Protection des données & cybersécurité - RGPD

Rédacteurs : jdelmas@urpslrmp.org

Les obligations du médecin libéral en matière de protection des données et de cybersécurité sont nombreuses et visent à garantir la confidentialité, la sécurité et la transparence dans le traitement des données des patients.

Elles sont principalement encadrées par le **Règlement Général sur la Protection des Données (RGPD)** et des réglementations spécifiques au secteur de la santé, telles que le **Code de la santé publique (CSP)**. Les dispositions du CSP imposent que le secret médical couvre à la fois les **données physiques et numériques des patients.**

Ces textes insistent sur la confidentialité des informations de santé, quelle que soit la forme sous laquelle elles sont conservées ou transmises et renforcent l'obligation de sécuriser ces informations lorsqu'elles sont hébergées ou partagées numériquement.

I Les données et leur protection

En tant que médecin libéral, vous traitez des informations sur vos patients pour assurer leur suivi, que ce soit dans des dossiers (papier ou informatique), via des plateformes de gestion des rendez-vous ou lors d'actes de télémédecine. Vous collectez également des données pour la gestion de votre cabinet, telles que la gestion des fournisseurs et du personnel.

Toutes ces informations sont considérées comme des données et toute action les concernant est considérée comme un « traitement ». Vous êtes donc **le responsable de traitement** de ces données, vous devez être conforme avec le RGPD.

Si vous conservez vos dossiers sous format papier, vous devez également vous assurer de leur sécurité avec des locaux sécurisés et des meubles pouvant se fermer à clé.

1 – Les données et leur traitement

Données personnelles ou à caractère personnel

C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement. Peu importe que ces informations soient confidentielles ou publiques.
Exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, une adresse IP, un identifiant de connexion informatique, etc.

Données de santé

Ce 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.

3 catégories :

- Les données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- Celles, qui croisées avec d'autres données, deviennent des données de santé car elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne.
- Celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Traitement de données

C'est toute opération portant sur des données personnelles et de santé, quel que soit le procédé utilisé, que cela touche des fichiers papiers ou numériques.

Exemple : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction des données.

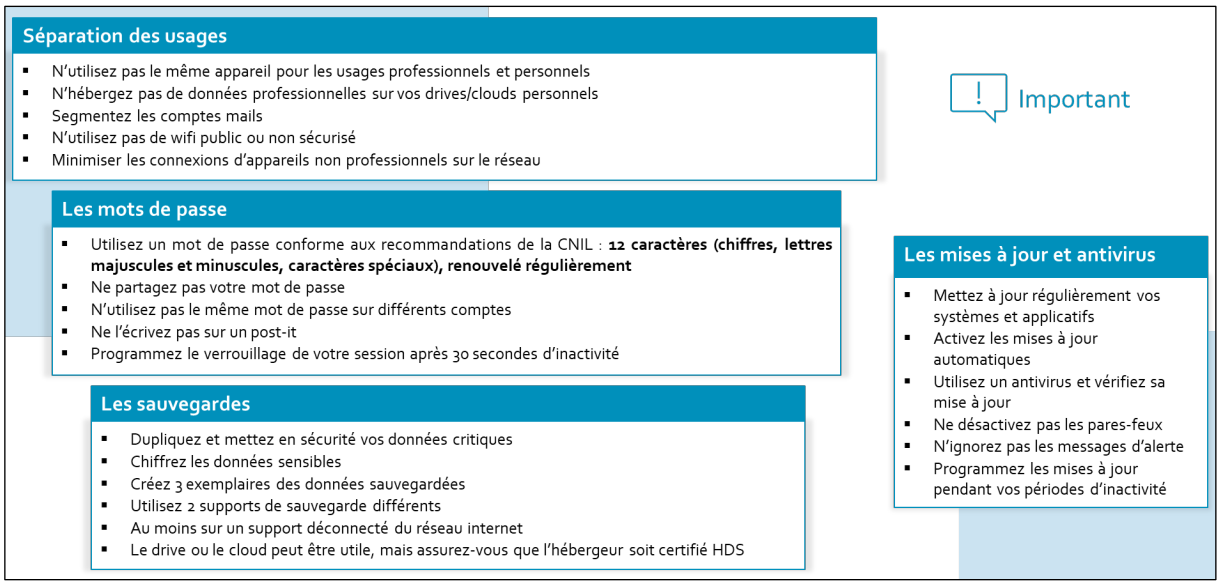
Attention : un traitement n'est pas uniquement un fichier ou une base de données. Il peut s'agir aussi d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc.

