

Le RGPD appliqué au cabinet

“ **Référentiel BTS — BC4 / C4.7** « Accéder aux données de santé numériques dans le respect de la réglementation ».

“ **L'essentiel** : le RGPD ne dit pas « interdit de traiter des données ». Il dit : **sachez pourquoi vous les traitez, n'en collectez pas plus que nécessaire, ne les gardez pas indéfiniment, et soyez capable de le prouver.**

Objectif

À la fin de cette page, vous savez :

- nommer les principes du RGPD et les appliquer à un dossier d'appareillage ;
- identifier la **base légale** des traitements d'un cabinet ;
- fixer une **durée de conservation** et savoir ce qui se passe ensuite.

Le vocabulaire minimum

Terme	Définition	Au cabinet
Donnée personnelle	Toute information se rapportant à une personne identifiée ou identifiable	Nom, NIR, téléphone, mais aussi un scan 3D ou une photo clinique
Donnée sensible	Catégorie particulière, dont les données de santé	Diagnostic, mesures, appareillage délivré, ordonnance
Traitement	Toute opération sur des données : collecte, consultation, stockage, envoi, suppression	Créer une fiche, facturer, télétransmettre, archiver
Responsable de traitement	Celui qui décide des finalités et des moyens	Le cabinet (la structure, via son dirigeant)
Sous-traitant	Celui qui traite pour le compte du responsable	L'éditeur du logiciel, l'hébergeur, le cabinet comptable

Les données de santé sont par principe **interdites de traitement**, sauf exceptions — dont la principale ici : le traitement **nécessaire aux fins de médecine préventive, de diagnostic, de prise en charge sanitaire**, par un professionnel soumis au secret. C'est ce qui rend l'activité du cabinet licite.

Les six principes, appliqués à l'appareillage

1. Licéité, loyauté, transparence — le patient sait quelles données sont recueillies et pourquoi. D'où l'obligation d'une **mention d'information** (voir page suivante).

2. Finalité déterminée — chaque donnée est collectée **pour un but précis** et ne peut être réutilisée pour un autre sans réexamen. *Exemple* : les coordonnées recueillies pour la prise en soins ne peuvent pas servir à une campagne commerciale sans base distincte.

3. Minimisation — on ne collecte que le **nécessaire**. La question test : *à quoi cette information me sert-elle concrètement ?* *Exemple* : la profession du patient est pertinente si elle conditionne le choix de l'appareil ; sa situation familiale détaillée, rarement.

4. Exactitude — les données doivent être à jour : adresse, droits, mutuelle, mais aussi l'**identité** du patient, dont l'exactitude conditionne tout le reste. Une donnée de santé rattachée au mauvais dossier est à la fois une erreur de traitement et un risque pour le patient.

5. Limitation de la conservation — on ne garde pas tout, pour toujours.

6. Intégrité et confidentialité — sécurité des données ; c'est l'objet du livre *Formation métier — Sécurité numérique*.

À quoi s'ajoute la **responsabilité** (*accountability*) : être capable de **démontrer** que tout cela est respecté — d'où le registre des traitements.

Les bases légales du cabinet

Ce n'est presque jamais le consentement.

Traitement	Base légale
------------	-------------

Dossier patient, prise en soins	Obligation légale / mission d'intérêt public en matière de santé ; le dossier est d'ailleurs imposé par l'article 21 de l'arrêté du 1 ^{er} février 2011
Facturation, comptabilité, télétransmission	Obligation légale
Gestion des rendez-vous, relation client	Intérêt légitime ou exécution du contrat
Envoi d'une enquête de satisfaction, newsletter	Consentement — libre, spécifique, révocable
Photos cliniques utilisées en formation ou en communication	Consentement explicite et distinct, par écrit

Conséquence pratique : un patient ne peut pas « retirer son consentement » au dossier patient, parce que ce dossier ne repose pas sur son consentement. En revanche, il peut **s'opposer** à une newsletter ou refuser l'usage de ses photos — et cela ne change rien à sa prise en charge.

Combien de temps garde-t-on les données ?

Le principe est qu'une durée doit être **déterminée, justifiée et écrite** dans le registre. Les repères usuels :

Donnée	Repère
Dossier de prise en soins	Conservé pendant toute la durée du suivi puis archivé ; la durée retenue doit tenir compte du suivi de l'appareillage (renouvellements, garantie, responsabilité) et des délais de prescription en matière de responsabilité médicale
Pièces comptables et factures	10 ans (obligation du code de commerce)
Données de facturation / télétransmission	Le temps nécessaire au recouvrement et aux contrôles
Candidatures non retenues	Quelques mois, sauf accord de la personne
Vidéosurveillance , le cas échéant	Quelques semaines au plus

“ **△ Points de vigilance.** Les durées applicables au dossier de santé varient selon le statut de la structure et évoluent : la durée retenue par le cabinet doit être **écrite, justifiée et vérifiée** auprès de la CNIL, de l'organisation professionnelle ou d'un conseil — ce n'est pas un chiffre à retenir par cœur. Et « archiver » n'est pas « laisser dans la base courante » : les dossiers clos doivent être **séparés** de l'actif, avec des accès restreints.

Au terme de la durée : **suppression** ou **anonymisation** véritable (une donnée anonymisée ne permet plus, par aucun moyen, de remonter à la personne — sinon elle reste personnelle).

Ce que le cabinet doit avoir mis en place

- Une **mention d'information** affichée et remise aux patients.
- Un **registre des traitements** (page *Registre, DPO et violations de données*).
- Des **durées de conservation** définies et appliquées.
- Des **contrats de sous-traitance** conformes avec l'éditeur, l'hébergeur, le comptable.
- Des **habilitations** limitées au besoin d'en connaître, et une **traçabilité** des accès.
- Une procédure pour répondre aux **demandes des patients** dans un délai d'un mois.

À retenir

- **Finalité, minimisation, durée limitée, sécurité, preuve** : les cinq réflexes.
- La base légale du dossier patient est l'**obligation légale, pas le consentement**.
- Le consentement est réservé à ce qui est **facultatif** (photos en communication, newsletter).
- Les **durées de conservation** doivent être **écrites et justifiées** — et vérifiées, car elles évoluent.
- Le cabinet est **responsable de traitement** ; l'éditeur et l'hébergeur sont **sous-traitants**.

Revision #5

Created 2026-09-15 17:24:30 UTC by Antoine

Updated 2026-09-16 07:03:19 UTC by Antoine