Doctolib

Votre cabinet est-il un lieu sûr ?

Comment protéger la confidentialité des données de vos patients

Janvier 2022

10 questions
sur la protection des données et la sécurité informatique

Quel protecteur de données êtes-vous ? Faites le test !

Cochez les questions auxquelles vous pouvez répondre

Assurer la confidentialité des données de santé de vos patients est essentiel, plus encore à l'heure du numérique. Êtes-vous à l'aise dans cet environnement ? Testez vos connaissances en matière de confidentialité des données ! Lisez les 10 questions ci-dessous et cochez celles auxquelles vous pouvez répondre.

- ○ **Savez-vous ce qu'est le "phishing" ou un "rançongiciel" ?**
- ○ **Pourriez-vous écrire en toutes lettres l'acronyme RGPD ?**
- ○ **Savez-vous comment le RGPD s'applique dans votre cabinet ?**
- ○ **Connaissez-vous la signification du sigle 2FA ?**
- ○ **Sauriez-vous répondre aux questions de vos patients à propos de leurs données ?**
- ○ **Utilisez-vous le chiffrement lorsque vous échangez des données ?**
- ○ **Utilisez-vous votre propre nom ou celui de votre cabinet comme mot de passe ?**
- ○ **Connaissez-vous la date de la dernière mise à jour de votre pare-feu ?**
- ○ **Savez-vous quelles données vous pouvez demander à vos patients ?**
- ○ **Savez-vous quand et comment supprimer les données de vos patients ?**

Vos résultats
Quel protecteur de données êtes-vous ?

Vous cochez entre 0 et 5 cases :

la sécurité des données est un sujet qui vous préoccupe et vous souhaiteriez en savoir et en faire plus. Rendez-vous page 7.

Vous cochez entre 5 et 7 cases :

la sécurité des données, vous maîtrisez. Mais vous pourriez aller plus loin. Rendez-vous page 11.

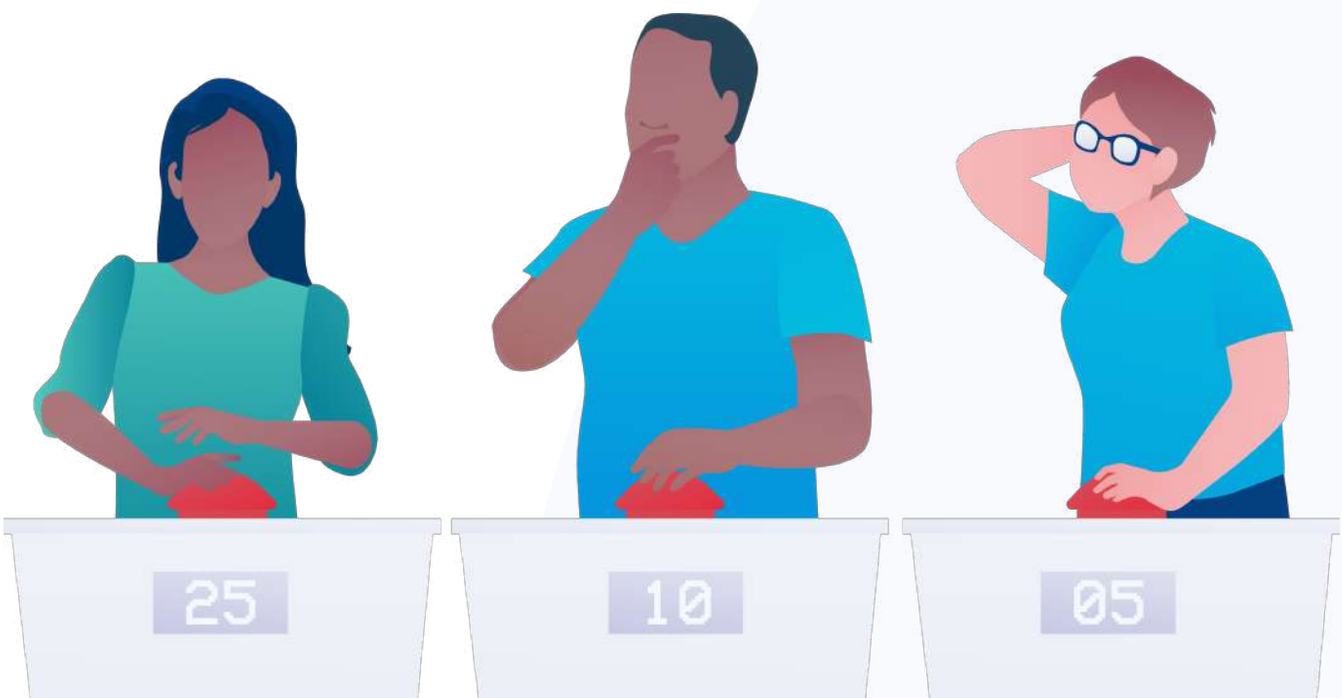
Vous cochez entre 7 et 10 cases :

la sécurité des données n'a (presque) aucun secret pour vous. Néanmoins, une petite mise à jour est toujours la bienvenue. Rendez-vous page 16.

Que vous cochiez 0 ou 10 cases :

l'ensemble de ces pages est conçu pour aider chaque praticien à renforcer la confidentialité des données au sein de son cabinet et à répondre aux éventuelles questions des patients.

Retrouvez l'ensemble des réponses au fil des pages de notre guide, grâce au symbole



Sondage

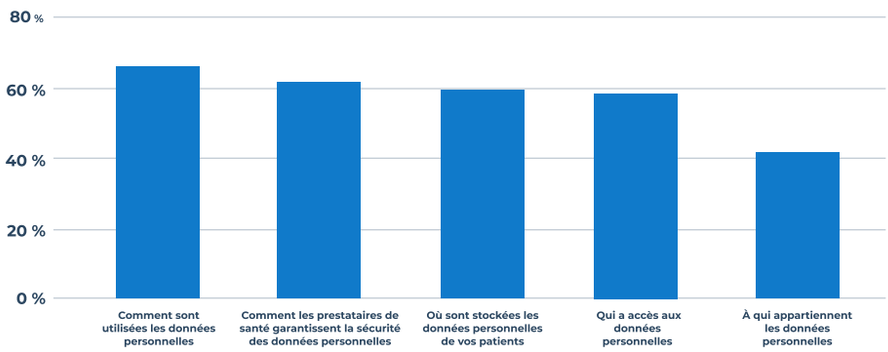
La protection des données de santé : qu'en pensent les praticiens et leurs patients ?