A savoir :
S'il est possible par recoupement de plusieurs informations d'identifier une personne, les données sont toujours considérées comme personnelles.

2 – Les principes d'hygiène informatique de base à appliquer

Dans le cadre de l'exercice quotidien de votre activité de médecin libéral, vous vous appuyez désormais sur des outils informatiques (ordinateurs, messageries, tablettes, smartphones, etc.). Ces usages vous exposent à des incidents de sécurité qui peuvent impacter votre activité de façon sévère.
Les principes listés ci-dessous ne requièrent aucune connaissance technique pour être mis en œuvre et visent à renforcer la sécurité de vos outils et système informatiques.

Illustration 1 : Les recommandations pour la sécurisation du système informatique



3 – Les règles à appliquer au regard de votre pratique professionnelle

Pour être en conformité avec le RGPD, le traitement de données doit obéir aux principes suivants : le **traitement doit être licite, transparent, proportionnel, pertinent, temporaire et sécurisé**. Il doit également avoir une finalité : **le responsable du traitement doit définir l'objectif poursuivi par la collecte des données.**
Pour garantir la sécurisation de vos données de santé, suivre certaines recommandations, qui, si elles sont appliquées de façon stricte et régulière, peuvent vous permettre de vous prémunir contre la majorité des attaques informatiques ou à défaut d'en limiter les impacts.

Illustration 2 : Les bonnes pratiques à respecter pour les dossiers patients et les prises de rendez-vous

Général	
▪ Tenir un registre à jour de ses « traitements » : Accès au modèle de registre de la CNIL ▪ Informer les patients et s'assurer du respect de leurs droits : Accès au modèle de notice d'information aux patients pour votre cabinet médical en page 27	
Dossier des patients	**Prise de rendez-vous**
▪ Limiter les informations collectées au nécessaire et utiliser les dossiers patients conformément aux finalités définies (ex : suivi des patients). ▪ Supprimer les dossiers patients et de manière générale toute information ayant dépassé la durée de conservation préconisée.	▪ Limiter les informations collectées par le secrétariat ou par le prestataire à qui est confié la prise de rendez-vous, notamment le motif de la consultation si la consultation ne nécessite pas de préparation. ▪ Vérifier la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance.

Les durées de conservation préconisées des données

- Double des feuilles de soins **: 3 mois** ;
- Dossier patient : **20 ans** à compter de la date de la dernière consultation du patient ;
- Si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations doit être prolongée jusqu'à cette date ;
- Si le patient décède moins de 10 ans après sa dernière consultation, ses informations doivent être conservées pendant **10 ans à compter de la date du décès** ;
- Données relatives à la prise de rendez-vous : suppression dès qu'elles ne sont plus nécessaires. Cette durée doit être pensée en fonction de votre activité, sachant que les dates des examens et consultations médicaux sont, de toute manière, inscrites dans les dossiers de vos patients.
- En cas d'action tendant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais de conservation.

Illustration 3 : Les recommandations quant aux outils numériques utilisés dans la pratique

Messagerie Electronique

Utilisation d'un service de messagerie sécurisée de santé pour les échanges avec d'autres professionnels de santé
Si utilisation de messagerie électronique standard ou messageries instantanées, qui ne garantissent pas la confidentialité des messages : ▪ S'assurer que ces messageries sont bien sécurisées et adaptées à l'utilisation professionnelle ; ▪ Chiffrer les pièces jointes, le cas échéant ; ▪ A défaut, aucune information relative à un patient ou à un professionnel de santé intervenant dans sa prise en charge ne peut être échangée.

