RGPD et médecine libérale : Tout ce que vous devez savoir

Partenaire :

Ordre du jour

1. **Présentation du RGPD**
2. **Données personnelles / Données sensibles**
3. **En quoi les Médecins libéraux sont-ils concernés ?**
4. **Les obligations**
5. **Les bonnes pratiques du RGPD en médecine libérale**
6. **Les sanctions**

Présentation du RGPD

Règlement Général sur la Protection des Données

- Énumère des exigences précises concernant la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et à la libre circulation de ces données

- A pris effet le 25 mai 2018 pour tous les organismes opérant en Europe

- Téléchargeable gratuitement sur internet :

  http://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32016


EUROPEAN COMMISSION

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Objectifs du RGPD

- Supprimer les faiblesses présentes dans les lois nationales
- Améliorer la protection de la vie privée des personnes physiques
- Actualiser la loi pour être en cohérence avec les nouveaux défis de sécurité liés à internet, aux médias sociaux, au big data et au marketing comportemental
- Faciliter la gestion administrative avec les organismes traitant avec plusieurs autorités de contrôle

En France, l'autorité de contrôle est la CNIL : Commission Nationale de l'Informatique et des Libertés

Données personnelles / Données sensibles

Données personnelles

Le RGPD définit une donnée personnelle comme toute information se rapportant à une personne physique identifiée ou identifiable.

1. **Identité**: Nom, prénom, adresse, numéro de téléphone, adresse e-mail, numéro de sécurité sociale, numéro de passeport etc.

2. **Caractéristiques personnelles**: Date de naissance, âge, sexe, état civil, nationalité, etc.

3. **Données de localisation**: Adresse postale, coordonnées GPS, adresse IP, etc.

4. **Données professionnelles**: Fonction, employeur, historique professionnel, etc.

5. **Données financières**: Informations bancaires, historique des transactions, numéro de carte de crédit, etc.

6. **Données comportementales**: Historique de navigation sur Internet, préférences personnelles, activités en ligne, etc.

Données sensibles

Les données sensibles sont une catégorie des données personnelles dont le traitement comporte un risque pour la personne concernée. Le RGPD prévoit un régime de protection renforcé pour ces données.

1.Données de santé: Informations médicales, antécédents médicaux, traitements en cours, résultats d'examens médicaux, etc.

2.Origine raciale ou ethnique: Informations sur l'ascendance, la race, l'ethnicité, la couleur de peau, etc.

3.Opinions politiques: Affiliations politiques, opinions politiques exprimées, etc.

4.Appartenance syndicale: Affiliation à un syndicat, participation à des activités syndicales, etc.

5.Croyances religieuses ou philosophiques: Appartenance religieuse, croyances philosophiques, pratiques religieuses, etc.

6.Orientation sexuelle: Information sur l'orientation sexuelle, l'identité de genre, etc.

7.Données génétiques: Informations génétiques, y compris les tests ADN, les marqueurs génétiques, etc.

8.Données biométriques: Empreintes digitales, reconnaissance faciale, caractéristiques physiques uniques, etc.

En quoi les médecins libéraux sont-ils concernés par le RGPD ?

Application du RGPD en médecine libérale

Pour rappel, le RGPD définit les données personnelles et sensibles comme « toutes informations se rapportant à une personne physique identifiée ou identifiable ».

Le médecin traite les informations du patient dans la cadre du dossier patient, d'une plateforme de gestion de rendez-vous, d'un acte de télémédecine etc. Une partie de ces données sont explicitement des données sensibles.

Le médecin collecte des informations pour gérer son cabinet (fournisseur, personnel, etc.), ces informations sont également des données personnelles.

Vous êtes donc concernés au plus haut niveau par le RGPD.

Avez-vous besoin d'un DPO ?

Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au Règlement européen sur la protection des données au sein de l'organisme qui l'a désigné. Il intervient sur l'ensemble des traitements mis en œuvre par cet organisme.

