Financé par l'Union européenne
NextGenerationEU

Cyber sécurité et RGPD pour les libéraux

Lundi 6 février 2023

l'Assurance Maladie
Agir ensemble, protéger chacun

sesan
SERVICE NUMÉRIQUE DE SANTÉ

AIUF
ASSOCIATION INTER-URPS FRANCILIENNE

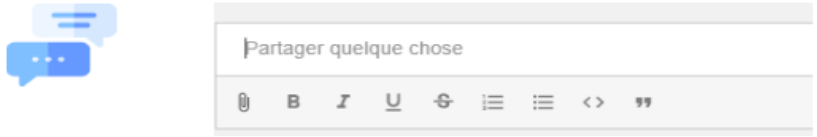
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

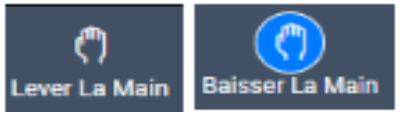
Informations pratiques

Bonnes pratiques de participation au webinaire

- Les questions doivent être posées par écrit, j'utilise le chat en bas de l'écran pour rebondir, poser mes questions ou commenter. Une réponse concise/synthétique sera effectuée à l'oral. Si besoin un retour dédié sera fait par email ou par une prise de contact.



- Si vous souhaitez compléter oralement, levez la main et la parole vous sera donnée.



Mise en ligne de l'enregistrement vidéo de la session : suivez le lien fourni ultérieurement

Introduction

Association Inter-URPS Francilienne (AIUF)

Assurance Maladie (DCGDR)

Ordre du jour

Première partie – Cybersécurité pour les professionnels de santé de ville 5

- Contexte en matière de cybersécurité
- Bonnes pratiques pour limiter les risques de cyber-attaque en ville
- Quelles conséquences en cas de cyber-attaque et comment réagir?

Deuxième partie – RGPD et utilisation des données par les professionnels de santé

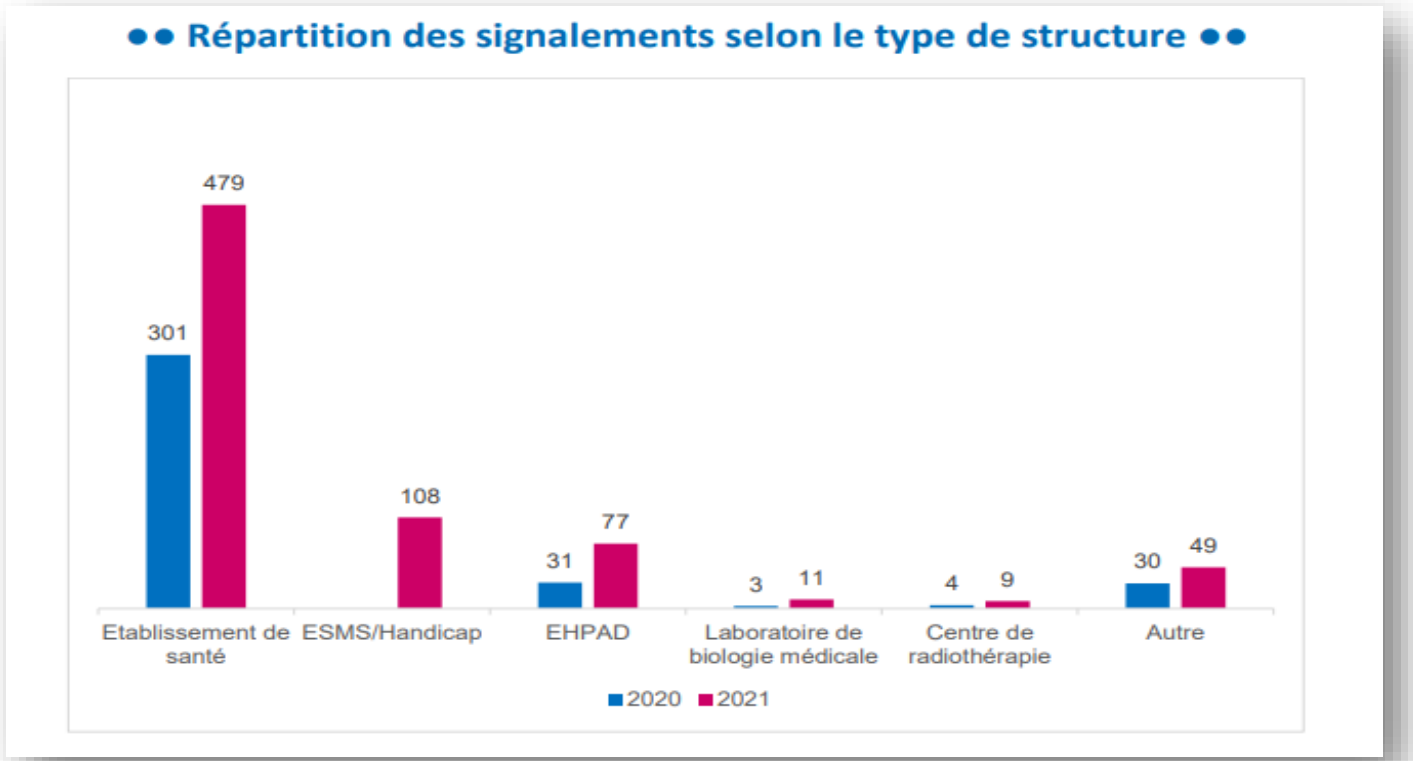
- Qu'est-ce-que le RGPD? Quel impact pour les professionnels de santé libéraux?
- Information des patients 21
- Règles relatives à la conservation et à la transmission des données personnelles

