Formation métier — Sécurité numérique

Environnement de travail, mots de passe, menaces, réaction aux incidents, sauvegardes (BTS : BC3 / C3.5 - C3.6).

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).

Concevoir son environnement numérique de travail

> **Référentiel BTS — BC3 / C3.5** « Concevoir et maintenir sécurisé son environnement numérique de travail ».

> **L'essentiel :** un environnement de travail sûr se construit sur trois principes — **chacun n'a accès qu'à ce dont il a besoin**, **chaque équipement est connu et tenu à jour**, **rien de professionnel ne transite par du matériel ou des services personnels**.

Objectif

À la fin de cette page, vous savez :

- appliquer le principe du **moindre privilège** aux comptes d'un cabinet ;
- lister les équipements à inventorier et à maintenir ;
- dire pourquoi le matériel personnel et le cloud grand public posent problème.

1. Des comptes nominatifs, pas de compte partagé

Le compte partagé est l'erreur fondatrice. Un identifiant `cabinet` / `cabinet` utilisé par tout le monde, c'est :

- l'impossibilité de savoir **qui** a consulté ou modifié un dossier — la traçabilité exigée par la réglementation disparaît ;
- un mot de passe que personne ne change jamais, et que les anciens salariés connaissent encore ;
- une responsabilité impossible à établir en cas d'incident.

La règle : un compte **par personne**, avec un **profil de droits** adapté à son rôle.

Rôle	Ce qu'il lui faut	Ce qu'il ne lui faut pas
Orthoprothésiste	Dossiers patients, consultations, appareils, devis	Paramétrage comptable, gestion des utilisateurs
Technicien d'atelier	Dossiers de fabrication, planning, stock	Données de facturation et de droits sociaux
Secrétariat / administratif	Identité, droits, rendez-vous, facturation	Contenu clinique détaillé au-delà du nécessaire
Gérant	Tableaux de bord, comptabilité, utilisateurs	Un accès « tout » permanent : privilégier un compte courant + un compte d'administration séparé
Apprenti / stagiaire	Accès **restreint et temporaire**, sous tutorat	Droits de suppression, exports de masse

Le départ d'un salarié est un événement de sécurité : désactivation du compte le jour même, restitution des cartes et du matériel, changement des accès qu'il partageait.

2. Un parc connu et tenu à jour

On ne sécurise pas ce qu'on ne connaît pas. Tenez un **inventaire simple** : chaque poste, tablette, téléphone professionnel, imprimante, scanner 3D, machine d'atelier connectée, avec son responsable et sa version de logiciel.

Les gestes de maintenance :

- **Mises à jour automatiques** activées, système et applications — la majorité des attaques exploitent des failles **déjà corrigées**.
- **Antivirus / protection** actif et à jour sur chaque poste.
- **Verrouillage automatique** de session après quelques minutes d'inactivité, et verrouillage manuel dès qu'on quitte le poste (un poste ouvert à l'accueil est lisible par tous les patients qui passent).
- **Chiffrement du disque** sur les portables et les tablettes — un ordinateur volé dans une voiture ne doit pas livrer les dossiers.
- **Fin de vie** : un poste réformé ou revendu doit être **effacé de façon sûre**, pas simplement « vidé de la corbeille ».

3. Le réseau

- **Changer les mots de passe par défaut** de la box et des équipements réseau.
- **Séparer le Wi-Fi visiteurs** du réseau du cabinet. Les patients en salle d'attente n'ont rien à faire sur le réseau qui porte les dossiers.
- **Pas d'accès à distance ouvert « pour dépanner »** sans contrôle : un accès de télémaintenance doit être nominatif, limité dans le temps et tracé.
- Les **machines d'atelier connectées** (imprimante 3D, fraiseuse, scanner) sont souvent anciennes et non mises à jour : les isoler sur un segment réseau à part.

4. Matériel personnel et services grand public

C'est le point le plus sensible en petite structure, parce qu'il part toujours d'une bonne intention : « je finis le dossier chez moi », « je m'envoie la photo sur mon téléphone ».