Supports mobiles (clés USB, disque dur externe)

Utilisation fortement déconseillée
Si malgré tout, leur utilisation est nécessaire, il convient de chiffrer les données sensibles qui y sont conservées.

Téléphones et tablettes

Sécurisation de l'accès à son téléphone ou à sa tablette et à son contenu (mot de passe, chiffrement, etc.) et de l'accès au logiciel de dossiers-patients sur le téléphone portable ou la tablette
▪ Aucun stockage d'informations médicales relatives aux patients sur le téléphone portable ou la tablette ; ▪ Consultation du logiciel de dossiers-patients avec précaution.

Télémédecine

Vérification de la conformité avec la règlementation du prestataire choisi
▪ Contrôle que le patient est informé de la conformité ; ▪ Vérification de la présence des mentions obligatoires dans le contrat du prestataire.

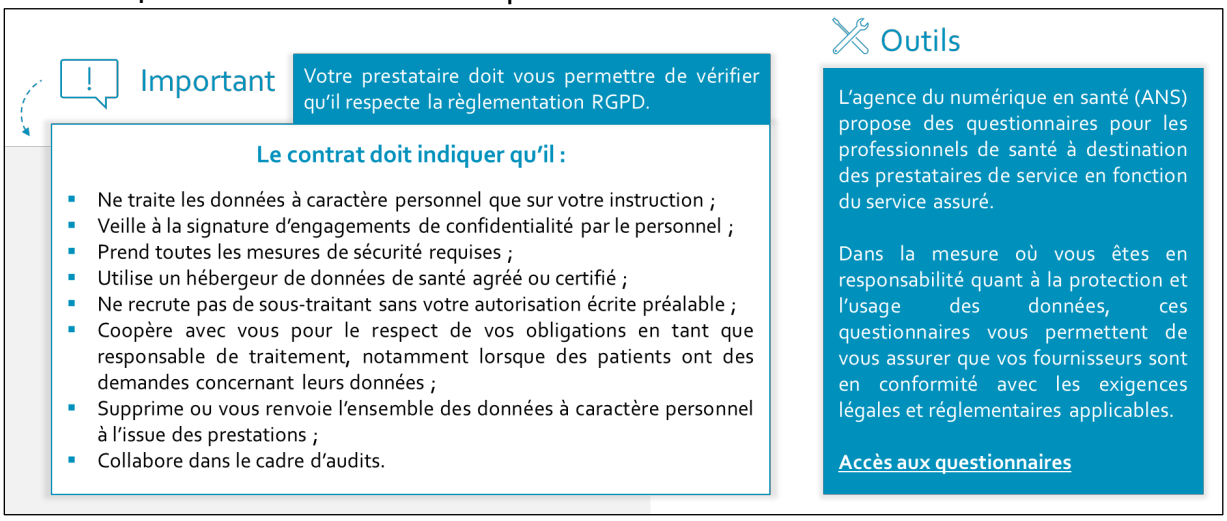
Les outils utiles faisant partie du socle interministériel de logiciels libres (SILL)

- **Chiffrement de données** : **7-zip** est un logiciel gratuit d'archivage de données. Il permet de chiffrer les données lors de la création d'une archive. Il est important de choisir AES comme méthode de chiffrement et de saisir un mot de passe robuste. Accès à la page de téléchargement de 7-zip.

- **Gestion des mots de passe** : **Keepass** est un exemple de gestionnaire de mots de passe open source faisant partie du socle interministériel de logiciels libres (SILL) et dont la sécurité a été évaluée par l'ANSSI. Accès à la page de téléchargement de Keepass.

