Protection des données médicales

Fiche pratique publié le **23/02/2021**, vu **1741 fois**, Auteur : Murielle Cahen

L'impératif de la protection des données de santé s'est accru à l'occasion de l'informatisation des structures de santé et de la dématérialisation des supports et des flux.

La notion de donnée de santé trouve son origine dans la convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée par le Conseil de l'Europe. Sans en donner de définition, ce texte prévoit que les données à caractère personnel relatives à la santé sont des catégories particulières de données, qui “ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées” (art. 6).

Avec le risque d'intégrité, l’atteinte à la confidentialité des données personnelles de santé constitue l'un des risques à l'obligation de sécurité les plus facilement identifiables.

En pratique, elle se caractérise par la nécessité de prendre les mesures requises pour interdire toute “utilisation non autorisée de données” personnelles (Règl. (UE) 2016/679, 27 avr. 2016, cons. 39. – Dir. (UE) 2016/680, 27 avr. 2016, cons. 28), en particulier du fait de “l'accès [à ces données] par des personnes non autorisées” (L. n° 78-17, 6 janv. 1978, mod. par Ord. n° 2018-1125, 12 déc. 2018, art. 4, 6°). Surtout, cela signifie a contrario que sont bien admis à disposer d'un tel accès les tiers, eux, autorisés.

À cette occasion, tant le législateur que l'autorité de protection des données personnelles, la Commission nationale de l'informatique et des libertés (CNIL), ainsi que l'État et ses agences, ont développé un corpus de règles et de recommandations destiné à assurer la protection des données de santé, non seulement du point de vue des garanties juridiques mais également de la sécurité des systèmes d'information

Par ailleurs, le secret médical a un caractère absolu précise la Cour de cassation, chambre criminelle du 5 juin 1985, n° 85-90.322. Le caractère secret et absolu dans le domaine médical permet de s’interroger sur comment sont protéger les données personnelles des personnes concernées.

Les données de santé ont toujours été considérées comme au cœur de l'intimité des personnes, dès lors que traditionnellement, elles se confondaient avec les données issues du dossier médical. À ce titre, elles bénéficient d'un haut niveau de protection, à la fois grâce à la protection de la vie privée (Code civil, article 9), du secret professionnel qui les protège (CSP, art. L. 1110-4) «Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant » et de la législation relative à la protection des données personnelles.

Les fichiers comportant des données à caractère personnel sont soumis à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique et aux libertés, ainsi qu'au règlement général de protection des données (RGPD), sous le contrôle de la CNIL.

Enfin, cette protection s'est accrue du fait que les données personnelles de santé sont devenues un véritable trésor très convoité par les géants de l'informatique en vue d'une monétisation (Les données de santé, un trésor mondialement convoité - Par Laure Belot Publié le 02 mars 2020 à 18h30 - Mis à jour le 03 mars 2020). Il se pose une de plus la question de la sécurité des données de santé (Orange Healthcare : La sécurité des données de santé est un enjeu de plus en plus primordial).

I) Approche définitionnelle de la donnée médicale

A) La définition des données de santé par l'article 4.15 du RGPD

Selon l'article 4.15 du RGPD les données à caractère personnel concernant la santé (https://www.cnil.fr/fr/reglement-europeen-protection-donnees) sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Cette définition comprend donc par exemple :

Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;

Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;

Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

Cette définition permet d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

B) L'importance ou le caractère précieux des données de santé

Les données de santé se trouvent dans la grande famille des données dites sensibles telles qu'énoncées à l'article 9 RGPD.

En effet, l'article 9 RGPD dispose que : « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ». Cet article souffre néanmoins de quelques exceptions.

Elles sont précieuses en ce qu'elles concernent la vie privée de la personne concernée. L'information à délivrer aux personnes concernées par un traitement de données de santé est soumise au régime de droit commun de l'information des personnes, prévu aux articles 12, 13 et 14 du RGPD.

La nature sensible des données de santé impose néanmoins aux responsables de traitement une particulière vigilance, notamment au regard de l'obligation de transparence de l'article 12.

De plus dans le considérant numéro 1 du RGPD, le parlement Européen élève la protection des personnes physiques à l'égard du traitement des données à caractère personnel comme un droit fondamental « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte ») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant ».

Conscient du caractère sensible des données médicales, la CNIL a été saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS-CoV-2.