Première partie – Cybersécurité pour les professionnels de santé de ville

Contexte en matière de cybersécurité

Contexte

Incidents SI Santé – quelques chiffres à l'échelle nationale



La majorité (65%) des incidents de sécurité est déclarée par les établissements de santé. Cependant, elle baisse au profit d'une nette augmentation des déclarations issues des établissements et services médico-sociaux (25% au lieu de 8% en 2020).

La catégorie « Autre » est en augmentation en 2021 et correspond à des déclarations réalisées par des **cabinets libéraux ou des GRADeS**.

A noter notamment des attaques en augmentation vers les cabinets dentaires.

Contexte

Incidents SI Santé – les impacts pour les professionnels de santé libéraux

Les incidents cyber peuvent avoir des impacts très lourds pour les PSL :

- Risques sur la **prise en charge des patients**
  - Désorganisation du cabinet avec une indisponibilité des rendez-vous, une absence d'accès aux bases de données,
  - Perte d'informations médicales sur un patient avec impact possible sur la prise en charge,
  - Possible modification d'informations médicales de patients,

- Risque de fuite de données et donc **risque juridique** majeur pour le cabinet
  - En application du RGPD, une déclaration initiale de l'incident doit être faite à la CNIL dans les 72 heures,
  - A noter : la CNIL a été amené à sanctionner des professionnels de santé sur ce point.

Bonnes pratiques pour limiter les risques de cyber-attaque en ville

Bonnes pratiques

Cybersécurité - les bonnes pratiques à adopter

https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/

Bonnes pratiques

Memento de sécurité

Financé par l'Union européenne NextGenerationEU

Ce mémento élaboré par l'ANS rassemble **les règles d'hygiène informatique** de base ne nécessitant pas de connaissance technique approfondie, à l'usage des professionnels de santé libéraux. Il contient.

- Une checklist de mesures d'hygiène numérique
- Des recommandations de sécurité

Mesure d'hygiène informatique	L	C	Voir chapitre…	OK ? (Oui/Non)
Maîtriser l'accès physique au lieu d'exercice	X		2.2.1	
Maîtriser la sécurité physique des équipements informatiques				
Assurer la protection de l'alimentation électrique des équipements informatiques (*prise parafoudre et parasurtenseur, onduleur…*)	X		2.2.2	
Ne pas laisser accessibles au public les équipements informatiques	X		2.2.2	
Être vigilant sur la protection des supports de stockage de données amovibles *(ne pas les laisser connectés à l'ordinateur ni sur une table entre les utilisations, les ranger…)*	X		2.2.2	
Assurer la protection des équipements informatiques mobiles (*utiliser un câble de sécurité pour les accrocher ou les ranger entre les usages*)	X	X	2.2.2	
Protéger le poste de travail et l'accès aux applications				
Respecter les règles de sécurité pour l'utilisation des cartes de type CPx et e-CPS (*garder le code PIN secret, garder la carte à portée de main ou la ranger entre les usages*)	X	X	2.3.1	
Utiliser des mots de passe robustes (*minimum 12 caractères de types variés, pas de mot du dictionnaire ou en lien avec vous, construit par exemple à partir d'un texte que vous connaissez selon une méthode que vous vous fixez*)	X	X	2.3.2	
Utiliser un gestionnaire de mots de passe (*pour conserver facilement et de façon sécurisée un mot de passe différent, même très complexe, par application*)	X	X	2.3.2	