98 %
des praticiens interrogés pensent que la sécurité des données est un sujet important.

5,3/10
Comment les praticiens évaluent leur propre niveau de connaissance en matière de protection des données

66 %
des praticiens se sentent en mesure de protéger les données de santé de leurs patients

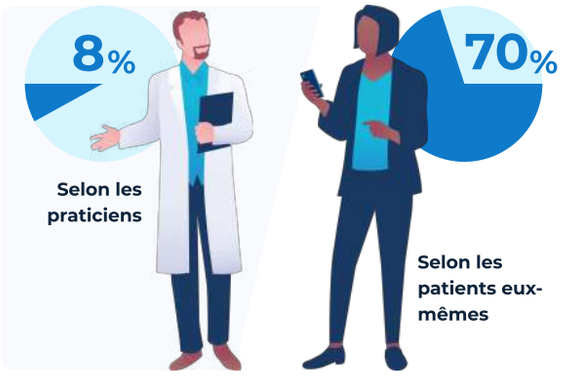
Toutefois, les praticiens veulent approfondir certaines thématiques spécifiques liées à la protection des données :



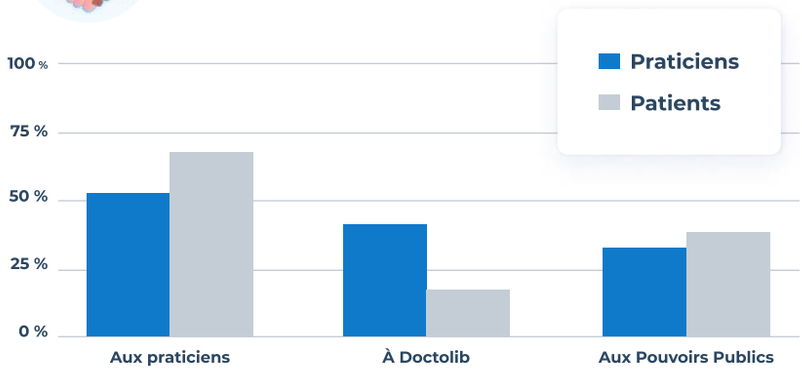
47 %

des praticiens interrogés savent quelles sont les données de leurs patients qu'ils peuvent recueillir

Quelle est la part de patients qui se sentent très concernés par la protection de leurs données ?



À qui les praticiens et les patients accordent-ils leur confiance pour protéger leurs données de santé ?



300 000 personnels de santé et les plus grands établissements de santé en Europe, ainsi que 60 millions d'Européens, utilisent nos services et nous font confiance pour assurer la confidentialité des données personnelles de leurs patients.
Plus d'infos sur la confidentialité des données sur : https://about.doctolib.fr/confidentialite/adn.html

Sources : sondages menés en France et en Allemagne, du 13 au 18 janvier 2022, auprès de la communauté Doctolib (140 praticiens en France et 93 en Allemagne, 9136 patients en France et 1520 en Allemagne)

Sommaire

Méthodologie des sondages

questionnaire envoyé aux praticiens utilisateurs de Doctolib entre le 13 et le 19 janvier 2022. 140 répondants

questionnaire envoyé aux patients utilisateurs de Doctolib entre le 14 et le 17 janvier 2022. 9 136 répondants