Ce qui ne doit pas se faire :

- envoyer des données patient sur une **boîte mail personnelle** ;
- stocker des photos cliniques ou des scans 3D sur un **cloud grand public** non conforme à l'hébergement de données de santé ;
- utiliser une **messagerie instantanée grand public** pour transmettre un nom de patient avec une information de santé ;
- travailler sur un **ordinateur familial** partagé, sans compte séparé ;
- brancher une **clé USB personnelle** sur un poste du cabinet.

Ce qu'il faut à la place : un poste ou une session professionnelle, la **MSSanté** pour les échanges, un hébergement **certifié HDS** pour les données de santé (voir *Formation métier — Données de santé & réglementation*), et un accès distant maîtrisé si le télétravail est nécessaire.

> Le smartphone professionnel utilisé en visite à domicile mérite le même soin qu'un poste fixe : code de déverrouillage, chiffrement, effacement à distance en cas de perte, pas d'installation d'applications hors usage professionnel.

5. Les prestataires

Le cabinet travaille avec un éditeur de logiciel, parfois un infogérant, un hébergeur. Cela **ne transfère pas la responsabilité** : le cabinet reste responsable de traitement.

À exiger d'un prestataire : un **contrat écrit** précisant la sécurité et la sous-traitance au sens du RGPD, la **localisation** et la **certification HDS** de l'hébergement, les **modalités de sauvegarde et de restauration**, et la **réversibilité** (récupérer ses données si l'on change de prestataire).

À retenir

- **Un compte par personne**, des droits adaptés au rôle, désactivation au départ.
- **Mises à jour, verrouillage, chiffrement** : trois gestes qui couvrent la majorité des risques courants.
- **Wi-Fi visiteurs séparé**, machines d'atelier isolées.
- **Aucune donnée de santé** sur matériel personnel, mail personnel ou cloud grand public.
- Un prestataire est **sous-traitant**, pas responsable à votre place : contrat, HDS, réversibilité.

Mots de passe et authentification

> **Référentiel BTS — BC3 / C3.5** « Concevoir et maintenir sécurisé son environnement numérique de travail ».

> **L'essentiel :** un mot de passe protège un dossier patient exactement comme une serrure protège un local. La **longueur** compte plus que la complexité, la **réutilisation** est le vrai danger, et l'**authentification à plusieurs facteurs** rend le vol de mot de passe presque sans effet.

Objectif

À la fin de cette page, vous savez :

- construire un mot de passe robuste et mémorisable ;
- expliquer pourquoi réutiliser un mot de passe est le risque principal ;
- utiliser un gestionnaire de mots de passe et l'authentification à plusieurs facteurs.

Comment un mot de passe est réellement cassé

Trois méthodes, par ordre de fréquence :

1. **La réutilisation.** Un site de commerce se fait pirater, votre adresse et votre mot de passe se retrouvent dans une liste publique. L'attaquant les essaie **partout ailleurs**. Si le mot de passe du logiciel métier est le même que celui d'un forum, la protection est nulle, quelle que soit sa complexité.

2. **L'hameçonnage.** On vous le demande, et vous le donnez. Aucune longueur ne protège de cela (voir la page *Reconnaître les menaces*).
3. **La force brute / le dictionnaire.** L'essai automatique de milliards de combinaisons et de mots courants. C'est **la longueur** qui y résiste, pas les caractères exotiques.

Construire un bon mot de passe

La règle courte : long, unique, et jamais deviné à partir de vous.

- **Longueur d'abord** : visez **au moins 12 à 15 caractères**. Une phrase de passe fonctionne très bien — *« MonChatDort3FoisParJour! »* est à la fois plus long, plus mémorisable et plus solide que *« Xk7$p2 »*.
- **Unique par service** : c'est le point non négociable.
- **Rien de personnel** : prénom des enfants, date de naissance, nom du cabinet, plaque d'immatriculation. Ces éléments se trouvent en quelques minutes.
- **Pas de variation évidente** : `Cabinet2024!` puis `Cabinet2025!` n'est pas un changement de mot de passe.