Les recommandations quant à la télémédecine

Illustration 4 : Les mentions recommandées pour un contrat de télémédecine – RGPD



Pour en savoir plus : outils complémentaires :
- Accès au guide pratique sur la protection des données personnelles – CNOM & CNIL
- Accès au mémento de sécurité informatique pour les professionnels de santé de l'ANS

Votre carte de professionnel de santé (CPS)

La carte CPS est votre carte d'identité professionnelle électronique. Elle vous permet d'attester de votre identité et de vos qualifications professionnelles et de façon générale, **de sécuriser les échanges des données de santé à caractère personnel.**

La CPS permet de multiples usages

- Transmettre les feuilles de soins électroniques ;
- Utiliser les messageries sécurisées de professionnels de santé (MSSanté) ;
- **Identifier via le processus d'authentification forte ;**
- Apposer une signature électronique ;
- Sécuriser les accès physiques (locaux, restaurant, parking…) dans les structures de santé ;
- Renforcer la sécurité des accès aux logiciels utilisés par le professionnel de santé ;
- Créer, alimenter et consulter le dossier médical partagé ou DMP ;
- Accéder aux autres téléservices nationaux contenant des données de santé, tel que le téléservice INSi ;
- Accéder à des plateformes régionales proposant des espaces collaboratifs destinés aux professionnels de santé.

Vigilances avec votre carte CPS

La CPS doit rester strictement personnelle. En aucun cas, vous ne pouvez communiquer vos codes secrets à votre personnel (ex : secrétaire médicale). Vous pouvez mettre en place une authentification forte pour votre personnel au moyen d'un mot de passe à usage unique par exemple (identifiant, mot de passe et envoi d'un code à chaque connexion) ou au moyen d'une Carte de personnel d'établissement (CPE) à demander à votre Caisse primaire d'assurance maladie. Si votre logiciel gérant vos dossiers « patients » est accessible à distance et est hébergé par un prestataire, vous devez vous assurer que ce tiers ou son sous-traitant est agréé ou certifié pour l'hébergement des données de santé (HDS)

Vos obligations auprès de la Commission Nationale de l'Informatique et des libertés (CNIL)

En cas de contrôle par la CNIL, il est demandé de pouvoir prouver que le cabinet est conforme au RGPD. En documentant soigneusement chaque processus, vous pouvez prouver que votre cabinet médical est conforme au RGPD - Si vous ne respectez pas vos obligations, vous pouvez faire l'objet d'une sanction administrative de la CNIL, voire d'une sanction pénale.

Il vous faut constituer et regrouper ces éléments

- Le registre des traitements : Accès au modèle de registre de la CNIL
- Le document d'information remis à vos patients et votre personnel,
- Les procédures mises en place – ex : exercice de leurs droits par les personnes concernées,
- Les contrats passés avec vos prestataires sous-traitants,
- Les réponses apportées aux personnes ayant exercé un de leurs droits,
- Les éventuelles mesures correctrices réalisées en cas de violation de données personnelles…).

Le 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. Uniquement les CPTS et les MSP doivent désigner un DPO pour démontrer leur conformité à la réglementation et limiter les risques juridiques et d'image qui pourraient survenir par un mauvais usage des fichiers comprenant des données personnelles.

Attention aux arnaques

Pratiques commerciales : agressives ou non. Toutes nouvelles règlementations entrainent l'arrivée sur le marché de sociétés spécialistes de la règle. A l'échelle de la pratique du médecin libéral, la mise en conformité peut être faite en interne. Vous pouvez en revanche décider de faire appel à un prestataire externe. Pour cela vérifiez l'authenticité, le statut juridique de l'entreprise sur des sites comme société.com ou infogreffe.fr, vérifiez les services proposés et le cas échéant lisez bien les conditions contractuelles et faites-vous aider par un expert au besoin avant la signature.

Tentatives d'escroquerie : réception de faux courrier, e-mails ou appels de personnes se faisant passer pour des agents de la CNIL et parvenant à usurper ou à afficher le numéro de téléphone de la CNIL. En cas de doute, contacter la CNIL au 01 53 73 22 22 afin de vérifier.