Nos experts

en protection des données personnelles

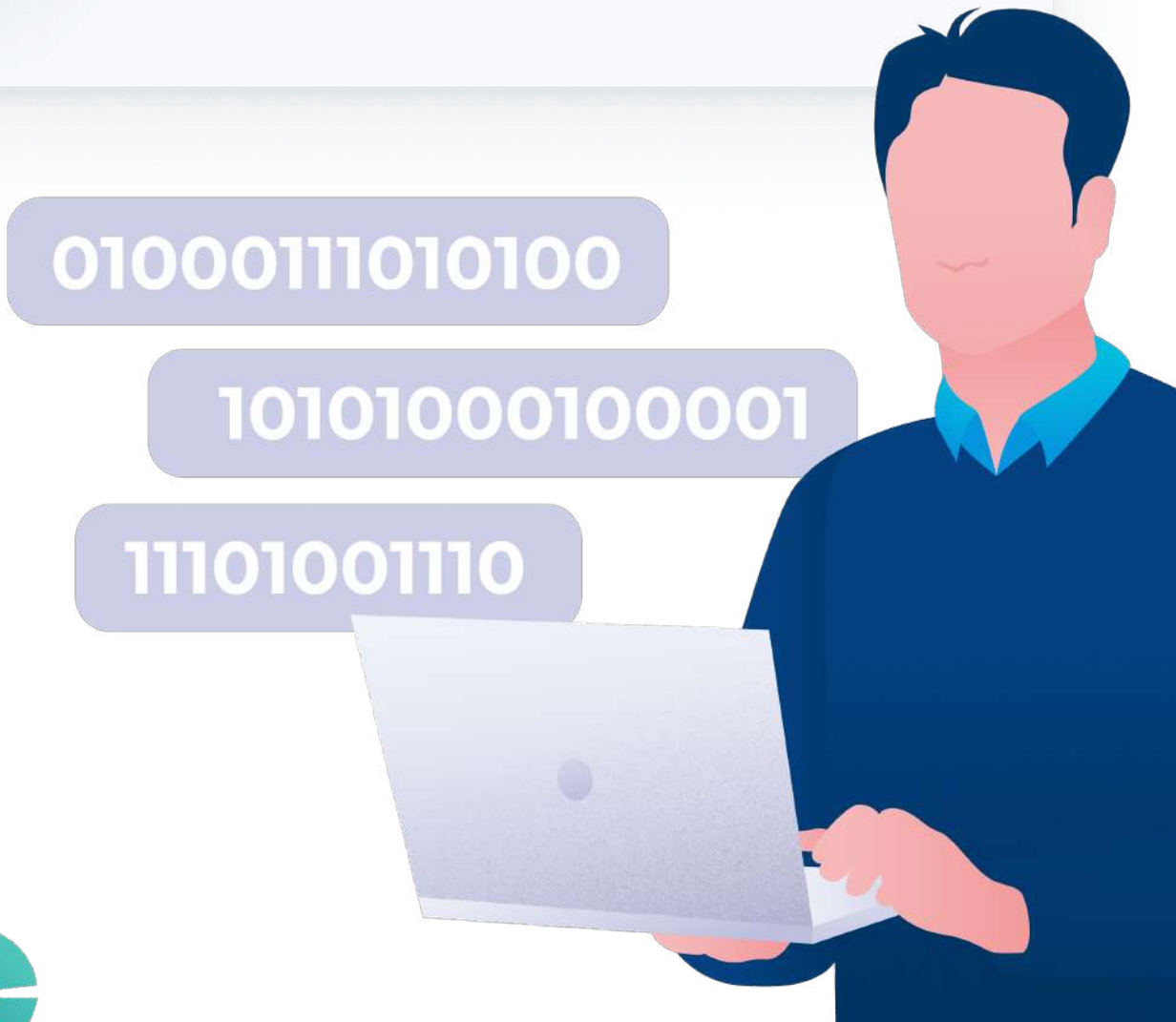
Cédric Voisin

Responsable de la sécurité des systèmes d'information du groupe Doctolib

Dr Olivier Esnault

Chirurgien maxillo-facial et stomatologue à Paris

Pionnier Doctolib



La protection

des données, un impératif sanitaire

Vous êtes un inconditionnel des fiches Bristol, soigneusement classées dans vos tiroirs. Vous ne jurez que par le dématérialisé. Que vous soyez adepte du papier ou du numérique, vous recevez, en tant que praticien, de nombreuses informations que vous consignez dans le dossier personnel de chacun de vos patients. Confidentielles et sensibles, les données qui vous sont confiées sont nécessaires au bon suivi de votre patient. Elles doivent être strictement protégées.

Donnée personnelle et donnée de santé : de quoi parle-t-on ?

Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable. Il peut s'agir de son nom, son prénom, son numéro de téléphone, son identifiant (numéro de client par exemple)...

Une donnée de santé est une donnée personnelle relative à la santé physique ou mentale, passée, présente ou future d'une personne physique qui révèle des informations sur l'état de santé de cette personne. Il peut s'agir des antécédents médicaux, de résultats d'examens, de traitements, du croisement de données comme la tension avec la mesure de l'effort...

On parle de **"traitement des données"** lorsque l'on collecte, enregistre, organise, consulte ou utilise des données personnelles. Un traitement de données doit avoir une finalité légale et légitime, en lien avec l'activité professionnelle. Dans le cadre de votre activité, il peut s'agir de la tenue du dossier du patient, de la prise de rendez-vous en ligne, etc... (01)

5,3

C'est la note, sur 10, que les praticiens attribuent à leur niveau de connaissance en matière de confidentialité des données personnelles de santé.

98 %

C'est la part des praticiens interrogés qui estiment que la protection des données personnelles de leurs patients est un sujet important.

53 %

C'est la part des praticiens interrogés qui reconnaissent ne pas savoir quelles données personnelles ils sont autorisés à collecter. (02)

(01) Source : CNIL
(02) Source : Sondage Doctolib

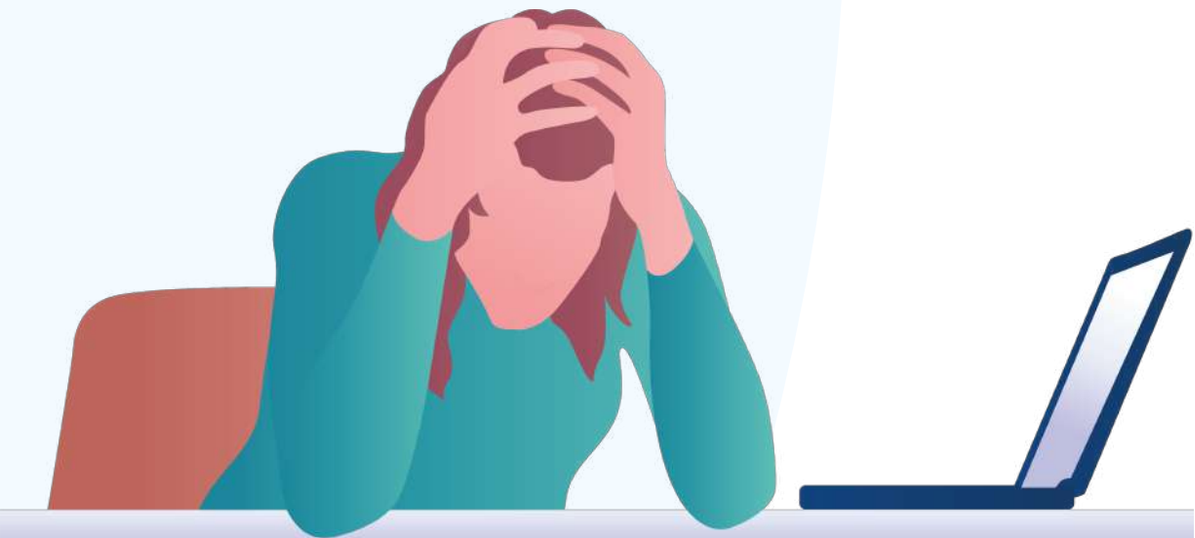
À quels moments recevez-vous des données de santé ?

- Lors de la consultation et la gestion du dossier patient ;
- Lors de l'utilisation d'une plateforme en ligne de gestion des rendez-vous ;
- Lors de la réalisation d'actes ou de consultations à distance (téléconsultation, télésurveillance, téléexpertise…) ;
- Lors d'échanges avec vos confrères, dans le cadre du parcours de soins du patient.

En tant que praticien,

vous traitez des données, il vous faut donc appliquer des mesures spécifiques pour assurer leur protection. L'enjeu, c'est d'une part de conserver le secret médical, et d'autre part, d'écarter toute altération des données pour offrir à vos patients les soins et traitements les plus adaptés possible.

Cédric Voisin
Responsable de la sécurité des systèmes d'information du groupe Doctolib



Pourquoi est-il important de protéger les données de santé ?

Les informations liées à la santé d'une personne n'appartiennent qu'à elle. La loi impose le respect de leur confidentialité de deux manières :

- **Le secret médical** prévoit que vos patients ont droit au respect de leur vie privée et au secret des informations les concernant. Toute divulgation, volontaire ou involontaire, constitue une entorse à la fois à la déontologie, mais aussi à la loi.
- **La sécurité des données** doit être garantie : qu'il s'agisse de ce qui vous aura été dit, ou de ce que vous aurez inscrit sur le dossier du patient, tout doit rester confidentiel. Les données des patients doivent être protégées contre des accès non autorisés ou illicites, contre la perte, la destruction ou les dégâts d'origine accidentelle.