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.

Les obligations du médecin libéral

- Les grands principes
- Le registre de traitement
- La violation de données
- Déclaration à la CNIL

Les principes du RGPD

Le RGPD a identifié six principes à appliquer lors de la collecte et lors du traitement des données. Ce sont ces principes qui guident l'ensemble des mesures à prendre afin d'être en conformité.

Principe 1

Les données sont traitées de manière licite, loyale et transparente

Principe 2

Les données dont collectées à des fins déterminées, explicites et légitimes

Principe 3

Les données collectées sont adéquates, pertinentes et limitées à ce qui est nécessaire

Principe 4

Les données sont exactes et tenues à jour

Principe 5

Les données sont conservées dans un format permettant l'identification des personnes concernées uniquement pour la durée nécessaire au traitement

Principe 6

Les données sont traitées de façon à garantir la sécurité

Principe n° 1 : Traitées de manière licite, loyale et transparente

- La licéité du traitement fait référence à son fondement juridique/base légale (consentement, intérêt vital, intérêt légitime, obligation légale, obligation contractuelle, missions de service public).

- La loyauté du traitement désigne quant à elle les modalités selon lesquelles les données sont collectées. Ce principe fait référence au droit à l'information des individus. Le responsable de traitement c'est-à-dire vous, devra fournir une information complète en termes clairs sur le traitement.

- Lors de la collecte de données à caractère personnel, vous devez également dire à la personne qui vous êtes et si les données seront transmises à d'autres parties.

Mise en œuvre du principe 1 pour les dossiers patients

CONSENTEMENT : 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,

INFORMATION : Vous devez informer les patients de l'existence de vos dossiers et de leurs droits à cet égard.
Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un document spécifique (ex : dépliant remis au patient ou mis à disposition dans la salle d'attente).

L'information doit comporter impérativement les éléments suivants :

- Votre nom et vos coordonnées ;
- Les finalités et la base juridique du traitement, y compris les finalités ultérieures ;
- Les destinataires des données ;
- La durée de conservation ;
- Les droits de la personne ;

Mise en œuvre du principe 1 pour les dossiers patients

Exemples de finalités/bases légales :

Finalités	Bases légales envisageables[3]
La tenue du dossier médical	Obligation légale
L'établissement et la télétransmission des documents à destination de l'assurance maladie	Obligation légale
La tenue du dossier de prise en charge sanitaire (comme par exemple le dossier de soins infirmiers)	Obligation légale
La prise de rendez-vous	Intérêt légitime
La tenue de la comptabilité	Intérêt légitime
La télémédecine (art. L. 6316-1 du CSP), le télésoin (art. L. 6316-2 du CSP)	Intérêt légitime

Principe n° 2 : La finalité

- Avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément annoncer aux personnes concernées les objectifs de la collecte des données ou autrement dit ce à quoi elles vont lui servir. Plus encore, les données personnelles collectées ne pourront pas être réutilisées pour une autre finalité que celle prévue initialement.

Mise en œuvre du principe 2 pour les dossiers patients

Les informations recueillies sont essentielles à l'exercice de votre profession médicale, notamment pour la prévention, le diagnostic, les soins et la gestion de votre cabinet.

Ces données servent spécifiquement à :

- Organiser les rendez-vous ;
- Maintenir à jour les dossiers médicaux ;
- Émettre des ordonnances ;
- Correspondre avec d'autres professionnels de santé ;
- Établir et transmettre électroniquement les feuilles de soins.

Toute autre utilisation des informations collectées lors de la prise en charge des patients doit être entreprise avec précaution.

En particulier, il est formellement interdit d'utiliser ces données à des fins personnelles ou commerciales.

Principe n° 3 : La pertinence ou le principe de minimisation

- Les données traitées doivent être pertinentes, adéquates et limitées au regard de la finalité poursuivis. Ainsi seules les données strictement nécessaires à la réalisation de l'objectif déterminé doivent être collectées : c'est le principe de minimisation.