L : stockage local

C : Stockage cloud

Voir chapitre… : Recommandation détaillée

Ok? : Etat de la mesure

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Bonnes pratiques

Par catégorie

Mails et réseaux sociaux

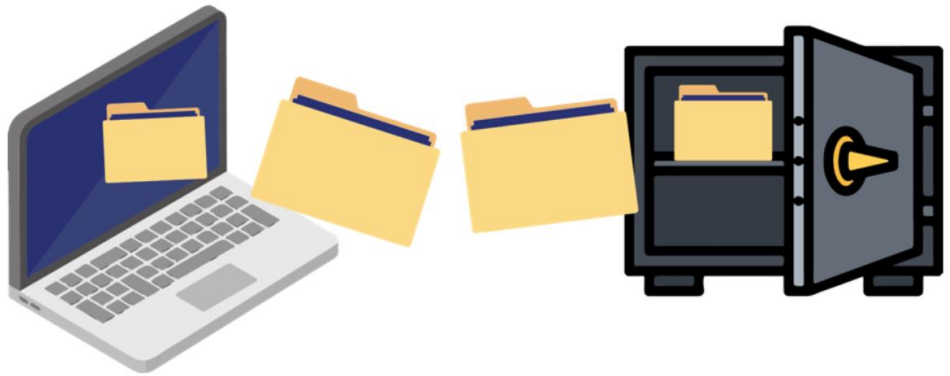
1. **Evitez d'ouvrir les pièces jointes, les liens contenus dans les mails** suspects (demande de virement, demande urgente, …)
2. **Vérifier l'identité des expéditeurs**
3. **Evitez de cliquer sur les liens raccourcis** (site, réseaux sociaux,..)
4. **Vérifier toujours l'origine des demandes d'informations personnelles et confidentielles** par mail, sms, ou téléphoniques
5. **Utiliser une Messagerie Sécurisée de Santé (MSSanté)** pour échanger des informations/données médicales avec d'autres professionnels de santé

Bonnes pratiques

Par catégorie

Sauvegardes

1. **Effectuer régulièrement des sauvegardes** de vos données en utilisant **des supports externes** dédiés à cet usage
2. Placer tous les supports de stockage amovibles **dans un coffre-fort ou dans une armoire à clé**

