Le règlement européen sur la protection des données personnelles (RGPD), qui est entré en application le 25 mai 2018, procède à une définition large des données de santé.

La protection des données de santé

Avec le DMP ou la carte vitale, les données des patients et des assurés sont transmises à des organismes publics ou à des professionnels de la santé. Ces différents dispositifs obéissent strictement à toutes les recommandations de la Cnil.

La loi Informatique et Libertés dispose que les données de santé sont particulières et **leur traitement est interdit sauf exception particulière l'autorisant.**

La notion de données de santé est désormais large.

Entrent dans cette notion les 3 CATÉGORIES DE DONNÉES DE SANTÉ **:**

1. **Celles qui sont des données de santé par nature :** antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
2. **Celles, qui du fait de leur croisement avec d'autres données**, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la mesure de l'effort, etc.
3. **Celles qui deviennent des données de santé en raison de leur destination**, c'est-à-dire de l'utilisation qui en est faite sur le plan médical.

Mesures juridiques :

Une fois la qualification de données de santé retenue, un régime juridique particulier justifié par la sensibilité des données s'applique. La liste, ci-dessous, propose un aperçu des différentes législations susceptibles de s'appliquer :

- ***Loi Informatique et Libertés (art. 8 et chapitre IX) ;***

Adoptée en France en 1978, établit un cadre juridique pour la protection des données personnelles. L'article 8 de la loi stipule que toute personne a le droit d'accéder et de faire rectifier, compléter, mettre à jour ou supprimer les informations la concernant.

Le chapitre IX de la loi concerne les sanctions en cas de non-respect de la législation.

- ***Dispositions sur le secret (art. L. 1110-4 du CSP) ;***

En résumé, cet article précise que toutes les personnes travaillant dans le domaine de la santé ont l'obligation de respecter le secret médical, qui s'applique à toutes les informations et données médicales relatives à une personne, qu'elles soient confidentielles ou non. Le secret médical ne peut être levé que dans certaines circonstances limitées, comme lorsque la personne concernée donne son consentement, lorsqu'il est nécessaire pour sauver une vie ou pour prévenir un danger grave pour la santé publique, ou encore lorsque la loi l'exige. Cette réglementation a pour objectif de protéger la vie privée et la confidentialité des informations médicales des patients.

- ***Dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du CSP) ;***

Cet article prévoit que les systèmes d'information de santé doivent respecter des référentiels de sécurité et d'interopérabilité, qui sont définis par des autorités compétentes en la matière. Ces référentiels visent à garantir la confidentialité, l'intégrité et la disponibilité des données de santé, ainsi que leur interopérabilité entre les différents systèmes.

Les autorités compétentes peuvent notamment être l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé), qui ont pour mission de définir et de mettre en place ces référentiels.

En somme, cet article vise à encadrer la gestion et l'utilisation des données de santé en France, en s'assurant que les systèmes d'information respectent des

normes de sécurité et d'interopérabilité pour garantir la confidentialité et la qualité de ces données.

- ***Dispositions sur l'hébergement des données de santé (art. L. 1111-8 et R. 1111-8-8 et s. du CSP) ;***

Énonce les règles relatives à la sécurité et la confidentialité des données de santé hébergées par les fournisseurs de services d'hébergement de données de santé.

En vertu de cette disposition, les fournisseurs d'hébergement de données de santé doivent satisfaire à des exigences strictes en matière de sécurité, notamment en matière de stockage, de transmission et d'accès aux données. Ils doivent également être certifiés et accrédités par des organismes compétents et autorisés par le ministère de la Santé.

De plus, les responsables des traitements de données de santé, tels que les professionnels de santé ou les établissements de soins, doivent s'assurer que les fournisseurs d'hébergement de données de santé qu'ils utilisent respectent ces règles de sécurité et de confidentialité.

Enfin, les patients ont le droit d'accéder à leurs propres données de santé, ainsi qu'un droit de rectification et de suppression de ces données.

- ***Dispositions sur la mise à disposition des données de santé (art. L. 1460-1 et s. du CSP)***

A pour objectif de réglementer la collecte, le stockage, la transmission et l'utilisation des données de santé en France

Elle impose aux professionnels de santé et aux établissements de santé de respecter certaines règles pour garantir la confidentialité et la sécurité des données de santé des patients. Elle prévoit également des règles pour la transmission des données de santé entre professionnels de santé et pour la mise à disposition de ces données aux organismes publics.

Enfin, elle établit le rôle de l'Agence nationale de santé publique en matière de gestion et de contrôle de l'utilisation des données de santé.