En effet, le projet de décret dont a été saisie la Commission prévoyait la création d'un système d'information pour la mise en œuvre, le suivi et le pilotage des campagnes vaccinales contre la covid-19 dénommé « Vaccin Covid » (ci-après, le SI « Vaccin Covid »), sous la responsabilité conjointe de la direction générale de la santé et de la Caisse nationale d'assurance maladie (CNAM), fondé sur les articles 6.1 e et 9.2 i du RGPD.

II) Applicabilité du Règlement Européen sur la protection des données dans le secteur médical

A) Les finalités

Lorsqu'un traitement de données personnelles de santé bénéficie d'une exception à l'interdiction prévue par l'article 9-1 du RGPD et de l'article 44 de la loi Informatique et Libertés, ce traitement doit par ailleurs justifier de l'existence d'un intérêt public, sauf exceptions prévues par la loi Informatique et Libertés.

Cette exigence est issue de la nouvelle section 3 (L. n° 78-17, 6 janv. 1978, mod., art. 65 et s.), qui prévoit que les traitements de données à caractère personnel de santé ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent.

Elle découlerait du « principe rappelé par le règlement européen, que les traitements de données de santé ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent », ce qui paraît renvoyer aux termes du considérant 53 du RGPD.

Certaines finalités de traitement peuvent être intrinsèquement constitutives d'un intérêt public. Les dispositions du RGPD permettent d'identifier des domaines dans lesquels des finalités d'intérêt public peuvent être identifiées, notamment :

La santé publique, tout particulièrement la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux (règl. (UE) 2016/679, 27 avr. 2016, cons. 45 et 73 ; art. 9 (2) i) ; art. 23 (1) e)). La loi Informatique et Libertés a repris exactement ces termes (L. n° 78-17, 6 janv. 1978, mod., art. 66) ;

La gestion des services et systèmes de soins de santé et de protection sociale, y compris les retraites, notamment à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé (règl. (UE) 2016/679, 27 avr. 2016, cons. 45, 52, 53 et 73) ;

Les finalités humanitaires (règl. (UE) 2016/679, 27 avr. 2016, cons. 73) ;

Dans le cadre des transferts, les échanges internationaux de données entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport (règl. (UE) 2016/679, 27 avr. 2016, cons. 112).

Au regard des dossiers de demande d'accès au SNDS, l'INDS a identifié comme finalités générales d'études présentant un intérêt public :

L’amélioration des soins et de la santé publique ;

L’amélioration du système de santé ;

La recherche et l'augmentation des connaissances ;

La contribution potentielle à l'intérêt général d'une étude poursuivant des finalités d'intérêt privé.

En somme, l’article 17 du RGPD mentionne toutes les exceptions au principe de la collecte et du traitement des données à caractère personnel (https://www.cnil.fr/fr/reglement-europeen-protection-donnees

).

B) Désignation dans le cadre de traitements de données de santé

À ce titre, les établissements publics de santé, de par leur nature publique, sont ainsi dans l'obligation de désigner un délégué à la protection des données. (Dit DPO)

Le G 29 a par ailleurs confirmé que devaient être considérés comme traitant des données de santé à grande échelle, dans le cadre de leur activité de base, tous les établissements de santé (G 29, 5 avr. 2017, Lignes directrices concernant les délégués à la protection des données (DPD), WP 243 rév. 01, p. 8 et 25), et la CNIL a par ailleurs visé les maisons de santé, les centres de santé, ainsi que les professionnels de santé exerçant au sein d'un réseau de professionnels, ou dans le cadre de dossiers partagés entre plusieurs professionnels de santé.

C) Les droits des personnes concernées

Les droits des personnes concernées par un traitement de données de santé, à savoir les droits d'accès, de rectification, d'effacement et de portabilité des données personnelles, de limitation ou d'opposition au traitement, le droit de ne pas faire l'objet d'une décision automatisée (règl. (UE) 2016/679, 27 avr. 2016, art. 15, 16, 17, 18, 20, 21 et 22), ainsi que le droit de définir des directives relatives à la conservation, à l'effacement et à la communication des données personnelles après le décès, prévu par la loi Informatique et Libertés (L. n° 78-17, 6 janv. 1978, mod., art. 85), sont des droits qui s'appliquent à tout traitement de données à caractère personnel, quelle que soit la nature des données.