La sécurité des données repose sur trois grands piliers :

- **la confidentialité :** la donnée ne regarde que la personne concernée
- **l'intégrité :** l'exactitude, la validité et la précision de la donnée doivent être garanties
- **la disponibilité :** la donnée doit être accessible à tout moment

Doctolib prend très à cœur le respect de ces trois piliers de la sécurité des données.

Ainsi, nous assurons :

- la confidentialité grâce à des mesures d'identification fortes (identification à double facteur, contrôle des accès…) et grâce au chiffrement de bout en bout des documents médicaux : seuls l'émetteur et le destinataire y ont accès.
- l'intégrité grâce au "hashing", une technique de chiffrement qui permet de s'assurer que les données ne sont pas altérées - sans pour autant que nous puissions consulter les données.
- la disponibilité grâce à un hébergement qui offre un taux de disponibilité moyen de 99,9 %. Notre logiciel est hautement disponible. Il n'y a que 52,6 minutes au cours de l'année pendant lesquelles il ne l'est pas (le 0,01 % manquant). Nous avons également pris soin de multiplier les sauvegardes, nous avons des équipes disponibles en permanence, un hébergement réparti sur plusieurs lieux, et nous procédons continuellement à des exercices de simulation pour nous améliorer.

Cédric Voisin
Responsable de la sécurité des systèmes d'information du groupe Doctolib

Comment réagir face à un piratage de données ?

Les données de santé sont des informations convoitées. L'informatisation du système de soins crée une certaine vulnérabilité et oblige à un souci permanent de sécurisation pour éviter les failles et limiter les intrusions. Les cyberattaques dans le monde de la santé (hôpitaux, laboratoires…) se sont multipliées ces dernières années, plus encore avec l'irruption de l'épidémie de Covid-19 en mars 2020. Toute porte entrebâillée sur un système informatique (mot de passe faible, absence de cryptage des données, pare-feu obsolète…) peut se transformer en accès libre pour un pirate.

Les attaques les plus fréquentes :

- **phishing ou hameçonnage :** tentative de récupération de données personnelles (coordonnées bancaires notamment) à travers un email usurpant l'identité d'un organisme connu (banque, organismes sociaux, service des impôts…).
  Que faire en cas d'attaque ?
  La CNIL recommande de :
  - signaler l'escroquerie auprès du site www.internet-signalement.gouv.fr ;
  - transférer les emails à votre service informatique ;
  - supprimer le message et vider votre corbeille ;
  - aller sur la plateforme cybermalveillance.gouv.fr pour obtenir de l'aide et des conseils pour identifier la nature de l'incident ;
  - contacter, si besoin, Info Escroqueries au 0 805 805 817.

- **ransomware ou rançongiciel :** infiltration d'un logiciel malveillant dans votre système informatique, à travers une clé USB, un fichier téléchargé, un email malveillant, etc. Ce programme crypte l'ensemble des données présentes sur votre ordinateur, bloque votre système et le rend hors d'usage. Une rançon est alors demandée pour le déverrouiller.
  Que faire en cas d'attaque ?
  La CNIL recommande de :
  - éteindre l'ensemble des appareils qui peuvent avoir été victimes de l'attaque ;
  - prévenir immédiatement son service informatique ;
  - éviter de payer la rançon demandée ;
  - conserver les preuves de l'attaque ;
  - déposer plainte auprès des services de police ou de gendarmerie ;
  - consulter le site cybermalveillance.gouv.fr pour recueillir de l'aide et des conseils et entrer en relation avec un professionnel spécialisé.

Bon à savoir :

en cas de violation de données, il vous revient de notifier l'incident à la CNIL dans les meilleurs délais. Un téléservice de notification en ligne est à votre disposition. Retrouvez plus d'informations et le détail de la marche à suivre sur le site de la CNIL.

+225 %

C'est l'augmentation du nombre de signalements d'attaque par rançongiciels recensés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) entre 2019 et 2020.

Il existe, malheureusement,

de très nombreux moyens de générer une fuite des données. Une vulnérabilité au sein de votre système peut constituer une porte d'entrée pour une attaque, qu'il s'agisse d'une exfiltration de données ou d'un chiffrement qui bloque tout votre système. C'est pourquoi il faut être sans cesse vigilant.

Cédric Voisin
Responsable de la sécurité des systèmes d'information du groupe Doctolib

Le risque de se faire pirater

est réel. Vous pouvez être victime d'un rançongiciel, d'un hacking… Il est difficile, pour un praticien, de tout sécuriser. Ou alors, il faut faire appel à un prestataire spécialisé, mais cela peut vite devenir un poste de dépense très important.

Dr Olivier Esnault
Chirurgien maxillo-facial et stomatologue à Paris

Les données

de santé, un bien sécurisé

La santé est un bien précieux. Les données de santé le sont tout autant. C'est pourquoi le législateur a mis en place une série de mesures de régulation afin d'assurer la sécurité et la protection des données des patients tout au long de leur parcours de soins. Votre cabinet est un maillon essentiel de cette chaîne. En tant que praticien, il vous incombe de garantir au mieux la sécurité des données, en vous prémunissant contre toute éventuelle attaque.

9 praticiens sur 10

savent qu'ils sont responsables de la sécurité des données personnelles de leurs patients.

66 %

des praticiens interrogés considèrent qu'ils sont en mesure de protéger correctement les données personnelles de leurs patients.

72 %

des praticiens interrogés indiquent connaître les gestes essentiels d'une bonne hygiène informatique.

Source : sondage Doctolib

RGPD, quatre lettres garantes de la protection des données

Entré en application le 25 mai 2018, le Règlement général sur la protection des données (RGPD) encadre le traitement des données personnelles à l'échelle européenne. Dans le sillage de la loi française Informatique et Libertés, adoptée en 1978, le RGPD garantit et renforce le contrôle par les citoyens de l'utilisation qui peut être faite de leurs données.

Tout organisme ou professionnel traitant des données y est soumis : les praticiens n'échappent pas à la règle.

Six grands principes doivent être respectés :

1. Seules les données nécessaires à votre activité de soins doivent être collectées. La finalité des données recueillies doit être claire, pertinente et légitime. En ce qui concerne les acteurs de la santé, il s'agit des données nécessaires à la bonne prise en charge des patients.

2. Les patients doivent être informés de l'utilisation qui sera faite de leurs données. Ainsi, ils conservent la maîtrise de leurs informations personnelles. Pour cela, une documentation détaillant leurs droits peut être mise à leur disposition dans votre salle d'attente.

