD ou EDPB) a récemment adopté, des lignes directrices apportant quelques clarifications à ces questions.

La pseudonymisation, de quoi parle-t-on ?

Le CEPD rappelle que la pseudonymisation est un « *traitement de données à caractère personnel de telle sorte que ces données ne puissent plus être attribuées à une personne concernée précise sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* »[2].

Concrètement, la pseudonymisation consiste à remplacer des données à caractère personnel directement identifiantes (exemples : nom, prénom, adresse, numéro de téléphone) par des données indirectement identifiantes (exemples : alias, codes) – les « données pseudonymisées » -, étant précisé que, pour pouvoir réidentifier la personne concernée par les données pseudonymisées, il faut disposer d'informations supplémentaires, telles que, comme l'indique le CEPD, un tableau de correspondance ou encore des clés cryptographiques. Le CEPD souligne le fait que ces informations supplémentaires – qui permettent donc d'identifier directement la personne concernée – ne doivent pas être divulguées ou utilisées par les personnes qui traitent les données pseudonymisées.

Les données pseudonymisées sont des données à caractère personnel, comme le rappelle le CEPD. Toutefois, le CEPD indique que « *si les données pseudonymisées et les informations complémentaires peuvent être combinées compte tenu des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par une autre personne, les données pseudonymisées sont alors à caractère personnel* ».

Pourquoi une telle précision ? Y aurait-il des données pseudonymisées qui ne seraient pas à caractère personnel ? Est-ce que cette précision vient faire écho à la position prise par le Tribunal de l'Union Européenne (TUE) dans une affaire de 2023 et, plus récemment, par l'Avocat général près la Cour de Justice de l'Union européenne (CJUE) ?

Le TUE a jugé que, pour déterminer si les informations transmises au tiers sont « *des informations se rapportant à "une personne physique identifiable"* », il convient de rechercher si ce tiers dispose « *de moyens légaux et réalisables en pratique lui permettant d'accéder aux informations supplémentaires nécessaires à la réidentification des auteurs des commentaires* »[3]. À défaut, les informations transmises ne sont pas des données à caractère personnel. L'Avocat général a adopté une approche similaire, considérant que le tiers ne doit être considéré comme traitant des données personnelles que sous réserve qu'il dispose *« de moyens raisonnables d'identifier* [les personnes concernées][4] ».

Pourquoi recourir à la pseudonymisation dans le secteur de la santé et comment ?

Le CEPD prend l'exemple d'un hôpital universitaire qui chercherait à améliorer ses services et ses processus de facturation. Pour ce faire, l'hôpital aurait besoin d'analyser des données de « traitement » (durée du séjour, procédures de diagnostic et interventions thérapeutiques appliquées, ressources consacrées aux soins du patient, données d'identification du patient, etc.). L'hôpital se trouverait alors confronté à la problématique suivante : permettre à son personnel administratif non médical travaillant dans « *un environnement de sécurité moyen* » une analyse de données médicales particulièrement sensibles, tout en étant en capacité de pouvoir remonter des informations aux gestionnaires de soins au cas où des irrégularités seraient constatées dans les données.

Selon le CEPD, l'hôpital pourrait recourir à la pseudonymisation afin que son personnel administratif non médical n'ait pas accès aux données de « traitement » identifiant les patients.

Le CEPD propose alors un processus de mise en œuvre d'une telle pseudonymisation.

Il s'agirait, dans un premier temps, de sélectionner les données pertinentes pour l'analyse à réaliser (ex. : durée du séjour, diagnostics, etc.), à l'exclusion (i) des « *documents très individuels* » (ex. : lettre de sortie), (ii) des documents présentant un risque particulier de confidentialité (ex. : notoriété d'un dossier, intérêt pour le public du patient, etc.) et (iii) des données permettant au personnel extérieur aux départements médicaux d'identifier directement les patients. Dans un deuxième temps, ces données pertinentes sélectionnées, ainsi que l'identifiant du patient et l'ID du dossier cryptés, seraient transmis à une base de données dédiée « *opérant en dehors de la zone du réseau médical* ». Quant aux informations supplémentaires nécessaires à l'identification des patients (clé de chiffrement, dossiers médicaux originaux), elles seraient stockées dans une autre base. L'analyse serait alors faite, dans un dernier temps, exclusivement sur les données figurant dans la base pseudonymisée dédiée, étant précisé que seul le personnel non médical n'ayant pas accès au SI de l'hôpital aurait un accès à cette base.

La pseudonymisation apparaît ici notamment comme une mesure de sécurité dans la mesure où la personne accédant à la base de données dédiée, sans autorisation et sans connaissance préalable de l'état de santé des patients sélectionnés, ne serait pas en mesure de tirer des conclusions sur l'état de santé d'un individu.

Si la pseudonymisaiton des données de santé reste un sujet épineux, ces nouvelles lignes directrices du CEPD constituent un nouveau document de référence à prendre en compte.

Alexandre Fievée
Alice Robert

[1] https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf
[2] Article 4(5) du RGPD.
[3] TUE, 26 avril 2023 (aff. T-557/20).
[4] Conclusions de l'Avocat général, M. Spielmann ? – 6 février 2025 (aff. C-413/23 P).

VU DANS LA PRESSE

« DSIH », MAI 2025

UN HOPITAL, SOUS-TRAITANT, SANCTIONNE POUR NE PAS AVOIR DECLARE LES SOUS-TRAITANTS ULTERIEURS

Par décision du 10 avril 2025[1], l'autorité de contrôle espagnole a infligé une amende de 500.000 euros à un hôpital qui avait recruté des sous-traitants ultérieurs sans en informer préalablement le responsable du traitement.