La nature sensible de ces traitements implique cependant une attention particulière. La CNIL a par exemple prononcé une sanction pécuniaire d'un montant de 10 000 euros à l'encontre d'un professionnel de santé libéral, pour défaut de réponse dans les délais à la demande de communication de son dossier médical par un patient. Cette sanction est intervenue après que la CNIL a envoyé plusieurs courriers, puis mis une première fois en demeure le professionnel de communiquer le dossier.

La CNIL a ainsi prononcé cette sanction au regard également du défaut de réponse à ses courriers, en rappelant par ailleurs que « le secret médical ne saurait s'opposer, en l'espèce, à la communication au patient des données le concernant et contenues dans son dossier médical » (CNIL, délib. n° SAN-2017-008, 18 mai 2017).

III) Le principe du consentement préalable assorti d'exceptions dans le cadre de la collecte des données des personnes concernées dans le domaine médical.

A) Le principe

Par principe, les traitements de données personnelles de santé sont interdits, comme tout traitement de catégories particulières de données (règl. (UE) 2016/679, 27 avr. 2016, art. 9. – L. n° 78-17, 6 janv. 1978, art. 6, mod.).

Une série d'exceptions, pour la plupart inspirées de celles prévues par la directive, fournissent cependant un fondement pour déroger à l'interdiction. De plus, depuis la loi du 20 juin 2018, s'ajoute une obligation générale de justifier d'un intérêt public pour traiter des données de santé, sauf dans certains cas énumérés de façon limitative (L. n° 2018-493, 20 juin 2018, art. 16. – Ord.

n° 2018-1125, 12 déc. 2018, art. 1 : JO 13 déc. 2018, texte n° 5).

Telle n'est pas la solution proposée par l'un des pays voisins européen en l'occurrence l'Espagne. En effet, face à la méfiance de la population européenne sur les vaccins Pfizer et BioNTech sortis plus tôt que prévu de ne pas se faire vacciner car considérant qu'elle ne serait pas un objet d'essai clinique voire de cobayes clinique, l'Espagne a décidé de répertorier les données personnelles des personnes ne voulant pas se faire vacciner.

Dans une interview à la chaîne de télévision La Sexta, Salvador Illa a souligné que la vaccination contre le coronavirus, qui a débuté dimanche en Espagne comme dans de nombreux autres pays de l'UE, ne serait pas obligatoire.

En ce qui concerne les personnes qui ne voudront pas se faire vacciner, « ce qu'on va faire, c'est un registre qui, de plus, sera partagé avec d'autres pays européens », a-t-il poursuivi, précisant qu'il se référait « aux personnes auxquelles on l'aura proposé (de se faire vacciner, NDLR) et qui, tout simplement, l'auront refusé ».

Alors la question serait de savoir si l'Espagne en tant que pays européen et soumis au RGPD est en droit de collecter les données personnelles des personnes ne souhaitant pas se faire vacciner ? Telle est la question de droit à résoudre.

D'autres questions seraient de savoir comment ces données personnelles seront collecter ? Qui sera le responsable du traitement ? Quels seront les sous-traitants ? Quelles seront les garanties apporter pour la confidentialité des données ? A quelles finalités se résument cette collecte ? Que risquent les personnes ne souhaitant pas donner leur consentement à la collecte de leurs données personnelles ?

Pourquoi partager les données des personnes ne souhaitant pas se faire vacciner entre pays européens ? Toutes ces nombreuses questions devraient être résolues pour éclairer les personnes concernées. Ces questions feront l'objet d'un autre article.

B) L'exception : l'obtention du consentement préalable à la collecte des données personnelles

Le consentement explicite de la personne concernée peut permettre, dans une certaine mesure, de déroger à l'interdiction de traitement des données de santé (règl. (UE) 2016/679, 27 avr. 2016, art. 9, (2).

Le consentement au sens de l'article 9 doit être conforme à la définition qu'en donne le RGPD, à savoir constituer une "manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement" (règl. (UE) 2016/679, 27 avr. 2016, art. 4 (11)), et respecter les conditions de l'article 7.

À cela s'ajoute l'exigence spécifique que le consentement soit explicite.

SOURCES :

https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante#:~:text=Les%20données%20à%20caractère%20personnel,de%20santé%20de%20cette%20perso
.

https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html

https://healthcare.orange.com/fr/dossiers/securite-des-donnees-de-sante/#:~:text=Les%20trois%20grands%20types%20de,sur%20le%20traitement%20du%20patient
.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

https://www.legifrance.gouv.fr/codes/id/LEGIARTI000036515027/2018-01-19/