CHECKLIST

Checklist RGPD du cabinet

Douze points à vérifier une fois par an. Les repères viennent du référentiel de la CNIL pour les cabinets médicaux et paramédicaux.

Cabinet _____ Revue faite le _____ Prochaine revue _____

- ☐ **1. Tenez un registre des traitements**
  Rendez-vous, dossiers, comptabilité : finalité, données, destinataires, durées, mesures de sécurité.
  RGPD, art. 30 ; modèle de registre de la CNIL

- ☐ **2. Ne collectez que le nécessaire**
  Des données utiles à la prise en charge, à jour, au bon endroit.
  RGPD, art. 5 (minimisation)

- ☐ **3. Informez vos patients**
  Affiche en salle d'attente ou document remis : responsable, finalités, base légale, destinataires, durées, droits, réclamation à la CNIL.
  RGPD, art. 13 ; référentiel CNIL, § 8

- ☐ **4. Répondez aux demandes de droits**
  Accès, rectification, effacement, limitation, opposition : réponse dans un délai d'un mois, prolongeable de deux mois.
  RGPD, art. 12 et 15 à 21

- ☐ **5. Fixez vos durées de conservation**
  Repère CNIL pour le dossier : 20 ans après la dernière prise en charge, dont 5 en base active. Pièces comptables : 6 ans.
  Référentiel CNIL, § 7 ; LPF, art. L102 B

- ☐ **6. Encadrez vos sous-traitants**
  Logiciel, hébergeur, secrétariat à distance : un contrat qui reprend les clauses de l'article 28.
  RGPD, art. 28

- ☐ **7. Faites héberger chez un hébergeur certifié**
  Les données de santé hébergées pour votre compte le sont chez un hébergeur certifié HDS.
  Code de la santé publique, art. L1111-8

- ☐ **8. Maîtrisez les accès**
  Un identifiant par personne, des mots de passe solides, une double authentification ; le secrétariat ne voit que l'administratif.
  Référentiel CNIL, § 10

- ☐ **9. Sécurisez postes, tablettes et sauvegardes**
  Verrouillage automatique, chiffrement, mises à jour, sauvegardes régulières stockées en lieu sûr.
  Référentiel CNIL, § 10

- ☐ **10. Sécurisez les échanges**
  Pas de données de santé en clair par e-mail : messagerie sécurisée ou fichier chiffré, secret envoyé par un autre canal.
  Référentiel CNIL, § 10

- ☐ **11. Protégez les locaux et le papier**
  Armoire fermée à clé, écran hors de vue, documents récupérés à l'impression, broyeur.
  Référentiel CNIL, § 10

- ☐ **12. Préparez la gestion d'une violation**
  Perte, vol, piratage : notez l'incident et notifiez la CNIL dans les 72 heures s'il présente un risque pour les patients.
  RGPD, art. 33 et 34

> **DPO et analyse d'impact** : la CNIL indique qu'ils ne sont pas exigés d'un praticien exerçant seul ; elle les estime nécessaires pour des professionnels en cabinet groupé qui partagent un système d'information, au-delà de 10 000 patients par an.
>
> Le référentiel de la CNIL vise les professionnels de santé libéraux ; les ostéopathes n'y sont pas cités. Il reste le repère le plus proche.