Un sous-traitant bénéficiant d'une autorisation générale de recruter des sous-traitants ultérieurs

Le ministère de la santé de Valence a eu recours aux services de l'hôpital Marina Salud, aux termes d'un contrat relatif à la fourniture de services de soins de santé. L'hôpital, qualifié dans le contrat de « sous-traitant » au sens du RGPD (ce qui est assez étonnant), bénéficiait d'une autorisation générale de recruter des sous-traitants ultérieurs, sous réserve d'en informer préalablement le ministère de la santé.

Au cours d'un audit réalisé auprès de l'hôpital, le ministère de la santé a constaté que son sous-traitant utilisait des logiciels tiers pour réaliser certains traitements qui lui étaient confiés, suggérant que l'hôpital avait recruté des sous-traitants ultérieurs à l'insu du ministère de la santé.

À la suite du refus de l'hôpital de communiquer les contrats des fournisseurs des logiciels tiers, le ministère de la santé de Valence a saisi l'autorité de contrôle espagnole (AEPD) d'une plainte.

L'autorisation générale de recruter des sous-traitants ne dispense pas le sous-traitant de son obligation d'informer le responsable du traitement

L'enquête menée par l'AEPD a mis en lumière que l'hôpital avait, dans le cadre des traitements réalisés pour le compte du ministère de la santé, eu recours à des sous-traitants ultérieurs, dont l'identité n'avait pas été communiquée au ministère de la santé.

Or, le contrat conclu avec le ministère de la santé, s'il instaurait une autorisation générale de recourir à des sous-traitants, assortissait cette autorisation d'une obligation de porter à la connaissance du ministère de la santé l'identité des sous-traitants auquel l'hôpital avait recours.

De même, l'article 28 du RGPD prévoit qu'en cas d'autorisation générale de sous-traitance ultérieure, il appartient au sous-traitant d'informer le responsable du traitement de « *tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitant* » et ce, afin de donner à ce dernier la possibilité d'émettre des objections à l'encontre de ces changements.

Compte tenu de ce qui précède, l'AEPD a considéré que l'hôpital avait non seulement violé le contrat conclu avec le ministère de la santé, mais avait aussi manqué à ses obligations au titre de l'article 28 du RGPD.

A noter enfin que, selon l'AEPD, le défaut d'information du responsable du traitement est une violation continue, qui persiste pendant toute la durée du recours au sous-traitant ultérieur à l'insu du responsable du traitement. La durée de cette violation a été prise en compte par l'AEPD, qui a fixé le montant de l'amende à 500.000 euros.

Alexandre Fievée
Alice Robert
Gaétan Dufoulon

[1]https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202307719

VU DANS LA PRESSE

« DSIH », JUIN 2025

IA & ETHIQUE DU NUMERIQUE EN SANTE : LE GUIDE D'IMPLEMENTATION DE L'ANS

Compte tenu, d'une part, des perspectives d'amélioration que l'IA promet dans le secteur de la santé et, d'autre part, de la montée en charge rapide de l'offre de systèmes d'IA (SIA), la cellule éthique de la Délégation au numérique en santé (DNS) a réuni un groupe de travail (GT) pluridisciplinaire dans l'optique d'identifier et de formaliser les critères d'un SIA en santé éthique.

Après la publication en 2022 de recommandations de bonnes pratiques pour une éthique by design des solutions d'IA en santé, ce groupe de travail a élaboré un Guide d'implémentation d'un SIA en santé éthique[1], et ce afin d'aider les fournisseurs de SIA à développer et mettre sur le marché des solutions conformes aux principes fondamentaux de l'éthique du numérique en santé.

Objectif et contenu du Guide

Le guide, destiné aux fournisseurs de SIA, a pour objet de « *mettre en lumière les enjeux éthiques spécifiques aux SIA en santé, que le Règlement sur l'intelligence artificielle (RIA) aborde partiellement ou pas du tout* ».

Ce guide est constitué de « *critères* », déclinés à partir des « *principes fondamentaux* » qui sous-tendent l'éthique, à savoir : la bienfaisance (l'amélioration et le bien-être des patients) ; la non-malfaisance (la sécurité des patients doit être la priorité) ; l'autonomie (les patients doivent rester pleinement acteurs de leur santé) ; la justice (l'accès aux technologies doit être équitable) ; l'écoresponsabilité (la prise en compte des impacts environnementaux).

A noter que ces critères s'intègrent dans les différentes phases de la construction d'un SIA : la phase projet (cadrage) ; la phase de développement (collecte des données, conception du SIA, etc.) ; et la phase de déploiement et d'usage.

Opposabilité du Guide

Comme l'indique l'ANS, « *ce document est un guide thématique, qui n'a pas vocation à devenir opposable en tant que tel* ». Toutefois, l'agence indique qu'il pourrait « *être décliné dans des référentiels sectoriels et certains critères pourraient devenir opposables où ils seraient exigés dans le cadre d'un bénéfice associé* ».

Ce guide, proposé par la DNS et l'ANS, a été mis en consultation publique (concertation) du 12 mai au 6 juin 2025.

Nous vous tiendrons informés des suites de cette consultation publique et nous vous invitons à participer à notre Matinale dédiée à l'IA, au cours de laquelle ce guide sera largement présenté. Cette matinale se tiendra le 19 juin prochain, au 5 de l'avenue d'Opéra à Paris[2].

Alexandre Fievée
Alice Robert

[1] https://participez.esante.gouv.fr/project/guide-dimplementation-dune-intelligence-artificielle-ia-en-sante-ethique/presentation/presentation
[2] https://derriennic.com/evenements/