FOIRE AUX QUESTIONS DU WEBINAIRE SUR LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD)

Données personnelles

Qu'est-ce qu'une donnée à caractère personnel (DCP) ?

Une donnée personnelle, c'est toute l'information qui se rapporte à une personne physique identifiée ou identifiable.

Selon l'article 4 du RGPD[1] : ce sont des informations qui se rapportent à des personnes physiques. Tout ce qui concerne les personnes morales (associations, l'ARS, le numéro FINESS, le numéro SIRET) ne rentre pas dans le champ du RGPD.

Exemples de données : adresse postale, nom, prénom, date de naissance, l'image, la signature, numéro identifiant la personne physique, comme le numéro de sécurité sociale, numéro de carte bancaire…

Exemple de personne physique identifiable : Si une personne donne son nom, elle est identifiable. Si on vous indique la DPO de l'ARS sans le nom, sachant qu'il n'y en a qu'une, il s'agit d'une personne identifiable.

Qu'est-ce qu'une donnée de santé au sens du RGPD ? Est-ce que l'information sur une affection de longue durée (ALD) sans détail est une donnée de santé au sens du RGPD ?

Une donnée de santé est l'ensemble des données se rapportant à l'état de santé d'une personne physique qui révèle des informations sur son état de santé physique ou mentale passé, présent ou futur.

« *Les données à caractère personnel relatives à la santé physique ou mentale 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* » (Article 4 du RGPD).

Exemples de données de santé : l'information relative à la résidence en établissement de personnes âgées dépendantes d'une personne, la nature des actes, médicaments

[1] Source : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000030466677

ou produits de santé et leurs codages détaillés, l'existence d'une grossesse ou d'une affection de longue durée et les éléments du protocole relatif à cette affection, etc.

Qu'est-ce qui n'est pas une donnée de santé à caractère personnel (DSP) au sens du RGPD ?

D'après la Commission nationale de l'Informatique et des Libertés (CNIL)[2] , une donnée de santé à caractère personnel (DSP) correspond aux :

- 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 ;
- 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 ;
- 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).

Par exemple, une information sur une ALD est une donnée de santé.

Les données qui ne répondraient pas à ces différentes catégories pourraient être considérées comme n'étant pas des DSP au sens du RGPD. Cependant, la notion de donnée de santé est désormais large. Elle est à apprécier, au cas par cas, compte tenu de la nature des données recueillies.

Des fichiers de professionnels de santé, avec des téléphones professionnels ou personnels sont-ils aussi concernés par le RGPD ?

Les fichiers de professionnels de santé comprennent des informations relatives à une personne physique. Dès lors que vous collectez son nom, son prénom, son numéro de téléphone, son adresse, même si c'est son adresse professionnelle, c'est un fichier concerné par le RGPD, qui doit être inscrit au registre des traitements.

Les assistants médicaux peuvent-ils accéder aux dossiers patients ?

Les assistants médicaux peuvent accéder aux dossiers des patients, mais cela dépend des tâches spécifiques qui leur sont confiées et des règles de confidentialité en

[2] Source : https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

vigueur. En général, leur accès est limité aux informations nécessaires pour accomplir leurs missions, comme la mise à jour des antécédents médicaux ou la préparation des consultations.

Les assistants médicaux doivent respecter strictement les règles de confidentialité et de protection des données personnelles des patients. Leur accès est encadré par des protocoles de sécurité pour garantir que les informations sensibles sont protégées[3] .

Comment peut-on stocker des données personnelles si cela ne peut être fait sur son ordinateur professionnel, sur clé USB ou sur disque dur ?

Il est possible de stocker des données sur un ordinateur professionnel à condition que l'ordinateur et la sauvegarde des données soient sécurisés. Il peut s'agir de mesures de sécurité physique, comme le contrôle des accès, la fermeture des salles où sont accessibles les données, des antivols pour le matériel ou des mesures logiques comme les antivirus ou des messageries sécurisées. Autrement, plusieurs solutions de stockage sécurisées alternatives existent comme les services de sauvegarde en ligne sécurisée, certifiées Hébergeurs des données de santé (HDS), s'il s'agit du stockage de données de santé.

Que se passe-t-il en cas de fuite de données ?

La première action à entreprendre est de mettre fin à la fuite le plus rapidement possible

La CNIL prévoit une procédure à suivre[4][5], surtout si c'est une fuite qui concerne un grand nombre de personnes et qui peut avoir des impacts importants sur ces personnes. C'est pour ça qu'il est important d'avoir un DPO, ainsi qu'un plan de gestion de crise préparant cette éventualité.

