Le RGPD en trois étapes

@marcsabek

Depuis le 25 mai dernier, le Règlement Général sur la Protection des Données personnelles (RGPD) est entré en application. Ce texte européen organise la gestion des informations personnelles détenues par les entreprises. Les interrogations des chirurgiens-dentistes se multiplient. Voici les réponses.

Le chirurgien-dentiste est-il concerné par le RGPD ?

Oui, comme tout professionnel utilisant et gérant des informations personnelles (données nominatives), le chirurgien-dentiste doit respecter le RGPD et veiller à son application.

De quelles données personnelles s'agit-il ? De celles des patients ?

Le RGPD concerne toutes les données personnelles collectées au cabinet dentaire. Celles des patients, bien sûr, mais également celles des salariés du chirurgien-dentiste, de ses fournisseurs aussi.

On entend par données personnelles toutes les informations concernant une personne physique identifiée ou identifiable, qu'elles soient sur support matérialisé (papier) ou dématérialisé (numérique).

Ces données, « collectées et traitées » par le chirurgien-dentiste, peuvent varier selon chaque catégorie.

=> Patients : des données administratives (nom, prénom, adresse, téléphone, profession, situation familiale, numéro de Sécurité sociale, etc.), des données médicales générales (informations relatives aux problèmes de santé, historique médical, médication en cours, etc.), des données médicales bucco-dentaires (tout le dossier clinique…).

=> Salariés : des données administratives essentiellement (nom, prénom, adresse, téléphone, profession, situation familiale, numéro de Sécurité sociale, etc.).

=> Fournisseurs : des données administratives limitées au champ professionnel (nom, prénom, fonction, téléphone, courriel, etc.).

Quelles sont les obligations du chirurgien-dentiste pour gérer toutes ces données ?

Le RGPD rappelle une question fondamentale, simple et de bon sens ; respecter les principes de protection des données personnelles : finalité, pertinence et proportionnalité, conservation limitée, sécurité (voir encadré « Sécurité des données personnelles »), confidentialité et respect des droits des personnes.

En pratique, le chirurgien-dentiste suivra une règle en 7 points.

Sécurité des données personnelles

Quelles mesures ?

Le RGPD n'y change rien. Ce sont des recommandations posées par la CNIL et que le chirurgien-dentiste doit appliquer pour protéger les données en sa possession et assumer sa responsabilité.

Parmi les principales mesures recommandées on peut rappeler :

- utiliser un mot de passe conforme aux recommandations de la CNIL ;
- donner à chaque salarié un mot de passe à usage individuel ;
- paramétrer un verrouillage de la session informatique automatiquement après 30 minutes d'inactivité ;
- utiliser un antivirus et un pare-feu ;
- effectuer des sauvegardes régulières des données et les conserver dans un lieu sécurisé, externe au cabinet ;
- assurer le chiffrement des données communiquées avec un logiciel adapté ;
- limiter la connexion d'appareils non professionnels au réseau du cabinet dentaire ;
- protéger les dossiers papiers des patients en un lieu sécurisé ;
- ne pas conserver de données personnelles des patients (ou des salariés) sur son téléphone mobile ou tablette ;
- privilégier les messageries électroniques sécurisées.

Des données personnelles conservées, jusqu'à quand ?

=> Les dossiers des patients doivent, en principe, être conservés pour une durée indéterminée. On admet cependant, conformément à l'usage instauré par l'Ordre des chirurgiens-dentistes (et l'Ordre des médecins) par référence à l'article R.1112-7 du Code de la santé publique, que les dossiers médicaux des patients doivent être conservés pendant vingt ans à compter de leur dernière consultation.

=> Les données des salariés peuvent être conservées jusqu'à ce qu'ils quittent le cabinet. Par la suite, il est recommandé d'archiver les données des salariés sans les détruire, en gardant en perspective les délais de prescription des actions.

=> Les données des fournisseurs sont conservées tant que la relation commerciale perdure.

1. Rédiger une **procédure interne** décrivant comment les informations personnelles sont collectées et traitées au cabinet dentaire.

Un **registre** des activités de traitement des données permet de noter et de recenser l'ensemble des traitements mis en œuvre. Ce registre constitue également la preuve de la conformité du praticien au RGPD ; il sera présenté en cas de contrôle.

2. Dans les grands cabinets de plusieurs praticiens, il pourrait être nécessaire de désigner un chirurgien-dentiste **délégué à la protection des données**. Son rôle est de veiller au respect du RGPD, en formant les autres praticiens et les salariés, en appliquant la procédure interne, l'adaptant à l'évolution de l'exercice et des règles, etc.

3. Respecter les **droits des patients** tels qu'ils figurent dans le Code de santé publique : droit à l'information (expliquer pourquoi des infos sont collectées, au besoin au moyen d'une affichette), droit d'accès, rectification ou de suppression, droit d'opposition pour motif légitime. Le RGPD ajoute le droit à la portabilité des données et le droit à l'oubli. La procédure interne du cabinet et le logiciel de gestion doivent intégrer ces deux droits, en préciser les modalités d'application pratique (par exemple, pourquoi le droit à l'oubli est tempéré lorsque les données médicales doivent être conservées, etc.)

4. Évaluer le **risque de sécurité** des données et le risque juridique pour les personnes en charge de leur traitement. En pratique, envisager les conséquences d'une perte (d'un vol, d'une détérioration, etc.) des données.

5. Revoir si nécessaire le contrat avec le **prestataire de services** informatiques (éditeur de logiciel, hébergeur de cloud, etc.). Des clauses garantissant que le prestataire respecte le RGPD doivent être explicites.

6. Ajuster régulièrement la procédure interne pour garantir la sécurité et la confidentialité des données. Il s'agit de fixer une **durée de conservation** (voir encadré « Données personnelles conservées, jusqu'à quand ? ») pour chaque catégorie de données, d'organiser les modalités d'archivage, d'assurer la capacité de restitution des données, etc.

7. Tous les **incidents de sécurité** impliquant des données personnelles doivent être signalés à la CNIL.