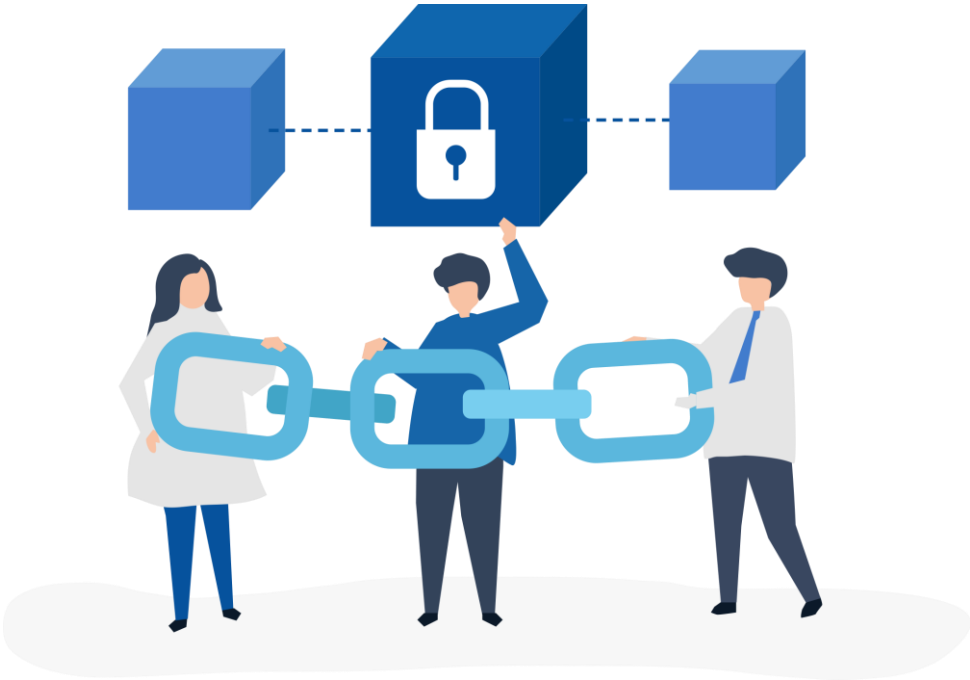


Bonnes pratiques

Par catégorie

Dispositifs techniques

1. **Installer et mettre à jour régulièrement un antivirus** supporté par son éditeur, non téléchargé gratuitement sur Internet
2. **Installer un pare-feu** sur votre poste de travail et le maintenir à jour
3. **Chiffrer les données sensibles** (dossiers médicaux…) en utilisant un logiciel de chiffrement adapté
4. **Mettre à jour le système d'exploitation** et les applications



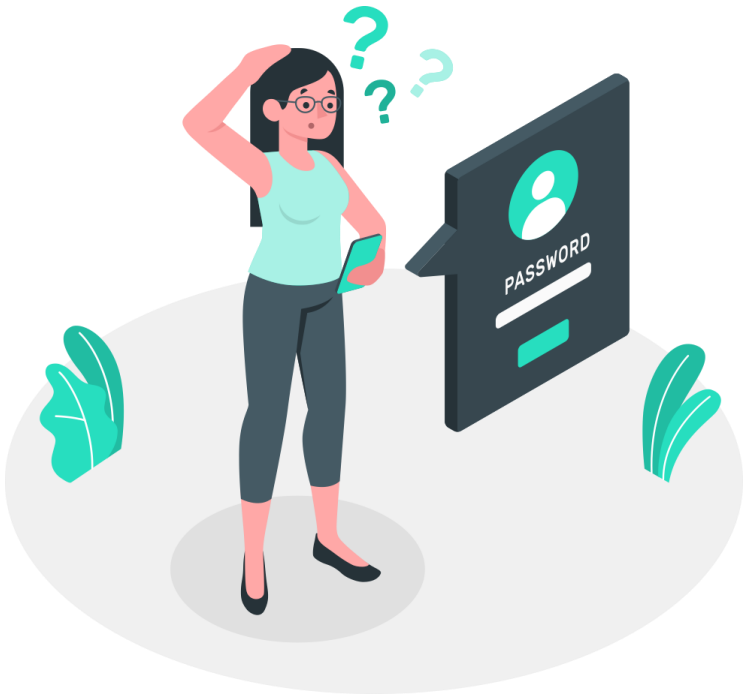
Bonnes pratiques

Par catégorie

Financé par l'Union européenne NextGenerationEU

Accès et mot de passe

1. **Choisir un mot de passe complexe, non lié à votre identité** (nom, prénom, date de naissance…) composé de lettres majuscules, lettres minuscules et caractères spéciaux et différents pour chaque usage.
2. Utiliser **l'authentification à facteurs multiples** quand cela est possible.
3. **Refuser systématiquement la mémorisation** de votre mot de passe sur les sites, privilégiez l'enregistrement sur un coffre-fort numérique certifié.
4. **Sécuriser l'accès à votre wifi** via un mot de passe complexe.
5. **Gérer les droits d'accès et limiter les accès** aux fichiers et aux documents à caractère confidentiel et au contenu sensible



Quelles conséquences en cas de cyber-attaque et comment réagir?

Comment réagir en cas de cyber-attaque

Généralités

Quels sont les premiers gestes à adopter face à une cyber-attaque ?

- Ne jamais communiquer avec les hackers (ni par mail, ni par téléphone).
- Ne jamais leur verser d'argent en cas de *rançongiciel.* En effet, rien ne garantit que vous pourrez accéder de nouveau à vos données sensibles.