- Autrement dit le responsable de traitement ne doit pas collecter plus de données que ce dont il a vraiment besoin.

Mise en œuvre du principe 3 pour les dossiers patients

Toutes les données partagées par vos patients au cours de vos échanges ne doivent pas automatiquement figurer dans leur dossier. Seules celles pertinentes pour leur suivi médical doivent être enregistrées et conservées.

À cet égard, la CNIL considère comme légitime la collecte de certaines catégories de données personnelles, telles que :

-Les données d'identification : nom, prénom, date de naissance, adresse, numéro de téléphone ;
- Le numéro de sécurité sociale : utilisé exclusivement pour l'édition des feuilles de soins et leur télétransmission aux caisses d'assurance maladie ;
- Si nécessaire, des informations sur la situation familiale : état matrimonial, nombre d'enfants ;
-Si nécessaire, des détails sur la vie professionnelle : profession, conditions de travail ;
-Les données de santé : antécédents médicaux, historique des soins, diagnostics, prescriptions médicales, nature des interventions, résultats d'examens de laboratoire, et tout autre élément pertinent pour évaluer la santé du patient, selon l'appréciation du médecin ;
- Les informations concernant les habitudes de vie : recueillies avec le consentement du patient et seulement si elles sont nécessaires au diagnostic et aux soins.

Mise en œuvre du principe 3 pour les dossiers patients

Si d'autres informations vous semblent pertinentes et nécessaires dans le cadre de votre pratique professionnelle, vous êtes autorisé à les collecter (par exemple, l'origine ethnique si elle influence une pathologie spécifique ou un traitement médical, ou les habitudes alimentaires).

En revanche, toute information sans rapport avec la raison de la consultation du patient ou non essentielle au diagnostic ou à la fourniture de soins doit être exclue. Par exemple, il est interdit d'enregistrer des données sur la vie privée du patient qui ne sont pas médicalement nécessaires, comme sa religion ou son orientation sexuelle.

Principe n° 4 : La limitation de la conservation des données

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées.

La durée de conservation des données doit ainsi être limitée au strict minimum. Cette durée de conservation doit être définie au préalable par responsable du traitement, en tenant compte des éventuelles obligations à conserver certaines données qui peuvent être variables.

Mise en œuvre du principe 4 pour les dossiers patients

Il est essentiel de prendre en considération les délais de prescription pour d'éventuelles actions en responsabilité, ainsi que toutes les dispositions spécifiques éventuelles.

En l'absence de directives particulières quant à la durée de conservation des dossiers des professionnels exerçant en libéral, le Conseil national de l'Ordre des médecins recommande de se conformer aux délais de conservation établis pour les dossiers médicaux des établissements de santé :

- Les dossiers doivent être conservés pendant 20 ans à partir de la date de la dernière consultation du patient.
- Si le patient est mineur et que le délai de 20 ans expire avant son 28ème anniversaire, les informations le concernant doivent être conservées jusqu'à cette date.
- Dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à partir de la date du décès.
- En cas d'action en responsabilité contre le médecin, il est recommandé de suspendre ces délais de conservation.

Par ailleurs, les doubles des feuilles de soins doivent être conservés pendant 3 mois.

Principe n° 5 : Respecter les droits des personnes

Au-delà du droit à l'information indiqué plus haut, les personnes dont les données personnelles sont collectées disposent également de certains droits qu'elles peuvent exercer auprès de l'organisme qui détient ces données:

- Un droit d'accéder à ces données,
- Un droit de les rectifier,
- Un droit de s'opposer à leur utilisation,
- Un droit d' effacer les données, dans certaines situations particulières (dossier patient conservé trop longtemps, données non adéquates, etc.)
- Un droit à la limitation de traitement,
- Un droit à la portabilité des données,
- Un droit de se plaindre auprès de la CNIL.