Des formalités sont à accomplir auprès de la CNIL, notamment leur faire remonter l'information rapidement et au plus tard dans les 72h, surtout s'il y a un risque pour les personnes concernées.
Au-delà des données administratives, si la fuite concerne les données médicales, vous pourriez être obligés d'informer les personnes concernées individuellement du fait du partage d'informations non voulu.

---

[3] Source : https://www.ameli.fr/medecin/exercice-liberal/vie-cabinet/aides-financieres/aide-emploi-assistants-medicaux

[4] Source : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

[5] Guide de la sécurité des données personnelles 2024

Quels sont les outils sécurisés pour conserver ou partager des fichiers sensibles ?

Tout dépend si c'est pour faire du partage ou du stockage. Il existe des solutions, si vous n'êtes pas éligible à certaines messageries sécurisées de santé, où le partage de données est possible, comme Bluefiles par exemple.

DPO ou DPD (délégué à la protection des données – en français)

Un DPO ou DPD est-il obligatoire pour une CPTS ?

Selon l'article 37 du RGPD, la désignation d'un DPO est obligatoire pour :

- Les autorités ou les organismes publics,
- Toutes les structures dont les activités principales les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- Toutes les structures dont les activités de base les amènent à traiter à grande échelle des données sensibles (donc de santé) ou relatives à des condamnations pénales et infractions.

Le RGPD ne définit pas la notion de grande échelle. Pour la CNIL, il revient à chaque responsable du traitement de décider de la qualification de son traitement de "traitement à grande échelle". Le considérant 91 du RGPD donne quelques précisions sur la notion de « grande échelle ». Il s'agit des traitements qui visent à traiter *« un **volume considérable de données personnelles** au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé »*.

La désignation d'un DPO est fortement recommandée par la CNIL et le Comité européen de la protection des données (CEPD). Cela permet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles et c'est toujours valorisant en termes d'image pour la structure, encore plus si ladite structure traite au quotidien des données sensibles.

Puis-je me mettre en conformité avec le RGPD sans DPO ?

La désignation d'un DPO est fortement recommandée par la CNIL et le CEPD. Cela permet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles et de limiter les risques liés au traitement des données. Le DPO est un point de contact facilement joignable, en interne comme en externe qui allie des connaissances juridiques et de sécurité informatique. Il est indépendant et peut bénéficier de soutien de la CNIL.

L'absence de DPO peut augmenter le risque d'erreur dans la gestion et le traitement des données personnelles.

C'est aussi valorisant en termes d'image pour la structure et encore plus si ladite structure traite au quotidien des données sensibles.

Si une CPTS traite des données de 100 patients en ALD sans médecin traitant (MT), est-ce qu'on doit désigner un DPO ?

La désignation d'un DPO est fortement recommandée pour la mise en œuvre de l'action 100% médecin traitant pour les patients en ALD car la CPTS traite de données sensibles et en application du principe cumulatif[6] sur le partage des données de santé, mentionné à l'article R1110-2 du Code de la santé publique. Sur ce principe cumulatif, les CPTS ne sont pas mentionnés.

Quelles doivent être les actions prioritaires des CPTS pour la mise en conformité au RGPD ?

D'après la CNIL, voici les 4 actions prioritaires à mettre en place par les CPTS pour être en conformité avec le RGPD[7] :

1. **Recenser les traitements de données** : Tenir un registre des activités de traitement pour avoir une vision claire des données collectées et traitées.
2. **Informer les personnes concernées** : Assurer la transparence en informant les individus sur la collecte et l'utilisation de leurs données personnelles.
3. **Garantir les droits des personnes** : Mettre en place des procédures pour permettre aux individus d'exercer leurs droits (accès, rectification, effacement, etc.).
4. **Sécuriser les données** : Implémenter des mesures de sécurité appropriées pour protéger les données contre les accès non autorisés, les pertes ou les fuites

Existe-t-il des outils pour accompagner la mise en conformité ?

Des ressources sont disponibles gratuitement sur le site de la CNIL pour vous accompagner dans la mise en conformité RGPD[8].