En cas d'activité anormale de votre ordinateur ou de votre serveur :

- Ne pas du reste éteindre l'ordinateur, pour éviter au logiciel malveillant d'effectuer des modifications importantes et irréversibles de votre système,
- Déconnecter vos ordinateurs d'internet, en coupant votre réseau Wi-Fi ou en débranchant le câble de connexion au réseau,
- Déconnecter votre appareil du réseau pour éviter une propagation à d'autres ordinateurs,
- Lancer une analyse de votre poste avec un logiciel de sécurité (anti-virus, anti-malware…),
- Effectuer une copie du disque dur de votre ordinateur afin de conserver une preuve exploitable dans le cadre d'éventuelles poursuites judiciaires.

Comment réagir en cas de cyber-attaque

Généralités

Vers quels organismes et services dédiés à la lutte contre la cybercriminalité se tourner pour se faire aider ?

- **L'Agence Nationale de la Sécurité des Systèmes d'information *(ANSSI)*** chargée de proposer des règles en matière de protection des systèmes d'information de l'Etat. Elle assure également un service de veille et de détection des attaques informatiques et conseille les entreprises privées pour la sécurisation de leurs systèmes d'information : https://www.ssi.gouv.fr/

- **La plateforme nationale d'assistance aux victimes d'actes de cybermalveillance** où vous trouverez :
  - Des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
  - Des services de proximité en cas de dommages causés par une attaque informatique. Pour en savoir plus : https://www.cybermalveillance.gouv.fr/

Déposer plainte

Il existe en France un arsenal législatif permettant de poursuivre les auteurs de cybercrime.
En cas de cyberattaque, il est nécessaire de déposer plainte, soit auprès des autorités compétentes (Gendarmerie Nationale, Police Nationale), soit en écrivant directement au Procureur de la République du tribunal judiciaire dont vous dépendez et de tenir à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.

Bon à savoir : en cas de cyberattaque avec violation de données à caractère personnel, le Règlement Général sur la Protection des Données (RGPD), entré en application en France depuis le 25 mai 2018, impose à toute entreprise de notifier l'incident à la CNIL dans les 72 heures.

Comment réagir en cas de cyber-attaque

Attaque ou piratage du compte d'accès à Ameli-Pro

Financé par l'Union européenne NextGenerationEU

Surveillance par l'Assurance Maladie des accès ou des activités atypiques Ameli-Pro :

- En cas d'une suspicion de compromission du compte Ameli-Pro (tentative d'accès frauduleux), l'Assurance Maladie met en œuvre les actions suivantes :
  - Mise hors fonctionnement du mot de passe du compte amelipro
  - Prise de contact avec le professionnel concerné pour :
    - Vous informer qu'une activité suspecte a été constatée sur son compte et l'inviter à vérifier si les soupçons sont confirmés.
    - Vous informer qu'une notification a été effectuée par la Cnam auprès de la Commission nationale de l'informatique et des libertés (CNIL) conformément à nos obligations en matière de protection des données (RGPD).
    - Vous indiquer la marche à suivre pour accéder à nouveau au compte Ameli-pro et aux données :
      - Utiliser la fonction *Mot de passe oublié* et de surveiller l'arrivée du message « Réinitialiser votre mot de passe amelipro » dans votre boîte mail, pour créer un nouveau mot de passe.
      - + des conseils en termes de bonnes pratiques notamment d'utiliser un mot de passe spécifique pour accéder à amelipro (différents de ceux utilisés sur d'autres site/comptes)

Actions conseillées pour limiter les risques :

- Surveiller régulièrement l'activité sur votre compte
  - en allant sur *Gestion de compte* (en haut à droite du portail amelipro) puis *Mon compte*, puis *Consulter mes derniers évènements* dans la rubrique *Connexion et sécurité*.
    - Les dates et heures des dernières connexions à votre compte y sont notifiées.
  - Si vous décelez une activité suspecte, n'hésitez pas à :
    - modifier votre mot de passe
    - ou appeler l'assistance technique amelipro au 3608.

Financé par l'Union européenne NextGenerationEU

Avez-vous des questions ?

Deuxième partie – RGPD et utilisation des données par les professionnels de santé

Qu'est-ce-que le RGPD?

Quel impact pour les professionnels de santé libéraux?

Qu'est-ce que le RGPD et pourquoi vous êtes concerné?