- ***Interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (art. L. 1111-8 du CSP, art. L 4113-7 du CSP)…***

En résumé, l'article L.1111-8 du Code de la santé publique en France interdit la cession ou l'exploitation commerciale des données de santé sans le consentement préalable de la personne concernée. De même, l'article L.4113-7 du même code interdit aux professionnels de la santé de tirer profit de l'exploitation des données de santé de leurs patients. Ces dispositions visent à protéger la confidentialité des

informations médicales et à prévenir toute utilisation abusive des données de santé à des fins commerciales ou lucratives.

CONSEILS POUR APPORTER UN NIVEAU DE PROTECTION SUPPLÉMENTAIRE AUX DONNÉES DE SANTÉ :

1- Réaliser une analyse d'impact :

L'analyse d'impact permet de comprendre quel type de données peut représenter un impact pour les droits et libertés des patients.

2- Informer le patient de la finalité de ses données :

Cela permet la transparence et le patient comprend pourquoi certaines informations lui sont demandées.

3- Limiter au maximum les informations collectées :

Que ce soit dans le cadre de la prise de rendez-vous ou de consultations, veillez à ce que les informations recueillies soient nécessaire à la finalité du recueil. Moins vous aurez de données à traiter, plus la sécurisation sera simple.

4- Supprimer les informations ayant dépassé la durée de conservation préconisée :

Pour chaque type de données, la CNIL recommande des durées de conservation. Une fois la durée dépassée, supprimez les données qui n'ont plus d'intérêt afin de limiter au maximum le stockage de données. Si vous souhaitez garder les données à des fins statistiques, vous pouvez néanmoins les anonymiser.

5- Vérifier le niveau de sécurité garanti par l'hébergeur de données de santé :

Au cas où vous utilisez un hébergeur de données de santé certifié, vous devez vous assurer que le niveau de sécurisation des données qu'il vous garantit est adéquat. Après vérification, pensez à signer conjointement un contrat en relation avec la sécurisation des données.

6- Utiliser un service de messagerie sécurisée de santé dans le cadre d'échange avec d'autres professionnels de santé :

Si vous utilisez une messagerie électronique classique, assurez-vous que cette dernière soit sécurisée et adaptée à votre utilisation professionnelle. Dans ce cas, il est également nécessaire de chiffrer les pièces jointes afin de garantir la confidentialité des échanges.

7- Sécuriser l'accès à vos appareils digitaux (smartphone, tablette, PC) :

La sécurisation des appareils digitaux par le biais de mots de passe ou autre chiffrement, garantie une mesure de protection de données supplémentaires. Dans le cas de présence de logiciel de dossier patient sur votre téléphone, assurez-vous que l'accès est bien sécurisé. Il est également recommandé de ne pas stocker d'informations de santé relatives ou patients sur le téléphone portable ou la tablette.

8- S'assurer que les recherches menées avec des tiers soient conformes à la réglementation :

Dans le cadre d'une recherche menée de façon conjointe avec des tiers, vous devez vérifier qu'ils mettent également en place des mesures de sécurisation des données de santé.

LA CERTIFICATION DES SERVEURS DEVENUE OBLIGATOIRE :

Les hébergeurs doivent désormais être certifiés « Hébergeur de Données de Santé » ou HDS, par un organisme indépendant**, à l'image de *Bureau Veritas.***

« *Les serveurs sont des points névralgiques de l'échange de données* »

Il est nécessaire de mettre en place une stratégie de sauvegarde de données de santé. Cette dernière doit être composée d'une solution de sauvegarde externalisée, en complément d'une solution de sauvegarde locale.

Mais pourquoi ?

Si un hacker entre dans votre système informatique, il aura facilement accès à vos sauvegardes en local. Les sauvegardes externalisées seront donc votre dernier rempart en cas de perte des sauvegardes locales.
Concernant la sauvegarde externalisée de données de santé, il est nécessaire de faire appel à un fournisseur spécialisé et certifié HDS (Hébergeur de Données de Santé).

À savoir que la certification HDS a remplacé l'agrément HADS. Cette certification est une norme internationale, délivrée par un organisme certificateur pour une durée de 3 ans avec des audits de suivi annuel.