Ce qui a changé depuis les vieilles consignes : on ne recommande plus le **changement périodique obligatoire** sans raison. Il pousse aux variantes prévisibles et notées sur un papier. On change un mot de passe **quand il y a une raison** : soupçon de compromission, départ d'un collègue qui le connaissait, service piraté.

Le gestionnaire de mots de passe

Retenir 30 mots de passe uniques est impossible. C'est exactement ce que résout un **gestionnaire de mots de passe** : un coffre chiffré qui les stocke tous, protégé par **un seul** mot de passe très solide (celui-là, on le retient) et idéalement une seconde vérification.

Il génère aussi des mots de passe aléatoires, les remplit automatiquement — ce qui, au passage, **protège de l'hameçonnage** : le gestionnaire ne remplit rien sur un faux site, parce que l'adresse ne correspond pas.

Ce qu'il ne faut pas faire à la place : le fichier `mots de passe.xlsx` sur le bureau, le carnet dans le tiroir de l'accueil, le post-it sous le clavier, l'enregistrement dans un navigateur partagé par plusieurs personnes.

L'authentification à plusieurs facteurs (MFA / 2FA)

Principe : pour se connecter, il faut **deux preuves de nature différente** —

- quelque chose que **je sais** (mot de passe),
- quelque chose que **je possède** (téléphone, carte CPS, clé de sécurité),
- quelque chose que **je suis** (empreinte, visage).

Un mot de passe volé ne suffit alors plus. C'est la mesure qui offre le meilleur rapport effort/protection.

En santé, vous l'utilisez déjà : la **carte CPS** et son équivalent mobile l'**e-CPS** sont des authentifications à deux facteurs — quelque chose que l'on **possède** (la carte, ou le téléphone) et quelque chose que l'on **sait** (le code), parfois complété par la biométrie. C'est pour cela qu'une carte CPS volée sans son code ne permet rien.

À activer partout où c'est proposé : messagerie professionnelle, banque, portail de l'éditeur, outils d'administration.

> ⚠ Un code reçu par SMS est **mieux que rien**, mais moins sûr qu'une application d'authentification ou une clé physique. Et un code de validation **ne se communique jamais** à quelqu'un qui vous appelle, quel que soit le motif invoqué.

Cas particuliers du cabinet

- **Le compte d'administration** du logiciel ou du système ne sert **qu'à administrer** : on ne travaille pas au quotidien avec.
- **Les comptes de service** (sauvegarde, interface comptable) doivent avoir des mots de passe propres, longs, stockés dans le coffre — pas le mot de passe du gérant.
- **La continuité** : les accès critiques doivent être récupérables si le gérant est absent ou empêché. Un coffre partagé avec accès d'urgence, ou une procédure écrite déposée en lieu sûr, évite la paralysie.

À retenir

- **Long, unique, impersonnel** : dans cet ordre.
- La **réutilisation** est le risque n°1, devant la complexité.
- **Gestionnaire de mots de passe** : la seule méthode réaliste pour tenir l'unicité.
- **Authentification à deux facteurs** partout où c'est possible — la CPS en est une.
- On **ne change plus pour changer** : on change quand il y a une raison.

Reconnaître les menaces

> **Référentiel BTS — BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** presque toutes les attaques réussies commencent par **une action humaine** — un clic, une pièce jointe ouverte, un virement accepté. Savoir reconnaître le scénario est donc la protection la plus efficace.

Objectif

À la fin de cette page, vous savez :

- identifier les principales familles d'attaques qui visent une structure de santé ;
- repérer les signaux d'alerte d'un message frauduleux ;
- nommer ce qui, dans un cabinet d'orthoprothèse, constitue une cible.

Ce qui intéresse un attaquant dans un cabinet

- Les **données de santé** — nominatives, sensibles, impossibles à changer (contrairement à un numéro de carte bancaire). Elles se revendent et servent au chantage.
- Les **coordonnées bancaires** du cabinet et des fournisseurs.
- L'**arrêt de l'activité** lui-même : un cabinet paralysé est prêt à payer vite.
- Le cabinet comme **rebond** vers un partenaire plus gros (établissement de santé, fournisseur).

