# Zoom sur la protection des données de santé :
## Quelles conséquences avec les prestataires de prise de rendez-vous ?

### Rappels généraux[1]

Les données de santé sont des données à caractère personnel particulières, car considérées comme sensibles.

La notion de données de santé est définie de façon très large par le règlement européen.
Cette notion recouvre les données collectées et produites dans le cadre du parcours de soins, mais aussi celles détenues par d'autres acteurs, comme par exemple les développeurs d'application.

**Que la prise de rendez-vous soit assurée par le cabinet ou par un prestataire tiers, vous restez « responsable de traitement » des données d'identification des patients et des données de santé collectées.[2]**

## ▶ Quelles sont vos obligations ?[2]

En tant que responsable de traitement, 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, sécurisation du planning et de son contenu, notification à la CNIL en cas de violation des données…

### Quelques bonnes pratiques relatives à la prise de rendez-vous

- Si la consultation ne nécessite pas de préparation au préalable ou la préparation d'outils spécifiques, les motifs de la consultation n'ont pas à être renseignés.
- Contrairement aux dossiers « patients » qui ont une durée de conservation assez longue, 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 des consultations sont, de toute manière, inscrites dans les dossiers de vos patients.
- Le prestataire est également responsable de traitement des données relatives aux comptes créés par les patients et les professionnels de santé.
- Les droits des patients sont identiques à ceux prévus pour les dossiers « patients ». Ils s'exercent auprès de vous de la même manière. Une information spécifique doit leur être délivrée.

[1] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante, page internet consultée le 27 mai 2020
[2] https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf, page internet consultée le 27 mai 2020

## ▶ Quelles sont les obligations du prestataire gérant la prise de RDV ?[2]

Le prestataire tiers agit pour votre compte. Il est considéré comme sous-traitant en vertu de la réglementation. Il doit être guidé par la volonté de protéger au mieux les informations concernant vos patients et de respecter la réglementation applicable.
Il ne peut ainsi utiliser les informations concernant vos patients que pour le strict accomplissement de ses missions.

**Le prestataire doit notamment mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité et la confidentialité des données confiées. Cela passe par la mise en place d'accès sécurisés, d'une politique d'habilitation (accès accordés aux personnes autorisées uniquement), d'un chiffrement des données (rendant impossible la lecture par un tiers ne possédant pas la clé de déchiffrement), d'une protection contre les attaques informatiques (antivirus, etc.).**

### Le contrat avec le prestataire

La relation avec votre prestataire doit être formalisée par **un contrat de sous-traitance.**
**Vous devez relire attentivement, avant toute signature**, **ce contrat** pour vérifier que le 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.

Le prestataire tiers, en cas d'incident lié aux données qu'il gère pour votre compte (faille de sécurité, piratage, perte, etc.), doit vous en informer dans les meilleurs délais, afin que vous remplissiez vos propres obligations à cet égard.

Si votre prestataire héberge informatiquement les informations issues de la prise de rendez-vous par vos patients, et notamment des données de santé, il doit faire appel à **un hébergeur de données de santé agréé ou certifié**.

## ▶ Pouvez-vous être sanctionné ?[2]

Les mêmes sanctions sont applicables en cas de non-respect de la réglementation dans le cadre de la prise de rendez-vous en ligne qu'en matière de gestion des dossiers « patients ». Si vous ne respectez pas vos obligations, vous pouvez faire l'objet d'une sanction administrative de la CNIL, voire d'une sanction pénale[3].
Si la CNIL vous met en demeure de vous conformer, vous avez encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction.

[3] La CNIL peut prononcer des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, 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.