A savoir :
La CNIL ne contacte jamais les professionnels ou particuliers par téléphone pour les mettre en demeure et ne demande jamais ni par téléphone, email ou sms de régler une somme d'argent.

Ne communiquez jamais vos coordonnées bancaires professionnels ou personnelles. Ne versez jamais de sommes d'argent sous la menace d'une sanction financière ou sanction contentieuse.

II Cybersécurité

La cybersécurité rassemble l'ensemble des mesures techniques, organisationnelles et humaines, mises en place pour protéger les systèmes informatiques et les données contre les cybermenaces, dont le cadre est défini et renforcé par le RGPD.

Au sein de votre exercice, il est fortement recommandé de former le personnel de votre structure aux bonnes pratiques de cybersécurité. Cela inclut des sessions régulières sur l'utilisation de mots de passe robustes, l'importance des mises à jour logicielles et la gestion sécurisée des accès aux dossiers médicaux. La sensibilisation aux cyberattaques est primordiale pour prévenir des menaces et autres formes de piratage. Cela peut aider à mieux détecter les risques et à savoir comment réagir en cas de crise.

Les situations de crise possibles

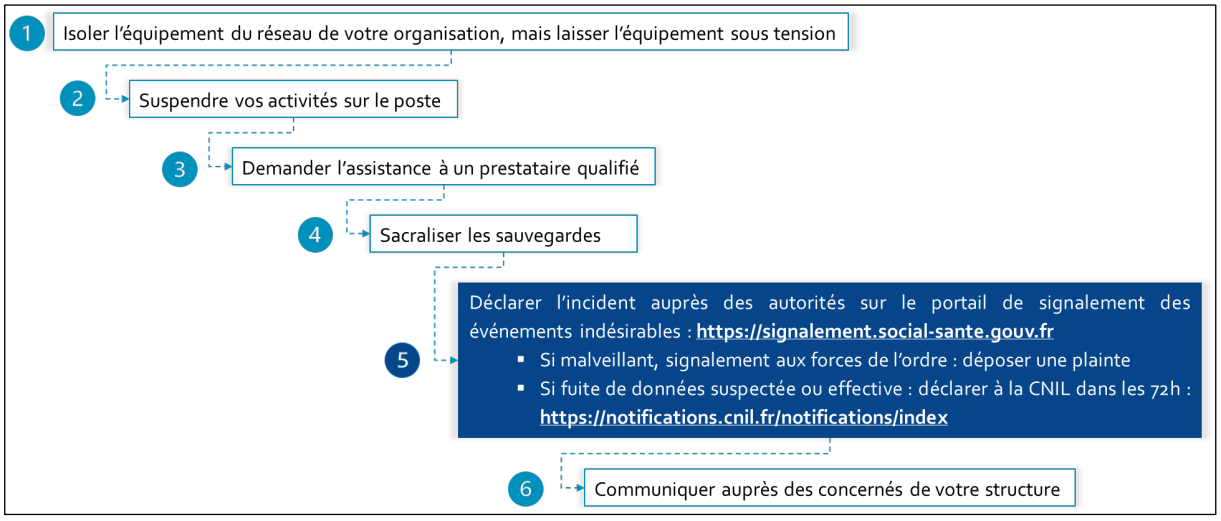
- Le **cybercrime** : obtention illégale des données personnelles pour exploitation ou revente : hameçonnage, phishing, rançongiciels.
- Les **atteintes à l'image, à l'e-réputation** : remplacement des contenus officiels affichés par la structure par des revendications politiques, religieuses ou par des propos susceptibles de nuire à la réputation.
- Les **attaques par espionnage** : accès à votre système informatique pour exploitation des données sur le long terme (objectif économique voire politique).
- Le **sabotage** : panne organisée, entrainant la désorganisation, voire la paralysie de la structure.