---

[6] Diapos 39 et suivantes du support webinaire RGPD

[7] Source : https://www.cnil.fr/fr/passer-laction/rgpd-les-premieres-etapes

[8] Source : https://www.cnil.fr/fr/les-outils-de-la-conformite

Traitement des données

Les CPTS peuvent-elles traiter des données de santé ? Est-ce que les CPTS ont l'autorisation de recueillir des données de santé ? Si oui, sous quelles conditions ? Sinon, comment faire compte tenu de nos missions ? Avec qui et comment puis-je partager des données (ex. : personnel de CPTS, CPAM, MT, Hôpitaux…) ?

Certaines missions impliquent nécessairement le traitement de données de santé des patients par les CPTS, ex : recherche de MT en priorisant selon l'état de santé, organisation de soins non programmés, de téléconsultation, organisation de parcours.

Il y a des obligations de respect du secret (articles 5 et 32 RGPD et L1110-4 du CSP).

L'échange et le partage de données médicales peuvent avoir lieu si trois conditions cumulatives sont réunies :

- Les professionnels appartiennent à des catégories mentionnées à l'article R1110-2 CSP
- L'échange et le partage d'informations ne peuvent porter que sur des informations strictement nécessaires à la coordination des soins ; la continuité des soins, la prévention ; au suivi médico-social de la personne,
- L'échange et le partage de données entre professionnels ne peuvent porter que **sur des informations relevant du périmètre de leurs missions.**

L'échange ou le partage de données médicales peut alors avoir lieu sous réserve de respecter une obligation d'information dans le cas d'un échange de données (R1110-3 CSP). En cas de partage de données entre professionnels de santé d'une même équipe de soins (L1110-12 CSP), une obligation d'information suffit. En cas de partage de données avec des professionnels de santé (R1110-2 CSP) ne faisant pas partie de la même équipe de soins, il existe une obligation d'information et de recueil de consentement.

A la page suivante se trouve un tableau récapitulatif.

	Obligation préalable d'information du patient	Obligation de recueillir le consentement du patient
Échange d'informations entre un professionnel relevant d'une des catégories de l'article R. 1110-2 et un professionnel relevant de l'autre catégorie de l'article R. 1110-2	OUI L'information doit porter sur la nature des informations échangées, l'identité des destinataires et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition (L 1110-4 IV. Et R1110-3 I. du CSP)	NON
Échange d'informations entre professionnels relevant d'une même catégorie mentionnée à l'article R. 1110-2 soit la 1° soit la 2°	? Le CSP ne prévoit rien, mais d'après le RGPD : OUI	?
Partage d'informations de santé entre professionnels relevant d'une des catégories mentionnées à l'article R. 1110-2 avec ceux qui relèvent de l'autre catégorie, et qui sont tous membres d'une même équipe de soins	OUI L'information doit porter sur l'existence du partage et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition. (L 1110-4 IV. Et R 1110-3 II.) (En attente des recommandations élaborées par la HAS avec le concours des ordres professionnels)	NON
Partage d'informations entre professionnels relevant d'une même catégorie mentionnée à l'article R. 1110-2 soit la 1° soit la 2° et faisant partie de la même équipe de soins	Le CSP ne prévoit rien, mais d'après le RGPD : OUI	?

Partage d'informations médicales avec un professionnel, relevant des catégories prévues à l'article R 1110-2 du CSP, ne faisant pas partie de l'équipe de soins (Article D1110-3-1 CSP)	OUI, nécessité d'un support écrit même sous forme électronique. L'information porte sur les catégories des informations échangées, catégories des destinataires, natures des supports utilisés pour le partage, les mesures prises pour préserver leur sécurité, notamment les restrictions d'accès, et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition, et plus généralement les modalités effectives d'exercice de leurs droits	OUI Consentement recueilli par tout moyen y compris sous forme dématérialisée

Un coordinateur de CPTS peut-il recueillir des données de santé avant de faire le lien entre un patient et un médecin, dans le cadre du 100 % MT en ALD par exemple ? Comment partager les données (ex : recherche MT) recueillies auprès des patients si les CPTS ne peuvent le faire ?

Il faut que ce soit un professionnel de santé mentionné à l'article R110-2 CSP qui collecte la donnée.

Un coordonnateur de CPTS qui ne réunit pas les conditions cumulatives sur le partage des données, ne peut pas recueillir de données de santé avant de faire le lien entre un patient et un médecin dans le cadre de l'action 100 % en médecin traitant.

Est-il possible de demander au patient s'il est ALD par exemple ? Comment graduer la demande dans le cadre de la mission accès à un médecin traitant ?

Certaines coordinatrices recueillent ces données ou contractualisent avec une IDE pour le faire, ce qui semble être une solution plus appropriée.