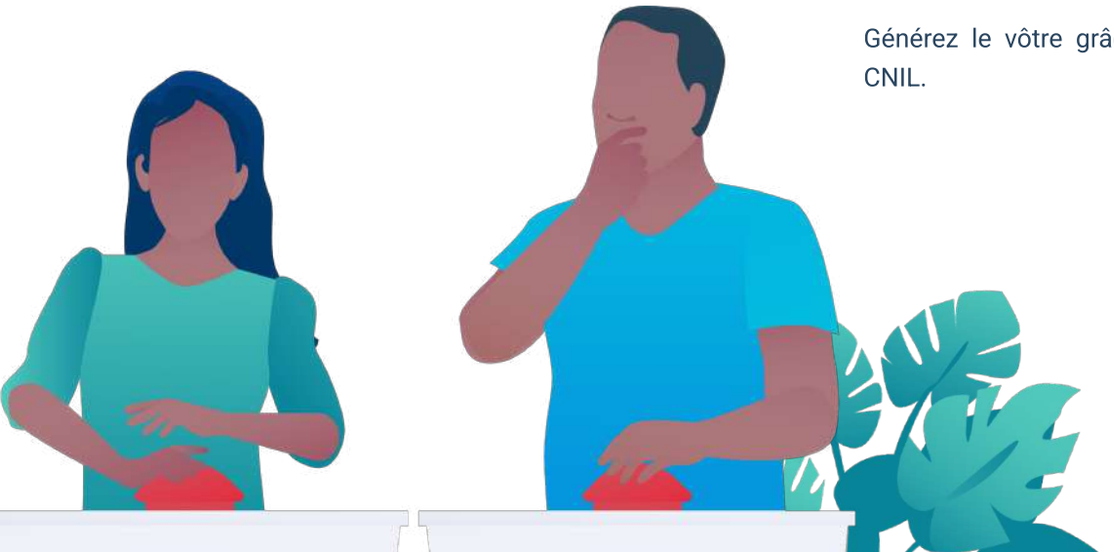
3. L'accès aux données doit être facilité. Vos patients doivent pouvoir consulter leurs données dans les meilleurs délais.

4. La durée de conservation des données doit être fixée et limitée au temps nécessaire à la réalisation de l'objectif visé. Dans le cadre de dossiers médicaux, le code de la santé publique fixe à 20 ans à compter de la date de la dernière consultation la durée de conservation des données. Les durées de conservation selon les situations (décès du patient, patient mineur, etc…) sont listées dans un référentiel de la CNIL.

5. Les données doivent être sécurisées et les risques, identifiés. Vous êtes responsable de la protection des données de vos patients. Ainsi, vous vous devez de prendre toutes les mesures utiles pour vous assurer que celles-ci sont bien gardées. Le partage des données, lorsqu'il est nécessaire, doit être limité aux seuls professionnels pour lesquels elles sont utiles.

6. Une mise à jour doit être effectuée continuellement. Votre mise en conformité est un travail quotidien, qui doit évoluer régulièrement, au gré des législations, des procédures de sécurité, etc…

Source : CNIL, CGM CompuGroup



Quiz : Évitez les comportements à risque

Comment puis-je créer un mot de passe fort (et dont je me rappelle) ?

La force d'un mot de passe dépend à la fois de sa longueur et de sa complexité. La CNIL considère qu'à partir de 12 caractères, mêlant majuscules, minuscules, chiffres et caractères spéciaux, un mot de passe peut résister aux attaques courantes.

D'autres mesures peuvent être ajoutées à la saisie du mot de passe : blocage du compte après plusieurs tentatives erronées, demande d'informations complémentaires…

Évitez tout mot de passe trop évident : 123456 (mot de passe le plus utilisé en France), azerty ou loulou. Oubliez également les mots de passe qui parlent de vous : votre nom, celui de votre cabinet, votre spécialité, le prénom de vos enfants...

Et pour s'en rappeler, comment fait-on ? La CNIL propose un générateur de mot de passe solide… et un moyen mnémotechnique pour s'en souvenir. Entrez une phrase de 12 mots, comprenant un nombre, une majuscule, un signe de ponctuation ou un caractère spécial, et laissez la magie opérer :

- Mon mot de passe est un secret bien gardé depuis 25 ans ! devient ainsi Mmdpeusbgd25a!
- Le carré de l'hypoténuse est égal à la somme des carrés des 2 autres côtés. devient Lcdl'heéàlsdcd2ac.

Générez le vôtre grâce à l'outil Phrase2passe de la CNIL.

Outre ces conseils de base, pour conserver un mot de passe inviolable, pensez également à :

- ne pas utiliser le même pour tous vos comptes ;
- ne pas les écrire sur des feuilles volantes, un post-it, dans votre téléphone ou dans un fichier texte sur votre ordinateur ;
- activez la double authentification ou authentification à deux facteurs (2FA) lorsque le service vous le propose ;
- utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe de façon sécurisée ;
- renouveler votre mot de passe régulièrement.

Quels moyens de communication puis-je utiliser pour échanger avec mes confrères soignants à propos d'un patient ?

Réservez l'usage des messageries instantanées comme WhatsApp, des SMS et de votre boîte mail classique à vos communications privées. Lorsque vous souhaitez échanger avec vos confrères soignants à propos d'un patient, utilisez une messagerie sécurisée.

Les pouvoirs publics ont mis en place le système de messagerie sécurisée de santé MSSanté. Au sein de cet espace, les professionnels exerçant en ville, à l'hôpital, dans les structures médico-sociales peuvent échanger par mail des données de santé dématérialisées en toute sécurité.

En 2021,

- 67 % des établissements de santé,
- 63 % des laboratoires de biologie médicale,
- 51 % des professionnels de santé libéraux,
- 34 % des EHPAD utilisent ce système.

Depuis l'entrée en vigueur du RGPD, il n'est plus nécessaire d'effectuer des formalités auprès de la CNIL pour utiliser cette messagerie. Le traitement des données en provenance du système doit cependant être inscrit sur votre registre des activités de traitement.

Reste que la messagerie MSSanté ne peut pas toujours être utilisée par l'ensemble de l'équipe soignante d'un patient. Les praticiens non professionnels de santé, comme les ostéopathes ou les psychologues, n'y ont pas accès. Aussi, pour fluidifier et sécuriser les échanges entre tous, Doctolib a mis au point Doctolib Team, une messagerie sécurisée, gratuite, accessible à l'ensemble des acteurs impliqués dans le parcours de soins du patient.

