

# Confidentialité des données de santé :

## votre cabinet est-il un lieu sûr ? Testez vos connaissances !

Cochez les questions 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 ?
-  Connaissez-vous la date de la dernière mise à jour de votre pare-feu ?
-  Utilisez-vous votre propre nom ou celui de votre cabinet comme mot de passe ?
-  Savez-vous quand et comment supprimer les données de vos patients ?
-  Savez-vous quelles données vous pouvez demander à vos patients ?

Découvrez les réponses sur les pages suivantes !

## 👁️ Savez-vous ce qu'est le "phishing" ou un "rançongiciel" ?

Le phishing ou hameçonnage est une tentative de récupération de données personnelles à travers un email usurpant l'identité d'un organisme connu (banque, impôts...)

Un rançongiciel ou ransomware est un logiciel malveillant qui s'infiltre dans votre système informatique, via une clé USB, un téléchargement, un email malveillant... Ces programmes chiffrent vos données et bloquent votre système. Une rançon est demandée pour le déverrouiller. Ces deux attaques informatiques sont les plus fréquentes et chacun peut en être victime.

## 🔗 Pourriez-vous écrire en toutes lettres l'acronyme RGPD ?

Il s'agit du Règlement général sur la protection des données. Ce texte européen est entré en application le 25 mai 2018. Il encadre le traitement des données personnelles, garantit et renforce le contrôle par les citoyens européens 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.

## 📁 Sauriez-vous répondre aux questions de vos patients à propos de leurs données ?

Les patients interrogés par Doctolib se disent très concernés par la protection de leurs données de santé et souhaiteraient être davantage informés.

Pour en savoir plus sur la confidentialité des données et ainsi être en mesure de répondre à vos patients, l'animateur scientifique Jamy vous propose en vidéo une approche pédagogique de ce sujet complexe.

🎧 [Écoutez Jamy décrypter les données de santé](#)

## 🔑 Utilisez-vous votre propre nom ou celui de votre cabinet comme mot de passe ?

Il ne faudrait que 52 secondes à un pirate pour "cracker" un mot de passe de 8 caractères, selon une étude menée par les outils How secure is my password et Passfault Analyser. Plus un mot de passe est long et composé de majuscules, minuscules, chiffres et caractères spéciaux, et le moins évident est-il (le nom de votre cabinet par exemple), moins il a de risque d'être piraté.

## 👤 Savez-vous comment le RGPD s'applique dans votre cabinet ?

En tant que praticien, vous êtes amené à collecter et traiter des données personnelles, et notamment des données de santé, de vos patients. Responsable de leur traitement, il vous appartient de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection de ces données. Pour vous aider, la CNIL propose un [référentiel](#) pour se mettre en conformité.

## 🔒 Connaissez-vous la signification du signe 2FA ?

Cela signifie "Authentification à double facteur (2 Factor Authentication)". Il s'agit d'une technique de sécurisation d'un compte avec un mot de passe (le 1er facteur) et une deuxième authentification depuis un appareil tierce (le second facteur).

Par exemple, lorsqu'un patient se connecte à son compte Doctolib depuis un nouvel ordinateur, un code d'identification lui est envoyé sur son smartphone. Il lui suffit de l'entrer sur son ordinateur pour accéder à son compte Doctolib. Sans lui, aucune connexion n'est possible.

## 🗑️ Savez-vous quand et comment supprimer les données de vos patients ?

Le Conseil national de l'Ordre des médecins recommande de conserver pendant une durée de 20 ans les dossiers médicaux des patients à compter de la dernière consultation. Les données de rendez-vous, prises par Doctolib, sont conservées 5 ans par défaut, sauf instruction contraire du professionnel de santé.

## 📄 Savez-vous quelles données vous pouvez demander à vos patients ?

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.

## 🔒 Connaissez-vous la date de la dernière mise à jour de votre pare-feu ?

Installez et pensez à mettre régulièrement à jour votre pare-feu, votre antivirus et vos logiciels afin d'éviter toute faille de votre système, qui pourrait constituer une porte d'entrée pour un pirate informatique.

## En combien de temps votre mot de passe peut être piraté ?

Nombre de caractères	Chiffres seulement	Lettres minuscules et majuscules	Chiffres, lettres minuscules et majuscules	Chiffres, lettres minuscules et majuscules, caractères spéciaux
5	instantanément	instantanément	3 secondes	10 secondes
8	instantanément	3 heures	10 jours	46 jours
9	instantanément	4 jours	153 jours	12 ans
10	40 secondes	169 jours	1 an	928 ans
12	1 heure	600 ans	6000 ans	5 milliards d'années
15	46 jours	28 millions d'années	1 milliard d'années	2000 milliards d'années
17	12 ans	36 milliards d'années	6000 milliards d'années	14 quindécillions d'années

Source : [Seasoned Cyber Security Professionals](#)