1. L'hameçonnage (phishing)

Un message imite un interlocuteur de confiance — la banque, l'Assurance Maladie, l'éditeur du logiciel, un fournisseur, la direction — pour obtenir un identifiant, un mot de passe, un paiement, ou faire ouvrir une pièce jointe.

Les signaux d'alerte :

Signal	Exemple
Urgence et menace	« Votre compte sera suspendu sous 24 h », « dernier rappel avant poursuite »
Demande d'identifiants	Un lien vers une page de connexion qui ressemble à celle que vous connaissez
Adresse d'expéditeur approximative	`ameli-remboursement.net` au lieu du domaine officiel ; nom affiché correct mais adresse réelle différente
Pièce jointe inattendue	Une « facture » d'un fournisseur avec qui vous n'avez rien en cours
Contexte qui ne colle pas	Un organisme qui vous écrit sur un canal qu'il n'utilise jamais
Français maladroit	Moins fiable qu'avant — beaucoup de messages sont désormais parfaitement rédigés

Le réflexe : ne jamais utiliser le lien du message. **Revenir au canal connu** — taper soi-même l'adresse du site, appeler le numéro habituel du fournisseur (pas celui indiqué dans le message).

Variantes : **smishing** (par SMS), **vishing** (par téléphone, souvent un « technicien informatique » très serviable), **hameçonnage ciblé** (le message mentionne votre nom, votre poste, un dossier réel — il faut supposer que l'attaquant s'est renseigné).

2. Le rançongiciel (ransomware)

Le scénario le plus redouté. Un programme chiffre l'ensemble des fichiers — dossiers patients, modèles 3D, comptabilité, sauvegardes accessibles depuis le réseau — puis réclame une rançon. De plus en plus souvent, les données sont **aussi volées** avant d'être chiffrées, avec menace de publication : c'est la **double extorsion**.

Comment il entre : pièce jointe ou lien d'hameçonnage, accès distant mal protégé, faille non corrigée sur un équipement exposé, mot de passe faible sur un compte d'administration.

Ce qui limite les dégâts : des **sauvegardes déconnectées** du réseau (voir *Sauvegardes et continuité d'activité*), des comptes à droits limités, un parc à jour, une segmentation réseau.

Faut-il payer ? Les autorités le déconseillent : payer ne garantit ni la restitution, ni l'absence de publication, finance l'activité criminelle et désigne le cabinet comme une cible qui paie. La décision

appartient au dirigeant, mais elle se prend **après** le dépôt de plainte et le signalement, pas dans la panique.

3. La fraude au virement

Pas de logiciel malveillant ici — de la manipulation. Deux formes :

- **Fraude au changement de RIB** : un « fournisseur » écrit que ses coordonnées bancaires ont changé. Le virement suivant part sur le compte de l'escroc.
- **Fraude au président** : un message qui semble venir du dirigeant demande un virement urgent et confidentiel.

La parade est organisationnelle, pas technique : tout changement de coordonnées bancaires est vérifié par **rappel téléphonique au numéro déjà connu** — jamais celui du message. Et aucun virement exceptionnel sans **double validation**.

4. Les supports amovibles et le matériel

- Une **clé USB trouvée** ou reçue en cadeau ne se branche pas sur un poste du cabinet.
- Une clé utilisée chez un fournisseur puis rebranchée au cabinet transporte ce qu'elle a croisé.
- Un **ordinateur ou un téléphone volé** non chiffré livre directement les dossiers.

5. Les risques internes et involontaires

Toutes les pertes de données ne sont pas des attaques :

- l'**erreur de destinataire** — un compte rendu envoyé au mauvais patient ;
- la **curiosité** — consulter le dossier d'une connaissance ; c'est tracé, et c'est une faute grave ;
- la **perte** d'un document papier, d'un téléphone, d'un carnet de rendez-vous ;
- la **conversation à voix haute** à l'accueil, entendue de la salle d'attente. Le secret professionnel ne s'arrête pas à l'écran.

Ces événements peuvent constituer des **violations de données** au sens du RGPD (voir *Formation métier — Données de santé & réglementation*).