Découvrez Doctolib Team en vidéo

Comment puis-je assurer la sécurité des postes de travail au sein du cabinet ?

Adoptez de bonnes habitudes :

- programmez votre ordinateur afin qu'il se verrouille automatiquement au bout d'un certain laps de temps ;
- installez un pare-feu et des antivirus sur votre ordinateur et mettez-les à jour régulièrement. Mettez également à jour vos logiciels ;
- cloisonnez : utilisez un ordinateur pour vos activités professionnelles et un autre pour votre usage personnel ;
- stockez et sauvegardez les données sur un espace accessible en réseau ou en cloud plutôt que sur votre poste de travail uniquement ;
- limitez l'utilisation et la connexion de matériel sur votre poste (clé USB, disque dur externe).

Source : CNIL, CGM CompuGroup

La confidentialité des données à l'heure du numérique en santé

Au cours des dernières années, les outils numériques ont pris toute leur place dans les cabinets. La numérisation de la santé et la panoplie de solutions qu'elle offre pour la prise en charge des patients demandent une nouvelle vigilance et de nouveaux réflexes afin de garantir un usage sécurisé.

Qu'il s'agisse de la prise de rendez-vous en ligne ou de la téléconsultation, les mêmes règles de sécurité s'appliquent : collecte des données strictement nécessaires, traitements des données à inscrire dans un registre…

Le prestataire à qui vous faites confiance se doit d'assurer les mesures de sécurité et de confidentialité les plus hautes.

Depuis sa création en 2013, Doctolib a fait de la protection de la vie privée de ses utilisateurs une priorité absolue. Nous avons pris 11 engagements garantissant ce respect total :

1. Nous respectons l'ensemble des réglementations relatives à la confidentialité des données personnelles.
2. Les certifications obtenues (ISO/IEC 27001 et Hébergeur de données de santé) démontrent un engagement à long terme.
3. Nous collaborons avec 300 000 personnels de santé et avec les plus grands établissements de santé en Europe.
4. La confidentialité des données est au cœur de chacune de nos actions et nous travaillons en étroite collaboration avec des experts en sécurité et en droit lors du développement de nos services et pour tester et améliorer notre résistance en permanence.
5. Les données sont en lieu sûr. Nous sommes à l'avant-garde dans le domaine de l'hébergement (hébergeur certifié HDS et ISO/IEC 27001), le cryptage (bases de données chiffrées au repos, clés de cryptage stockées dans une entreprise tierce, chiffrement de bout en bout de tous les documents médicaux partagés via Doctolib), la protection (authentification à deux facteurs, protection intelligente contre les attaques DDoS et le scraping, pare-feux dernier cri pour le cloud).
6. Nous ne sommes pas propriétaires des données personnelles de nos utilisateurs, nous en sommes seulement les gardiens.
7. Le grand public peut vérifier à tout moment, à partir de son compte Doctolib, tous les paramètres de sécurité mis en place pour protéger ses données (chiffrement de bout en bout pour les documents médicaux, ajout d'un code d'accès à quatre chiffres pour limiter l'accès à l'application…).
8. Nous n'utilisons pas les données de santé de nos utilisateurs à des fins commerciales. C'est interdit par la loi. Le modèle économique de Doctolib n'est pas fondé sur la monétisation des données ou sur l'affichage de publicités : il repose uniquement sur un abonnement payé par les personnels et les établissements de santé afin d'utiliser les logiciels que Doctolib développe.
9. Nous n'utilisons plus de cookies marketing tiers à des fins publicitaires depuis juillet 2021.
10. Les données personnelles des patients leur permettent de créer un compte Doctolib, de prendre rendez-vous en ligne et d'interagir avec leurs praticiens, entre autres.
11. Les données de nos utilisateurs sont conservées aussi longtemps qu'elles sont utiles : tout compte inactif depuis 3 ans est supprimé. Un e-mail est envoyé au préalable pour les avertir.

Définir une nouvelle norme en matière de secret médical en ligne : Doctolib fait l'acquisition de Tanker

Après 3 années d'une collaboration fructueuse, Doctolib a fait l'acquisition, en janvier 2022, de Tanker, entreprise qui fournit l'une des technologies les plus fiables pour sécuriser les données sensibles : le chiffrement de bout en bout. Cette technique empêche tout accès non autorisé aux données chiffrées, en interne ou en externe, y compris par des tiers comme Tanker lui-même. Le rapprochement entre Doctolib et Tanker va permettre de déployer cette technologie de pointe à une échelle plus importante et de soutenir la croissance de Doctolib : le chiffrement de bout en bout continuera d'être mis en œuvre dans tous les services développés par Doctolib afin de sécuriser les données personnelles de santé, tant pour les 300 000 personnels de santé que pour les 60 millions de patients qui utilisent les services de Doctolib en France, en Allemagne et en Italie. Et plus encore : Doctolib va pouvoir accélérer le rythme de l'innovation et ira à terme au-delà du chiffrement de bout en bout. Les nouvelles équipes de Doctolib investissent d'ores-et-déjà dans des technologies de pointe telles que les enclaves sécurisées et le chiffrement homomorphe, afin de créer de nouvelles fonctionnalités avancées et sécurisées pour les patients et le personnel de santé. L'objectif de Doctolib est simple : définir une nouvelle norme du secret médical en ligne.

Je suis très sensibilisé

à la protection des données, depuis le début de mon exercice. J'ai été très vite informatisé et ai toujours mis en place des solutions de sauvegarde. Ma préoccupation était avant tout de ne pas perdre les données. Pour sécuriser mon cabinet, j'ai fait appel à un informaticien, qui a notamment supprimé tous les ports ouverts sur ma box Internet, je vais aussi installer un pare-feu physique. N'oublions pas non plus que la protection s'applique aussi aux données papiers : les documents doivent être sous clé.