Attention, l'exercice de ces droits n'est pas automatique et le RGPD conditionne leur emploi.

Mise en œuvre du principe 5 pour les dossiers patients

Chaque demande portant sur ces droits doit être examinée dans un délai raisonnable. Dans le cas d'une demande d'accès au dossier « patient », le délai est obligatoirement de 8 jours, porté à 2 mois lorsque les informations datent de plus de 5 ans.

Principe n° 6 : La sécurité des données personnelles

- En utilisant les mesures techniques et organisationnelles appropriées, les données à caractère personnel doivent être conservées de manière sécurisée afin :

  - D'assurer la protection contre le traitement non autorisé ou illégal,
  - D'éviter la perte, la dégradation ou destruction accidentelle des données.

Mise en œuvre du principe 6 pour les dossiers patients

Accès aux données de santé :

C'est à vous de prendre toutes les précautions nécessaires pour empêcher que des tiers non autorisés aient accès aux données de santé.

Professionnels de santé : accès spécifique aux seules informations nécessaires à la prise en charge, ou si cela n'est pas possible, le médecin peut envoyer les informations nécessaires directement à ces professionnels.

Personnels administratifs : Accès global aux dossiers des patients. Certaines données (nom, prénom, code acte, NIR, date de la consultation) sont adressées aux organismes d'assurance maladie via la télétransmission ou les feuilles de soins.

Prestataires de services pour assurer la maintenance du logiciel dossiers patients : rôle purement technique, aucun accès aux données à caractère personnel (données chiffrées).

Mise en œuvre du principe 6 pour les dossiers patients

Accès aux données de santé suite :

Prestataire assurant le stockage et la conservation des données dans des serveurs à distance : il doit être hébergeur agréé ou certifié pour l'hébergement, le stockage, la conservation de données de santé conformément aux dispositions de l'article L. 1111-8 du code de la santé publique.

Relation formalisée avec un contrat de sous-traitance mentionnant que ce prestataire :

- ne traite les données à caractère personnel que sur votre instruction ;
- veille à la signature d'engagements de confidentialité par le personnel ;
- prend toutes les mesures de sécurité requises ;
- ne recrute pas de sous-traitant sans votre autorisation écrite préalable ;
- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement notamment lorsque des patients ont des demandes concernant leurs données ;
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- collabore dans le cadre d'audits.

Mise en œuvre du principe 6 pour les dossiers patients

Sécurisation du système informatique (recommandations CNIL):

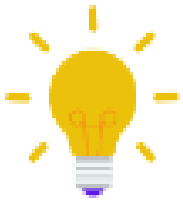
- Utilisation d'un mot de passe conforme aux recommandations de la CNIL, 12 caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux), renouvelé régulièrement ;
- Verrouillage de votre session informatique automatiquement après maximum 30 minutes d'inactivité ;
- Antivirus à jour, pare-feu, application systématique des correctifs de sécurité du système informatique et des logiciels ;
- Sauvegardes régulières des données Chiffrement des données avec un logiciel adapté ;
- Absence ou minimisation des connexions d'appareils non professionnels sur le réseau ;
- Authentification via votre carte de professionnel de santé (CPS) ou tout moyen alternatif d'authentification forte (CPS strictement personnelle, codes à ne diffuser à personne y compris le personnel)

Si vous conservez vos dossiers sous format papier, vous devez également vous assurer de leur sécurité (locaux sécurisés, armoire contenant les dossiers, fermée à clé).

Le registre des activités de traitement

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles.

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD.



Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.

Quelles informations doit-on retrouver dans ce registre ?

Pour chaque activité de traitement de données personnelles que vous aurez répertoriée (suivi des patients, prise de rendez-vous, messagerie sécurisée, télémédecine, gestion de la paie, gestion des fournisseurs, etc.), il est obligatoire de constituer un registre et de le garder en interne.