Assurer la confidentialité et la sécurité des données patients

Il existe plusieurs mesures à mettre en place afin d'assurer que les données patients et la communication restent confidentielles et sécurisées :

L'authentification forte :

La CNIL recommande à la plateforme de médecine digitale de mettre en place une méthode d'authentification forte pour protéger les informations confidentielles des patients. Cela implique l'utilisation d'identifiants uniques et de mots de passe forts, ainsi que l'activation de l'authentification multifacteur. Les informations d'identification ne doivent jamais être stockées dans un endroit non sécurisé et un dispositif de gestion des habilitations des utilisateurs doit être mis en place pour limiter l'accès aux données strictement nécessaires. Différents niveaux d'habilitation doivent être créés en fonction des besoins.

Chiffrement de bout en bout :

Une plate-forme de médecine digitale doit utiliser un cryptage de bout en bout pour assurer la confidentialité et la sécurité des données des patients. Seules les parties autorisées peuvent participer à la communication, et les parties non autorisées ne pourront pas écouter ou intercepter les informations échangées entre les parties.

Garder un poste de travail propre :

Les prestataires de soins et les patients doivent garder une machine propre. Qu'il s'agisse d'un ordinateur portable, d'un appareil mobile, d'un ordinateur de bureau, le poste de travail doit disposer d'un système d'exploitation et d'applications les plus récents. En outre, les réseaux **Wi-Fi publics ne doivent jamais être utilisés** pour échanger des informations sensibles, telles que les données patients, ou effectuer une téléconsultation.

Eviter le phishing :

Très courant, le phishing est la principale cause d'incidents de sécurité importants. Les prestataires en soins de santé, ainsi que les patients, reçoivent de

gros volumes d'e-mails de phishing. Ces e-mails sont conçus pour **obtenir des informations sensibles** de la part du destinataire. Ils peuvent inclure une **pièce jointe malveillante** et/ou un lien destiné à infecter la machine du destinataire avec un logiciel malveillant. Dans les deux cas, ils doivent être ignorés et supprimés.

Poser un cadre restrictif :

Mettre en place des mesures restrictives pour les échanges avec les patients, en évitant autant que possible l'utilisation de canaux non sécurisés, en informant les patients des canaux de communication sûrs et en précisant les délais et la nature des questions ou des demandes. Il est également recommandé de préciser que pour toute urgence, les patients doivent s'adresser au SAMU ou à une structure compétente, et de toujours vérifier l'identité de la personne avec qui vous communiquez

> ***La solution Hellocare Pro, agréée et sécurisée, vous permet de communiquer en toute sécurité et confidentialité avec vos patients. Toutes les données patients, ainsi que les documents médicaux (comme les ordonnances) sont protégés conformément à la loi.***

La solution Hellocare Pro :

Hellocare Connect. Il vous suffit de prendre rendez-vous avec lui comme d'habitude, et de spécifier qu'il s'agit d'une consultation en ligne. Le médecin, après avoir créé la proposition de rendez-vous, vous envoie une invitation à vous connecter qui contient la date et l'heure du rendez-vous.

HEALTH DATA HUB :

La protection des données de santé est une question cruciale pour le Health Data Hub. Voici quelques conseils pour aider à protéger les données stockées sur cette plateforme :

1. Mettre en place des contrôles d'accès rigoureux : Il est important de limiter l'accès aux données de santé aux seules personnes autorisées à les consulter. Utilisez des mots de passe forts, des politiques de sécurité strictes et une authentification à deux facteurs pour protéger les accès.

2. Chiffrer les données stockées : Utilisez des algorithmes de chiffrement forts pour protéger les données stockées contre les accès non autorisés. Les données stockées doivent être chiffrées au repos et en transit.

3. Appliquer des mises à jour de sécurité régulières : Assurez-vous que tous les logiciels et systèmes utilisés sur la plateforme sont régulièrement mis à jour avec les derniers correctifs de sécurité.

4. Surveiller en permanence la plateforme : Utilisez des outils de surveillance de sécurité pour surveiller les activités suspectes et les tentatives d'accès non autorisées.

5. Sensibiliser les utilisateurs : Éduquez les utilisateurs sur les risques de sécurité et les meilleures pratiques à suivre pour protéger les données de santé. Faites des formations sur les risques, les comportements à éviter, etc.

6. Établir des politiques de sécurité claires : Mettez en place des politiques de sécurité claires et strictes pour définir les pratiques à suivre en matière de sécurité des données. Faites des campagnes de sensibilisation et de communication pour que les utilisateurs respectent ces politiques.

En somme, pour protéger les données de santé stockées sur le Health Data Hub, il est essentiel de mettre en place des mesures de sécurité robustes, de surveiller constamment la plateforme, de sensibiliser les utilisateurs et d'établir des politiques de sécurité claires et strictes.