

Sécurité numérique — à lire en premier

“ **Référentiel BTS Orthoprothésiste** (arrêté du 27 novembre 2024) — **BC3**, compétences **C3.5** « Concevoir et maintenir sécurisé son environnement numérique de travail » et **C3.6** « Se prémunir et réagir face aux incidents numériques ».

“ **L'essentiel** : un cabinet d'orthoprothèse détient des **données de santé**, la cible la plus recherchée par les attaquants. La sécurité n'est pas l'affaire du prestataire informatique : elle repose d'abord sur **les gestes quotidiens de l'équipe**.

Pourquoi ce livre existe

Le secteur de la santé est l'un des plus attaqués en France. Les structures visées ne sont pas seulement les hôpitaux : les **petites structures** sont des cibles de choix, parce qu'elles détiennent des données sensibles avec des moyens de défense réduits.

Pour un cabinet d'orthoprothèse, une attaque réussie, c'est :

- des **dossiers patients chiffrés** et inaccessibles — plus de mesures, plus d'historique, plus de plannings ;
- une **activité arrêtée** — on ne peut plus facturer, ni commander, ni savoir qui vient demain ;
- une **fuite de données de santé** — avec obligation de notifier la CNIL et, souvent, d'informer les patients ;
- une **perte de confiance** durable, et un coût financier qui met en jeu la survie de la structure.

La compétence **C3.5** demande de savoir **concevoir et maintenir** un environnement de travail sûr ; la **C3.6**, de savoir **réagir** quand quelque chose arrive. Ce livre couvre les deux.

Le principe qui résume tout

“ On ne protège pas un ordinateur, on protège une activité de soin.

Chaque mesure décrite ici se justifie par une question simple : *si cet élément disparaît ou tombe entre de mauvaises mains, que devient la prise en soins des patients ?*

Les pages de ce livre

1. **Concevoir son environnement numérique de travail** — postes, comptes, réseau, matériel personnel.
2. **Mots de passe et authentification** — la première ligne de défense, et la plus souvent négligée.
3. **Reconnaître les menaces** — hameçonnage, rançongiciel, fraude, supports amovibles.
4. **Réagir à un incident** — les premiers gestes, qui prévenir, quoi tracer.
5. **Sauvegardes et continuité d'activité** — travailler quand l'informatique est à l'arrêt.
6. **Mémo — l'hygiène numérique au quotidien** — la fiche à afficher au cabinet.

Lien avec les autres livres

- La **protection juridique** des données (RGPD, secret professionnel, violation de données) est traitée dans *Formation métier — Données de santé & réglementation*. Sécurité et réglementation sont deux faces d'un même sujet : l'une décrit **comment** protéger, l'autre **ce que la loi exige**.
- L'**authentification par carte CPS** relève du même sujet : c'est une authentification à deux facteurs, décrite dans la page *Mots de passe et authentification*.

À retenir

- Les **petites structures de santé sont des cibles**, pas des exceptions.
- La sécurité repose sur des **gestes d'équipe**, pas sur un seul outil ni sur un seul prestataire.
- Deux compétences complémentaires : **prévenir** (C3.5) et **réagir** (C3.6).