On y retrouve à minima :

- Vos noms et coordonnées
- Les finalités du traitement, l'objectif en vue duquel vous avez collecté ces données
- Les catégories de personnes concernées (patients, personnel, etc)
- Les catégories de données personnelles (données de santé, identité, données bancaires, etc)
- Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
- Les délais prévus pour l'effacement des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en œuvre

Le RGPD impose uniquement que le registre se présente sous une forme écrite. Le format du registre est libre et peut être constitué au format papier ou électronique.

La violation de données

Une violation de données se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Il s’agit de tout incident de sécurité, d’origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l’intégrité, la confidentialité ou la disponibilité de données personnelles.

La violation de données

1ère étape : Procéder à une analyse exhaustive de l'ampleur du problème afin d'identifier les mesures nécessaires pour prévenir toute récurrence de cet incident. Cette analyse devrait inclure des questions telles que :
"Qui a eu accès aux données ? Quelle est l'origine du problème ? Les données ont-elles été transmises à un tiers ? Des données de santé sont-elles impliquées ? Quelles actions auraient pu empêcher cet événement ? Quelles mesures peuvent être prises pour atténuer ses conséquences ?"

Puis si la violation engendre un risque pour les droits et libertés des personnes :
Elle doit être notifiée de façon détaillée dans les 72 heures à la CNIL via un formulaire https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles précisant :

- La nature de la violation
- Les catégories et nombre approximatif de personnes et de données concernées
- Vos noms et coordonnées
- Les mesures prises et/ou à prendre pour remédier à la violation
- Le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

Si l'incident a eu lieu au sein d'un établissement de santé , la structure doit également notifier l'incident à l'Agence Régionale de Santé compétente

La violation de données

Si la violation engendre un risque pour les droits et libertés des personnes :
Sur la demande de la CNIL ou à votre propre initiative, vous devez communiquer dans les meilleurs délais à la personne ou aux personnes concernées cette violation : sauf si les données étaient chiffrées ou si les mesures prises ultérieurement garantissent qu'il n'y a plus de risque élevé.

- Communication individuelle ou si trop de personnes concernées communication publique.

- Informations à transmettre : vos coordonnées, les conséquences probables, les mesures prises pour remédier à la violation et le cas échéant les mesures prises pour atténuer les éventuelles conséquences négatives.

Dans tous les cas : La violation doit être inscrite soit dans un registre spécifique, un tableau récapitulatif des incidents ou au sein du registre des activités de traitement.

Puis informer le plus rapidement possible votre assurance de responsabilité professionnelle.

Déclaration à 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.

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.

Les bonnes pratiques du RGPD en médecine libérale

La prise de rendez-vous

Si vous choisissez de faire appel à une plateforme de prise de rendez-vous en ligne :

- Vous devez limiter les informations collectées par le prestataire et vérifie la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance que vous passez avec lui.

Dans tous les cas :

- Vos obligations sont identiques à celles applicables pour les dossiers « patients » : enregistrement des données strictement nécessaires, utilisation légitime des informations obtenues dans le cadre de la prise de rendez-vous, inscription dans le registre des activités de traitement, limitation des accès, sroits des patients, sécurisation du planning et de son contenu.

- Si la consultation ne nécessite pas de préparation au préalable ou la réservation d'outils spécifiques, les motifs de la consultation n'ont pas à être renseignés.

- Les données relatives à la prise de rendez-vous peuvent être supprimées lorsqu'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.

La messagerie électronique

La messagerie sécurisée :

Le système de messagerie sécurisée de santé est un espace dématérialisé qui permet l'échange de données de santé en toute confiance entre professionnels de santé et, plus largement, entre professionnels des secteurs sanitaire, social et médico-social.

De nombreux acteurs de la santé ont intégré ce système fondé, avant l'entrée en application du RGPD, sur la réalisation d'un engagement de conformité à l'autorisation unique 037. Depuis l'entrée en application du RGPD, l'utilisation de la messagerie sécurisée est possible sans avoir à accomplir une formalité auprès de la CNIL. Pour autant, le traitement découlant de l'utilisation de la messagerie sécurisée devra être inscrit sur votre registre des activités de traitement.