Des équipes composées de salariés coordinateurs non professionnels de santé peuvent-elles collecter ou traiter les données ?

Les équipes qui sont composées de salariés coordinateurs non professionnels de santé ne peuvent pas collecter les données.

Est-ce qu'une simple "Délégation de tâche pour l'accès aux données médicales d'un patient par un professionnel administratif de santé" écrite et signée peut suffire ?

Non.

Lorsqu'une CPTS est sollicitée par un établissement hospitalier pour faciliter la sortie d'hospitalisation (recherche MT, IDE, MK), est-ce à l'équipe hospitalière de se charger de recueillir de consentement du patient pour le partage des données ?

C'est l'établissement qui donne les informations de sortie d'hospitalisation à la CPTS qui doit recueillir le consentement Si la CPTS doit transmettre l'information à d'autres, elle doit recueillir le consentement de la personne ou son représentant légal.

Quelle est la différence entre le traitement des données par un médecin/professionnel de santé en individuel ou par un professionnel en structure de groupe ?

Il y a des exemples de traitements à grande échelle et de traitements qui ne seraient pas à grande échelle. Si c'est un médecin qui exerce à titre individuel et qu'il traite les données de ses patients, ce n'est pas un traitement à grande échelle. En revanche, si c'est un État, un hôpital, un établissement qui traite les mêmes données, les données de ces patients, il s'agit un traitement à grande échelle.

Quelle est la procédure pour enregistrer les fichiers d'annuaire des professionnels de santé ? Doit-on les faire référencer à la CNIL ?

Les fichiers d'annuaires sont un traitement de données devant être inscrits au registre de la structure. Si ce ne sont que des données d'identité, des coordonnées, il ne s'agit pas de données sensibles[9], il n'y a pas de formalités à faire vis-à-vis de la CNIL. Cependant, l'annuaire doit a minima figurer dans le registre.

[9] Ce sont des informations qui révèlent la prétendue 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. Source : Donnée sensible | CNIL

Accompagnement

Le GIP SESAN peut-il accompagner les CPTS sur les questions de RGPD ?

Le GIP SESAN dispose d'un service d'assistance au DPO ou de DPO externalisé pour les CPTS. Pour toute demande d'information, contactez ssi@sesan.fr.

Y a-t-il un budget de prévu pour les CPTS afin de financer la mise à conformité aux exigences RGPD ?

La conformité RGPD est une obligation légale et n'est pas financée.

Dans le cadre de son offre, le SESAN propose un audit des besoins en SI des CPTS. Cela intègre-t-il la question de protection des données ?

Ce service est en cours de construction. Pour toute demande d'information, contactez ssi@sesan.fr.

Où en est le déploiement de la solution régionale de coordination médicale ?

La nouvelle solution de coordination régionale Santélien[10], à savoir le tchat sécurisé et le dossier de coordination, est disponible pour tous les acteurs de santé en Île-de-France.

Outils

Est-ce que les deux dispositifs : DMP et mon espace santé vont persister ?

Le DMP et Mon Espace Santé sont deux services nationaux qui vont persister. Ces 2 services font partie d'un ensemble d'outils et services socles nationaux visant à garantir le stockage ainsi que le partage des données de santé de manière sécurisée.

Est-ce qu'une CPTS peut avoir une adresse MSSanté ?

Une CPTS peut avoir une MSSanté. Nous conseillons une MSSanté de type organisationnelle permettant à plusieurs personnes d'avoir accès à cette boîte aux

[10] Santélien | la solution eParcours d'Ile-de-France

lettres (BAL). Cette BAL sera sous la responsabilité d'un professionnel avec un numéro RPPS.

Ne faudrait-il pas que les CPTS soient équipés d'un dossier patient informatisé ?

Les CPTS ne sont pas effectrices de soins. A cet effet, elles n'ont pas vocation à collecter et stocker des données de santé de volumes importants de patients en dehors de leurs missions.

De plus, l'investissement dans un DPI (dossier patient informatisé) pourrait être très couteux (financièrement et en temps) pour une CPTS.

Quid d'un outil de type covidom/covisan qui avait une partie médicale et une partie administrative et sociale ?

Pour l'heure, les outils et services socles nationaux se concentrent sur les aspects médicaux et médico-sociaux. L'accès à ces données est régi par une matrice d'habilitation permettant de définir les accès selon les professionnels et ainsi respecter le secret médical.

D'autres outils permettant d'intégrer des informations administratives plus précises ou sociale existent en complément, en IDF la solution Santélien est proposée.