À retenir

- La porte d'entrée la plus fréquente est **un humain qui clique**, pas une faille exotique.
- Face à une demande urgente : **ralentir** et **revenir au canal connu**.
- Un **changement de RIB** se vérifie toujours par téléphone au numéro déjà connu.
- Le rançongiciel se combat **avant** : sauvegardes déconnectées, mises à jour, droits limités.
- L'incident interne involontaire est aussi fréquent que l'attaque — et relève des mêmes obligations.

Réagir à un incident

> **Référentiel BTS — BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** face à un incident, les premières minutes comptent. Trois réflexes : **isoler**, **alerter**, **ne rien détruire**. Et une règle : on **ne gère pas seul**, on applique une procédure décidée à froid.

Objectif

À la fin de cette page, vous savez :

- exécuter les premiers gestes face à un incident numérique ;
- dire qui prévenir, dans quel ordre, et dans quels délais ;
- distinguer l'incident technique de la **violation de données personnelles**.

Reconnaître qu'il se passe quelque chose

Signaux qui doivent déclencher l'alerte, même en cas de doute :

- des fichiers **renommés ou illisibles**, une note de rançon à l'écran ;
- l'ordinateur **anormalement lent**, des fenêtres qui s'ouvrent seules, un curseur qui bouge seul ;
- une **connexion inconnue** signalée sur un compte, ou un mot de passe qui ne fonctionne plus ;
- des **messages partis de votre boîte** que vous n'avez pas écrits ;
- un **document envoyé au mauvais destinataire**, un **téléphone ou un portable perdu** ;
- un patient qui signale avoir reçu un message étrange « de votre part ».

>

> Le pire réflexe est le silence. Beaucoup d'incidents s'aggravent parce que la personne qui a cliqué a eu honte de le dire. **Le cabinet doit poser explicitement qu'un signalement rapide ne sera jamais reproché** — c'est une règle de management autant que de sécurité, et elle doit être dite à l'équipe avant l'incident, pas après.

Les premiers gestes

1. Isoler — déconnecter le poste concerné du réseau : câble réseau débranché, Wi-Fi coupé. Objectif : empêcher la propagation aux autres postes et au serveur.

2. Ne pas éteindre (sauf consigne contraire d'un professionnel) — l'extinction peut détruire des traces utiles à l'analyse. Isoler ≠ éteindre.

3. Ne rien « nettoyer » — ne pas supprimer les fichiers suspects, ne pas vider les journaux, ne pas réinstaller dans la précipitation. Ce sont des **preuves**, nécessaires pour comprendre l'étendue et pour la plainte.

4. Alerter — le responsable désigné dans le cabinet, puis le prestataire informatique ou l'éditeur.

5. Tracer — noter par écrit, au fil de l'eau : **date et heure**, ce qui a été constaté, par qui, ce qui a été fait. Ce journal sera indispensable pour la CNIL, l'assurance et la plainte.

6. Changer les mots de passe concernés — **depuis un autre poste**, sain.

Qui prévenir

Destinataire	Quand	Pourquoi
Responsable interne / dirigeant	Immédiatement	Il décide et engage la structure.
Prestataire informatique / éditeur	Immédiatement	Diagnostic, endiguement, restauration.
CNIL	**Sous 72 h** après en avoir pris connaissance, si des **données personnelles** sont touchées et que le risque pour les personnes n'est pas négligeable	Obligation légale (notification de violation de données).
Les personnes concernées (patients)	Sans délai, si le risque est **élevé** pour elles	Obligation légale ; leur permettre de se protéger.

Destinataire	Quand	Pourquoi
Dépôt de plainte (police, gendarmerie)	Rapidement	Nécessaire pour l'assurance, et pour l'action pénale.
cybermalveillance.gouv.fr	En parallèle	Aide au diagnostic, annuaire de prestataires de proximité.
CERT Santé / ARS	Selon le statut de la structure	Le signalement des incidents graves de sécurité des SI relève de l'article **L. 1111-8-2** du code de la santé publique, dont le champ (établissements de santé, médico-sociaux, laboratoires…) est précisé par le décret n° 2022-715 du 27 avril 2022. Une petite structure libérale n'entre pas nécessairement dans ce champ, mais peut solliciter l'appui du CERT Santé.
Assureur	Selon le contrat, souvent sous quelques jours	Déclaration de sinistre, garantie cyber le cas échéant.