La messagerie électronique

La messagerie électronique standard :

Pour sécuriser vos échanges, notamment concernant les données de santé, l'utilisation d'une messagerie électronique sécurisée est impérative. Cependant, pour communiquer avec d'autres professionnels, non professionnels de santé mais intervenant dans la prise en charge du patient (par exemple, ostéopathes, psychologues, etc.), ou avec les patients eux-mêmes, l'envoi de données de santé via une messagerie électronique standard nécessite :

- Le chiffrement des données sensibles à transmettre. À cet égard, il est recommandé de suivre les préconisations de la CNIL.
- L'utilisation d'un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP ou HTTPS, en privilégiant les versions les plus récentes des protocoles.
- L'assurance du secret nécessaire à la lecture du fichier (par exemple, via un mot de passe) en utilisant un canal de communication différent (tel que téléphone, SMS, etc.).

L'utilisation de toute messagerie ne chiffrant pas les données et hébergeant celles-ci dans un pays ou chez un prestataire ne garantissant pas la protection des données conformément aux règles européennes est à proscrire. Les messageries instantanées ou "chat" sont à utiliser avec précaution et de façon sécurisée.

La télémédecine

La télémédecine représente une pratique médicale à distance exploitant les technologies de l'information et de la communication. Lorsque vous optez pour une téléconsultation ou une téléexpertise, vous réalisez un acte médical.

Toutes vos obligations déontologiques habituelles restent en vigueur, de même que vos engagements concernant les informations que vous êtes amené à recueillir à propos de vos patients ou d'autres professionnels de santé impliqués dans leur prise en charge. Les normes régissant l'échange et le partage de données entre professionnels de santé sont également de rigueur.

Lorsque vous décidez d'utiliser une plateforme de télémédecine à l'occasion de votre activité, vous devez vous assurer que le prestataire (qui met à votre disposition cette plateforme et qui est votre sous-traitant), respecte la réglementation.

Le contrat de sous-traitance doit indiquer les mêmes informations que précédemment citées page 28.

Les sanctions

La responsabilité

- Le responsable du traitement (vous) est en charge de démontrer la conformité aux principes de protection des données du RGPD et doit donc s'assurer que tous les sous-traitants du traitement disposent de mesures mises en place pour se conformer au RGPD
- Cependant, en cas de violation, le responsable du traitement et le sous-traitant seront tenus responsables
- Il est donc important de préciser les responsabilités et obligations de chacun dans tout accord contractuel entre les responsables du traitement et les sous-traitants
- La norme ISO est reconnue à l'international comme étant un moyen efficace de prouver que les mesures techniques et organisationnelles appropriées ont été mises en place

Les sanctions

Avertissements et réprimandes : Les autorités de contrôle peuvent émettre des avertissements ou des réprimandes aux médecins libéraux qui ne respectent pas les dispositions du RGPD.

Il est donc impératif de vous mettre en conformité avec la réglementation et de documenter cette conformité (registre des activités de traitement, traçabilité des violations de données, engagements de confidentialité du personnel, etc.). Si la CNIL constate un défaut de conformité et vous met en demeure de vous conformer, vous avez encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction

Limitations sur le traitement des données : Les autorités de contrôle peuvent imposer des limitations sur la manière dont les médecins libéraux traitent les données personnelles, y compris des interdictions ou des restrictions sur certaines pratiques de traitement.

Les sanctions

Amendes administratives : Les médecins libéraux peuvent se voir infliger des amendes administratives en cas de violation grave du RGPD. Ces amendes peuvent atteindre jusqu'à 4 % du chiffre d'affaires annuel mondial de l'organisation ou 20 millions d'euros, selon le montant le plus élevé.

Sanctions pénales : Les peines pénales maximales pour une personne physique sont de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.