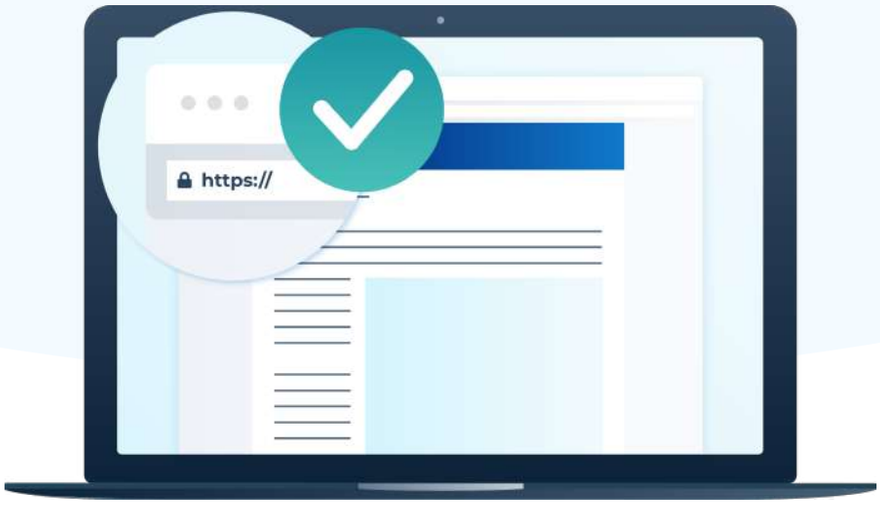
Dr Olivier Esnault
Chirurgien maxillo-facial et stomatologue à Paris

Quels sont les risques si je manque à mes obligations ?

Le non-respect de la réglementation en matière de protection des données personnelles peut conduire à des sanctions de la part de la CNIL : amendes administratives pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel, peines pénales de 5 ans d'emprisonnement et 300 000 euros d'amende pour une personne physique, 1,5 million d'euros pour une personne morale.

Vos patients

et leurs données



Vos patients utilisent de façon exponentielle le numérique en santé, plus encore depuis le début de la crise épidémique de la Covid-19 : applications santé, prise de rendez-vous en ligne, téléconsultation, sites d'informations santé… 88 % des Français utilisent au moins un service numérique dans le cadre de leur parcours de soin, selon un sondage réalisé par France Assos Santé en septembre 2021. Pour autant, leurs connaissances à propos des données de santé demeurent lacunaires.

Parce que les patients sont acteurs à part entière de la protection des données, les sensibiliser et les impliquer est essentiel. Soyez incollable sur le sujet !

Les patients et leurs données de santé…

… vus par les praticiens :

66 %
estiment que les patients ne semblent pas du tout préoccupés par le sujet

74 %
indiquent ne jamais être interrogés par leurs patients sur le sujet

15 %
savent parfaitement répondre aux questions des patients sur le sujet, 62 % partiellement

… vus par les patients eux-mêmes :

70 %
se disent très concernés par la protection de leurs données de santé

26 %
estiment que le sujet leur est très familier

61 %
souhaitent être mieux informés sur la confidentialité des données

66 %
font confiance à leur équipe soignante pour assurer la confidentialité de leurs données

Source : Sondages Doctolib

Les données de santé des patients en questions

Qui peut les consulter ?

Le patient et les praticiens pour qui elles sont pertinentes.

Comment sont-elles utilisées ?

Les données de santé collectées par l'équipe soignante ont une finalité précise et légitime : le bon suivi du patient dans son parcours de soins.

Où sont-elles stockées ?

Les données qui transitent par les services de Doctolib (à travers la prise de rendez-vous en ligne, la téléconsultation, le logiciel de gestion) sont stockées en France, à Paris, chez un hébergeur agréé. Cet hébergeur est certifié par le label français "HDS" (Hébergeur de Données de Santé), conformément à la loi et aux normes établies par l'Agence du numérique en santé, en concertation avec la CNIL. Notre hébergeur est aussi certifié par les principales normes internationales, dont la norme ISO/IEC 27001, et est audité chaque année par un organisme indépendant. Les centres de données bénéficient d'une sécurité physique 24/7 et de mesures de protection technologiques parmi les plus avancées au monde.

Comment sont-elles protégées ?

Les bases de données de Doctolib sont chiffrées au repos. Les clés de cryptage sont stockées chez un HSM (Hardware Security Module) externe, afin de renforcer les mesures de sécurité, en l'occurrence ATOS, une société française sous juridiction européenne. Ce système de protection nous permet d'empêcher l'accès aux données de santé de nos utilisateurs, même depuis notre fournisseur de solutions d'hébergement. Tous les documents hébergés sur Doctolib ainsi que les flux de téléconsultation sont chiffrés de bout en bout. Toutes les données partagées entre les différents logiciels développés par Doctolib sont cryptées.

Écoutez Jamy décrypter les données de santé

Les comptes Doctolib sont protégés par :

- Une authentification à 2 facteurs par défaut pour les comptes des patients et des praticiens.
- Une politique de mot de passe exigeante.
- Un processus sécurisé de récupération des comptes.
- Une gestion au cas par cas de l'accès à un compte utilisateur.
- Des notifications relatives à la sécurité pour les utilisateurs.

L'application Doctolib est protégée par :

- Des mises à jour de sécurité automatiques.
- Une protection intelligente contre les DDoS et le scraping.
- Un pare-feu professionnel pour les applications Web.

L'infrastructure Doctolib est protégée par :

- Des pare-feux dernier cri pour protéger les données transitant par le cloud.
- Des systèmes de détection et de prévention des intrusions.
- Des systèmes de filtrage d'accès.
- Un centre d'opérations de sécurité (SOC) 24h/24 et 7j/7.

Quels droits ont les patients sur leurs données ?

Les patients ont un droit d'accès, un droit à l'effacement, un droit de rectification et de limitation, et un droit d'opposition au traitement des données (pour motif légitime). Par ailleurs, Doctolib permet aux utilisateurs d'accéder aux données qu'ils ont renseignées à tout moment sur leur compte patient : grâce à un système de sauvegarde et de récupération automatique, ils peuvent les récupérer ou même les détruire 24h/24, en quelques clics. Pour toute demande concernant leurs données de santé (dossier médical, données de consultation, etc), Doctolib agissant en qualité de sous-traitant pour le compte des professionnels de santé, responsables de traitement, les patients doivent se rapprocher de ces derniers afin d'exercer leurs droits.

Offrez aux données

la meilleure des protections

Suivre quelques règles d'or et adopter de saines et durables habitudes peuvent considérablement diminuer les risques qui vous entourent. Les recommandations qui suivent doivent devenir des réflexes :

Maintenez votre hygiène informatique :

- votre login et votre mot de passe sont réservés à votre usage professionnel ;
- votre mot de passe est robuste ;
- vous utilisez une authentification à plusieurs facteurs dès que cela est possible ;
- vous n'installez pas de logiciels inconnus, ne cliquez pas sur des sites qui vous semblent louches ;
- vous mettez à jour régulièrement vos applications, votre système, votre antivirus ;
- vous sauvegardez vos données.