> ⚠ Le délai de **72 h** vers la CNIL court **à partir du moment où la structure a connaissance** de la violation — pas à partir de la fin de l'analyse. En cas d'incertitude sur l'ampleur, on notifie et on complète ensuite.

Incident technique ou violation de données ?

Les deux ne se recouvrent pas :

- Un serveur qui tombe en panne sans fuite ni perte est un **incident technique** : pas de notification CNIL, mais un enjeu de **continuité d'activité**.
- Un compte rendu envoyé au mauvais patient est une **violation de données** sans la moindre attaque informatique.
- Un rançongiciel est **les deux à la fois** : indisponibilité **et**, très souvent, fuite de données.

La qualification détermine les obligations. Elle se documente dans le **registre des violations**, que toute structure doit tenir — même pour les incidents non notifiés à la CNIL (voir *Formation métier — Données de santé & réglementation*).

Après : le retour d'expérience

Un incident correctement traité se termine par une analyse à froid, en équipe :

1. **Par où est-ce entré ?**
2. **Qu'est-ce qui a fonctionné** dans notre réaction, et **qu'est-ce qui a manqué** (numéro introuvable, sauvegarde non testée, personne ne savait qui prévenir) ?
3. **Quelles mesures** on met en place, avec un responsable et une date.
4. **Mise à jour de la procédure**, et information de toute l'équipe.

À retenir

- **Isoler, ne pas éteindre, ne rien effacer, alerter, tracer.**
- **72 h** pour notifier la CNIL en cas de violation de données personnelles à risque.
- **Déposer plainte** et conserver les preuves.
- Un incident se **documente** et se **débriefe** : c'est ce qui évite le suivant.
- Signaler vite doit être **encouragé**, jamais sanctionné.

Sources

- Le cadre législatif — Portail du CERT Santé
- Article L. 1111-8-2 du code de la santé publique — Légifrance

Sauvegardes et continuité d'activité

> **Référentiel BTS** — **BC3 / C3.5** et **C3.6**. Voir aussi **BC4 / C4.3** « Participer à la gestion administrative de la structure ».

> **L'essentiel :** la sauvegarde est la **seule** protection qui fonctionne encore quand tout le reste a échoué. Mais une sauvegarde **jamais testée** et **connectée au réseau** ne protège de rien : le rançongiciel la chiffre aussi.

Objectif

À la fin de cette page, vous savez :

- appliquer la règle **3-2-1** ;
- dire pourquoi une sauvegarde doit être testée et déconnectée ;
- construire un **mode dégradé** permettant de recevoir les patients sans informatique.

La règle 3-2-1

Chiffre	Signification	En pratique dans un cabinet
3	Au moins **3 copies** des données	L'original + 2 sauvegardes
2	Sur **2 supports différents**	Le serveur/poste + un disque externe, ou un service de sauvegarde en ligne
1	Dont **1 hors site**	Un disque emporté et rangé ailleurs, ou une sauvegarde chez un hébergeur — protège aussi de l'incendie, du dégât des eaux et du vol

À quoi certains ajoutent un **« 1 » de plus : une copie déconnectée** (hors ligne, *offline*). C'est le point décisif contre le rançongiciel : un disque branché en permanence sur le réseau est chiffré en même temps que le reste.

Les questions à trancher, à froid

1. **Que sauvegarde-t-on ?** Pas seulement la base du logiciel métier : aussi les **modèles 3D** , les **photos cliniques**, les **documents scannés**, la **comptabilité**, les **fichiers d'atelier**, et les **paramétrages**. Un point souvent oublié : la liste des accès et des contrats.
2. **À quelle fréquence ?** Répondez par une autre question : **combien de travail acceptez-vous de perdre ?** Une sauvegarde quotidienne signifie qu'on peut perdre une journée d'activité.
3. **En combien de temps peut-on repartir ?** Restaurer 500 Go depuis un service en ligne peut prendre plus d'une journée. Ce délai doit être **connu à l'avance**, pas découvert le jour de l'incident.
4. **Qui vérifie ?** Une sauvegarde doit être **surveillée** — beaucoup de structures découvrent qu'elle avait cessé de fonctionner des mois plus tôt.
5. **Combien de temps garde-t-on les sauvegardes ?** Assez longtemps pour revenir **avant** une corruption découverte tardivement.