Définitions

Le Règlement général sur la protection des données personnelles (RGPD), adopté au niveau européen, est entré en application le 25 mai 2018 et s'applique à toute organisation, publique et privée, quels que soient sa taille (entreprise, ministère, administration, collectivité, association, etc.).

En tant que **professionnel de santé libéral**, vous êtes amené à **recevoir ou à émettre des informations sur vos patients** pour assurer leur suivi que ce soit dans le **dossier « patient » (papier ou informatique),** dans le cadre de l'utilisation d'une plateforme en ligne de gestion des rendez-vous ou encore de la réalisation d'actes de télésanté. De manière plus globale, **vous collectez également des informations pour gérer votre cabinet** (ex : gestion des fournisseurs, des personnels que vous employez, etc.). Ces informations que vous recevez et / ou émettez, à l'occasion de votre activité professionnelle, **sont considérées comme des données personnelles**.

Le RGPD définit les données personnelles comme **« toute information se rapportant à une personne physique identifiée ou identifiable »**

Une personne peut être identifiée : **directement** (exemple : nom, prénom) **ou indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique

L'identification d'une personne physique peut être réalisée : **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN) ou **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

RGPD et professionnels de santé libéraux : ce que vous devez savoir (1/2)

En pratique

1. **Les dispositions du RGPD s'appliquent-ils uniquement à vos traitements informatiques (ex : logiciel utilisé pour le suivi de vos patients) et pas à vos dossiers papiers ?**

Les dispositions du RGPD s'appliquent à tous les traitements de données personnelles *(ex : nom, prénom, numéro de patient, etc.)* que vous utilisez pour l'exercice de votre activité professionnelle, que ces traitements soient sous une forme informatique *(ex : logiciel de gestion de votre cabinet médical, logiciel utilisé pour l'exploitation de votre pharmacie, de votre cabinet d'orthophonie, pour l'exploitation de votre laboratoire de biologie médicale, etc.)* ou papier *(ex : dossier patient papier)*.

2. **Quelles informations sur les patients pouvez-vous collecter ?**

Les données que vous collectez sur les patients doivent être **adéquates, pertinentes et limitées** à ce qui est strictement nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.
A titre d'exemple, la collecte d'informations sur la vie familiale d'un patient n'est en principe pas appropriée.

RGPD et professionnels de santé libéraux : ce que vous devez savoir (1/2)

En pratique

Financé par l'Union européenne NextGenerationEU

3. Pouvez-vous transmettre les données de vos patients à tous les professionnels, organismes ou autorités qui vous les demandent ?

Vous devez limiter l'accès aux données de santé de vos patients : seules certaines personnes sont autorisées, au regard de leurs missions, à accéder à celles-ci *(ex : équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, secrétaire médicale, organismes d'assurance maladie pour le remboursement des actes et prestations et leur contrôle, etc.)*. Ces personnes n'accèdent qu'aux données nécessaires à l'exercice de leur mission *(ex : le secrétaire médical accède aux données administratives permettant de gérer les prises de rendez-vous, mais n'accède pas à la totalité du dossier médical)*.
Par ailleurs, la loi peut autoriser certains tiers à avoir accès aux données de vos patients *(ex : les organismes de sécurité sociale dans le cadre de la lutte contre la fraude, etc.)*.

4. Combien de temps pouvez-vous conserver les données que vous collectez sur vos patients ?

Les données que vous collectez sur vos patients doivent être **conservées pour une durée déterminée**.

RGPD et professionnels de santé libéraux : ce que vous devez savoir (2/2)

En pratique

Financé par l'Union européenne NextGenerationEU

5. Etes-vous responsable de la mise en place de mesures de sécurité pour garantir le respect de la confidentialité des données de santé de vos patients ?

Vous devez respecter des règles de sécurité pour protéger les données des patients contre des accès non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle. Pour ce faire vous devez **mettre en place des mesures techniques et organisationnelles** appropriées pour préserver la confidentialité et l'intégrité des données *(ex : utilisation de la carte professionnel de santé, mot de passe personnel, utilisation d'un système de chiffrement fort en cas d'utilisation d'internet, etc.)*.