Faites-vous épauler par des experts :

- demandez de l'aide à un informaticien aguerri ;
- accordez votre confiance à des prestataires ayant de hauts standards de sécurité ;
- souscrivez une assurance cyber-sécurité.

Recommandations

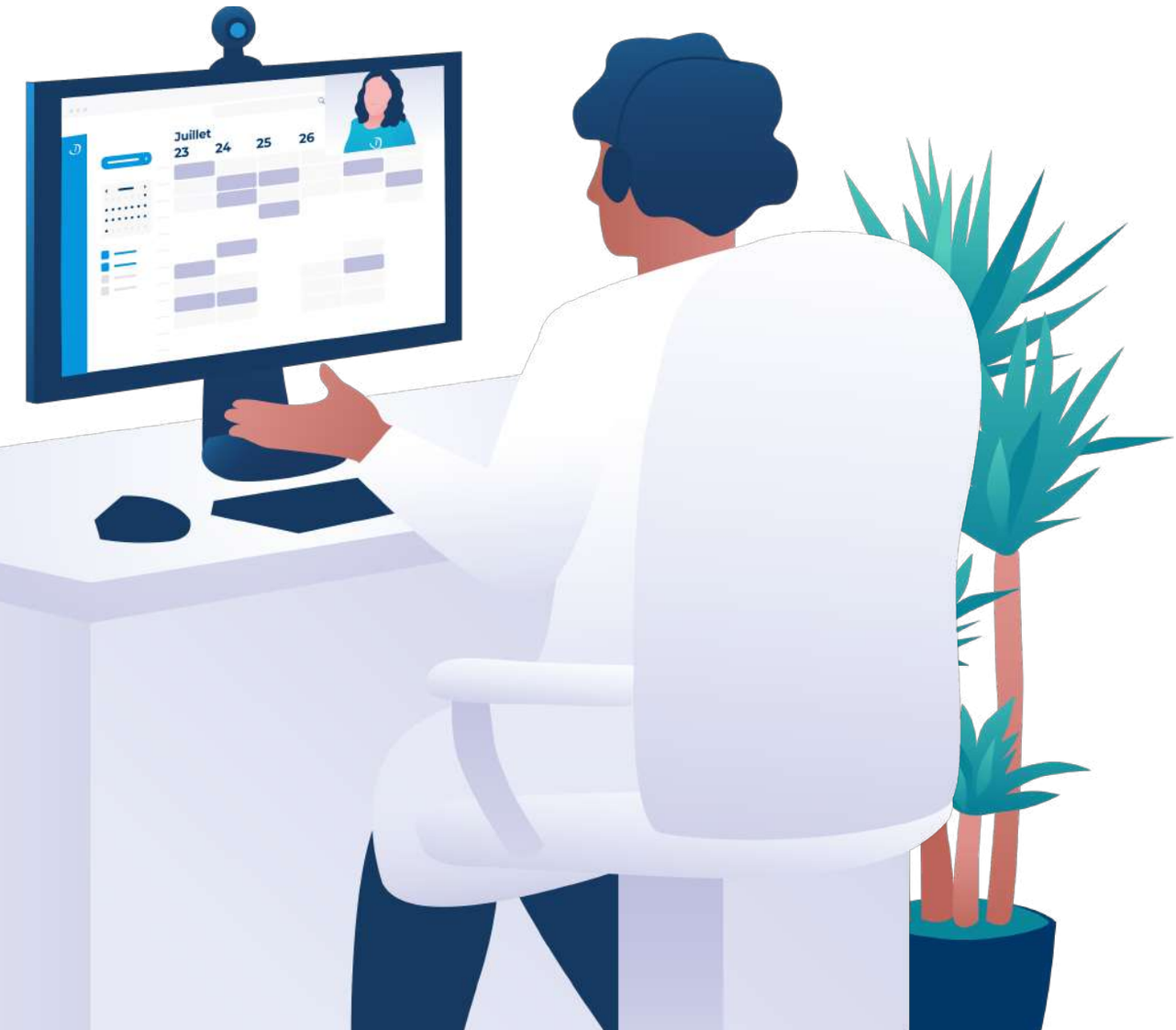
Il serait très utile aux professionnels de santé de pouvoir avoir accès à un référent informatique / RGPD au travers, par exemple, d'une association. Cela permettrait à chacun de bénéficier d'une vraie sécurisation de son cabinet.

Dr Olivier Esnault
Chirurgien maxillo-facial et stomatologue à Paris

Recommandations

Ne serait-ce que mettre en place les basiques de l'hygiène informatique permet de diminuer drastiquement les risques. À chacun de trouver un juste milieu entre ce qu'il souhaite protéger et les moyens à y consacrer.

Cédric Voisin
Responsable de la sécurité des systèmes d'information du groupe Doctolib



Doctolib à vos côtés

La confidentialité des données est une priorité absolue pour Doctolib. Plus de **300 000 personnels de santé** en France et en Allemagne nous font confiance et utilisent nos solutions. Plus de **60 millions de patients européens** ont un compte Doctolib et prennent leurs rendez-vous de santé en ligne.

Doctolib vous accompagne

Simplifiez votre quotidien avec nos solutions de gestion du cabinet intuitives nouvelle génération.

1. Gagnez en visibilité et optimisez votre activité

60 millions de patients gèrent leur santé avec Doctolib. Bénéficiez de cette visibilité pour communiquer sur vos expertises et créer une patientèle qualifiée.

2. Réduisez votre charge administrative et les rendez-vous non honorés

Parce que votre temps est précieux, Doctolib Patient vous fait gagner 1h30 par semaine grâce à la réservation en ligne et réduit de 60% les RDV non honorés.

3. Améliorez la prise en charge de vos patients

Offrez à vos patients de nouveaux services pour gérer plus simplement leur santé et celle de leur famille au quotidien.

Pour en savoir plus sur Doctolib et échanger avec un expert :

Contactez-nous

Échangez avec vos confrères

Partagez vos expériences et vos conseils avec vos pairs et accédez aux informations qui vous concernent sur Doctolab, votre média.

Restez à la pointe de l'actualité. Sur Doctolab, retrouvez des études, des guides pratiques, des interviews, des podcasts et de nombreux articles qui concernent votre quotidien.
Rejoignez la rédaction et contribuez à faire de Doctolab plus encore votre média.

Découvrez Doctolab

Echangez avec vos confrères sur de nombreux sujets, découvrez en avant-première les nouveautés Doctolib, participez à nos événements en rejoignant la Communauté Doctolib.

Rejoignez la Communauté