Les enjeux et impacts de l'évènement

- Atteinte portée à l'image de la structure, du professionnel
- Impossibilité de communiquer
- Interruption d'activité
- Perte d'informations confidentielles

En cas de crise

Illustration 5 : Cybersécurité : la marche à suivre en cas de crise



Accès à la fiche réflexe en cas d'incident de sécurité informatique de l'ANS

III L'utilisation de l'Intelligence Artificielle et le RGPD

L'utilisation de l'IA dans la pratique médicale soulève des questions importantes en matière de RGPD et de cybersécurité sur la gestion des données de santé. L'utilisation de l'IA en médecine offre des avancées prometteuses, il faut cependant bien vérifier que les outils utilisés respectent strictement le RGPD pour garantir la confidentialité des données personnelles des patients.

Aspects positifs

Optimisation de la gestion des données :

- Amélioration du stockage, de l'organisation et de l'analyse des données de santé, pour une gestion plus efficace des dossiers médicaux. Grâce à l'automatisation de certaines tâches administratives tout en assurant la traçabilité des accès aux données.
- Aide à identifier les anomalies dans les accès ou utilisations des données de santé, renforçant ainsi la protection des informations personnelles.

Conformité avec le RGPD (si bien implémentée) :

- Configuration pour respect des principes fondamentaux du RGPD, tels que la minimisation des données et application automatique des droits des patients, comme le droit à l'effacement ou à la portabilité des données.
- Automatisation du chiffrement des données, leur pseudonymisation et leur anonymisation, pour une meilleure sécurité des informations sensibles.

Détection d'anomalies de sécurité :

- Utilisation pour surveiller en temps réel les cybermenaces et signaler des comportements inhabituels, comme les tentatives d'accès non autorisées, renforçant la cybersécurité.

Outil
Accès à la grille d'autoévaluation de la CNIL pour évaluer les systèmes d'Intelligence Artificielle

Aspects négatifs

Risques accrus de cyberattaques :

- Cibles privilégiées pour les cyberattaques, une faille peut entraîner des violations massives de la confidentialité des données patients.
- Augmentation du risque d'attaque avec la centralisation des données, une faille pourrait potentiellement compromettre une grande quantité d'informations sensibles.

Non-conformité potentielle avec le RGPD :

- Mauvaise utilisation ou non-respect du RGPD. Par exemple, les algorithmes pourraient sur-traiter des données ou conserver des informations au-delà de la durée nécessaire, en violation des principes de minimisation et de limitation de la conservation.
- Manque de transparence des algorithmes d'IA : risque de non-respect du consentement et droit à l'information des patients sur l'utilisation de leurs données.

Problèmes de confidentialité et de consentement :

- L'IA nécessite souvent d'énormes volumes de données pour fonctionner efficacement. Les patients doivent être informés de manière claire et concise sur la manière dont leurs données sont utilisées, ce qui peut être difficile dans le cas d'algorithmes complexes.
- Le consentement éclairé pourrait être problématique si les patients ou les praticiens ne comprennent pas exactement comment l'IA utilise ou analyse les données de santé.

Responsabilité en cas de violation :

- En cas de violation de données due à une mauvaise utilisation de l'IA, la responsabilité du médecin pourrait être engagée. Le médecin doit donc veiller à ce que les fournisseurs de solutions d'IA respectent pleinement les normes de sécurité et de protection des données.

Essentiel

Pour un médecin libéral, le respect du RGPD et la mise en place de bonnes pratiques en matière de cybersécurité sont indispensables pour protéger les données sensibles des patients. L'utilisation croissante des technologies, y compris l'intelligence artificielle (IA), offre des outils puissants pour améliorer les soins, mais elle nécessite également une vigilance accrue sur la confidentialité des données et la sécurisation des systèmes. En intégrant ces technologies de manière responsable et conforme aux réglementations, le médecin peut optimiser son activité tout en garantissant la protection des informations personnelles de ses patients.

Date de mise à jour : Septembre 2024

Mots clés : #RGPD #Cybersécurtié #Cyperprotection #Données #CNIL #ANSSI