6. Devez-vous toujours déclarer les traitements de données personnelles auprès de la CNIL ?

Avec l'entrée en application du RGPD, **vous n'avez plus de formalité à accomplir auprès de la CNIL** pour les traitements de données personnelles nécessaires à la gestion de votre activité (cabinet médical, d'infirmiers, d'orthophonistes, laboratoire de biologie médicale, officine pharmaceutique, opticien, etc.).
En revanche, **vous devez être en mesure de démontrer à tout moment votre conformité aux exigences du RGPD en traçant toutes les démarches entreprises** : mise en place d'un registre recensant vos fichiers, modalités de l'information délivrée au patient, actions menées pour garantir la sécurité des données de santé, etc.

RGPD et professionnels de santé libéraux : ce que vous devez savoir (2/2)

En pratique

Financé par l'Union européenne NextGenerationEU

7. Êtes-vous obligé de désigner un délégué à la protection des données (DPO) ?

Dès lors que vous exercez à titre individuel, vous n'êtes pas soumis à l'obligation de désigner un DPO.

Néanmoins, si en raison de votre activité, vous estimez que vous traitez des données de santé à grande échelle (ex : exercice au sein d'un réseau de professionnels, maisons de santé, centre de santé, dossiers partagés entre plusieurs professionnels de santé, etc.), vous devez soit désigner un DPO en interne, soit solliciter les services d'un DPO externe (consultants, cabinets d'avocats, etc.).

Pour en savoir plus, vous pouvez consulter la fiche thématique « Devenir délégué à la protection des données ».

Information des patients

RGPD et information des patients

Vous devez délivrer aux patients une **information portant sur le traitement de données que vous effectuez pour leur prise en charge** *(soit dans votre logiciel de suivi, soit dans votre dossier papier)*.

Le support d'information est libre :

- par oral,
- par écrit
- ou par tout autre moyen (affichage dans les lieux de soins, dans les secrétariats, remise de documents écrits d'information, etc.).

Cela peut être sous la forme d'une affiche, dans votre salle d'attente.

Vous n'avez pas besoin de recueillir le consentement des patients pour collecter et conserver les données de santé les concernant, dans la mesure où leur collecte et leur conservation sont nécessaires aux diagnostics médicaux et à la prise en charge sanitaire ou sociale des patients concernés.
Le consentement pour le traitement de données ne doit pas être confondu avec le consentement requis pour la réalisation de certains actes médicaux *(ex : le code de la santé publique impose le recueil du consentement du patient pour la réalisation d'un examen des caractéristiques génétiques).*

Lien vers la page de la CNIL dédiée : https://www.cnil.fr/fr/traitement-de-donnees-de-sante-comment-informer-les-personnes-concernees

Règles relatives à la conservation et à la transmission des données personnelles

Règles relatives à la conservation et à la transmission des données personnelles

Combien de temps pouvez-vous conserver les données que vous collectez sur vos patients ?

Les données que vous collectez sur vos patients doivent être conservées pour une durée déterminée.

A titre d'exemple, les médecins libéraux conservent, conformément aux recommandations du Conseil national de l'Ordre des médecins, les dossiers médicaux des patients pendant 20 ans à compter de leur dernière consultation.

Pouvez-vous transmettre les données de vos patients à tous les professionnels, organismes ou autorités qui vous les demandent ?

Vous devez limiter l'accès aux données de santé de vos patients : seules certaines personnes sont autorisées, au regard de leurs missions, à accéder à celles-ci (ex : équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, secrétaire médicale, organismes d'assurance maladie pour le remboursement des actes et prestations et leur contrôle, etc.).
Ces personnes n'accèdent qu'aux données nécessaires à l'exercice de leur mission (ex : le secrétaire médical accède aux données administratives permettant de gérer les prises de rendez-vous, mais n'accède pas à la totalité du dossier médical).

Par ailleurs, la loi peut autoriser certains tiers à avoir accès aux données de vos patients (ex : les organismes de sécurité sociale dans le cadre de la lutte contre la fraude, etc.).

Financé par l'Union européenne NextGenerationEU

Avez-vous des questions ?

Ressources disponibles

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

- Guide pratique sur la protection des données à l'usage des professionnels libéraux
- Guide sur la sécurité des données personnelles

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

- Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

sesan
SERVICE NUMÉRIQUE DE SANTÉ

- Les bonnes pratiques de sécurité

Financé par l'Union européenne NextGenerationEU

MERCI DE VOTRE ATTENTION

Financé par l'Union européenne
NextGenerationEU