Réparations pour les personnes concernées : En plus des sanctions administratives, les médecins libéraux peuvent être tenus de verser des dommages et intérêts aux personnes concernées en cas de préjudice résultant d'une violation du RGPD.

La CNIL a indiqué que les contrôles de conformité qu'elle pourrait réaliser seront, dans les premiers mois d'application du RGPD, à visée pédagogique. L'essentiel est de pouvoir démontrer que vous êtes engagé dans une démarche de mise en conformité.

Quiz

Qu'est-ce qu'une donnée sensible selon le RGPD ?

- A : Tout type d'information personnelle
- B : Les informations médicales, y compris les antécédents médicaux, les traitements en cours, etc.
- C : Les informations sur l'origine ethnique d'une personne
- D: Les données financières d'un individu
- E : L’orientation sexuelle
- F : La marque de la voiture

Quiz

Qu'est-ce qu'une donnée sensible selon le RGPD ?

- A : Tout type d'information personnelle
- B : Les informations médicales, y compris les antécédents médicaux, les traitements en cours, etc.
- C : Les informations sur l'origine ethnique d'une personne
- D: Les données financières d'un individu
- E : L’orientation sexuelle
- F : La marque de la voiture

Quiz

Quelles sont les mesures de sécurité que les professionnels de la santé doivent mettre en place pour protéger les données de santé conformément au RGPD ?

- A : Chiffrement des données
- B : Mots de passe sécurisés
- C : Formation du personnel sur la protection des données
- D : Toutes les réponses ci-dessus

Quiz

Quelles sont les mesures de sécurité que les professionnels de la santé doivent mettre en place pour protéger les données de santé conformément au RGPD ?

- A : Chiffrement des données
- B : Mots de passe sécurisés
- C : Formation du personnel sur la protection des données
- D : Toutes les réponses ci-dessus

Quiz

Quelles sont les conséquences du non-respect du RGPD en ce qui concerne les données de santé ?

- A : Avertissements uniquement
- B : Amendes financières uniquement
- C : Amendes financières et réparations pour les personnes concernées
- D : Sanctions pénales
- E : Aucune conséquence, le RGPD ne concerne pas les données de santé

Quiz

Quelles sont les conséquences du non-respect du RGPD en ce qui concerne les données de santé ?

- A : Avertissements uniquement
- B : Amendes financières uniquement
- C : Amendes financières et réparations pour les personnes concernées
- D : Sanctions pénales
- E : Aucune conséquence, le RGPD ne concerne pas les données de santé

Quiz

Quelle est la première étape qu'un professionnel de la santé devrait suivre avant de collecter et de traiter les données de santé d'un patient ?

- A : Demander l'avis d'un collègue
- B : Informer de façon explicite le patient de la manière dont ses données seront utilisées
- C : Consulter les autorités de contrôle
- D : Pas le temps je soigne mon patient et c’est tout

Quiz

Quelle est la première étape qu'un professionnel de la santé devrait suivre avant de collecter et de traiter les données de santé d'un patient ?

- A : Demander l'avis d'un collègue
- B : Informer de façon explicite le patient de la manière dont ses données seront utilisées
- C : Consulter les autorités de contrôle
- D : Pas le temps je soigne mon patient et c’est tout

Quiz

Chez mon médecin, dans la salle d'attente, à son arrivée, chaque patient doit inscrire son nom et son prénom sur un cahier. Le médecin utilise cette liste pour appeler les patients par ordre d'arrivée. Ce mode de gestion est-il conforme au RGPD ?

- A : Oui
- B : Non

Quiz

Chez mon médecin, dans la salle d'attente, à son arrivée, chaque patient doit inscrire son nom et son prénom sur un cahier. Le médecin utilise cette liste pour appeler les patients par ordre d'arrivée. Ce mode de gestion est-il conforme au RGPD ?

- A : Oui
- B : Non

Merci de votre attention