Tester la restauration

> **Une sauvegarde qui n'a jamais été restaurée n'est pas une sauvegarde : c'est une hypothèse.**

Au moins **une fois par an** — et après tout changement majeur — restaurez réellement un jeu de données sur un environnement de test, et vérifiez que les fichiers s'ouvrent. Notez la date du test et le temps qu'il a pris.

Ce test répond à des questions qu'on ne se pose jamais autrement : la sauvegarde contient-elle vraiment les photos ? l'éditeur est-il joignable pour réinstaller le logiciel ? où est la licence ?

Le mode dégradé : travailler sans informatique

C'est la partie **métier** du sujet, et celle que l'examen attend. Un cabinet doit pouvoir continuer à recevoir des patients pendant plusieurs jours sans accès au logiciel.

À préparer **maintenant**, pas le jour J :

- **Le planning du lendemain imprimé** chaque soir — sinon, personne ne sait qui vient.
- Les **coordonnées** des patients des jours à venir, accessibles hors ligne.
- Des **formulaires papier** : fiche de mesures, bon de livraison, feuille de soins de secours, reçu.
- Les **numéros essentiels** sur papier : prestataire informatique, éditeur, assureur, fournisseurs principaux, CNIL.
- Une **consigne d'accueil** : que dit-on aux patients ? qui décide de reporter ?
- La **saisie de rattrapage** : qui ressaisira les actes réalisés en mode dégradé, et quand ?

> Point de vigilance réglementaire : en mode dégradé, on continue de traiter des données de santé **sur papier**. Les mêmes exigences de confidentialité s'appliquent — les feuilles ne restent pas sur le comptoir, et elles sont détruites ou classées correctement après ressaisie.

Cas des données hébergées chez un tiers

Si le logiciel est en ligne, la sauvegarde est assurée par l'hébergeur — **vérifiez-le par contrat**, ne le supposez pas. Trois points à faire écrire :

- la **fréquence** et la **durée de rétention** des sauvegardes ;
- le **délai de restauration** garanti ;
- la **réversibilité** : sous quel format et dans quel délai récupérez-vous vos données si vous changez de prestataire ou si l'éditeur cesse son activité ?

À retenir

- **3-2-1**, plus une copie **déconnectée**.
- Une sauvegarde **non testée** ne compte pas.
- On sauvegarde **aussi** les modèles 3D, les photos et les paramétrages.
- Le **mode dégradé papier** se prépare à froid : planning imprimé, formulaires, numéros.
- En hébergement externe : **sauvegarde, délai de restauration et réversibilité par contrat**.

Mémo — l'hygiène numérique au quotidien

> **Référentiel BTS** — **BC3 / C3.5** et **C3.6**. Page de synthèse, conçue pour être **imprimée et affichée** au cabinet.

> **L'essentiel :** douze gestes. Ils ne demandent ni budget ni compétence technique, et couvrent la majorité des incidents réels.

Les douze gestes

Mon poste

1. **Je verrouille ma session** dès que je quitte mon poste — même pour deux minutes, même à l'atelier.
2. **Je laisse les mises à jour se faire.** Je ne repousse pas indéfiniment le redémarrage.
3. **Je ne branche pas de clé USB** dont je ne connais pas l'origine.

Mes accès

4. **Un compte par personne.** Je n'utilise pas celui d'un collègue et je ne prête pas le mien.
5. **Un mot de passe long et unique par service**, rangé dans le gestionnaire — pas sur un post-it.
6. **Ma carte CPS ne quitte pas ma poche** et ne reste jamais dans le lecteur quand je pars.

Mes échanges

7. **Données de santé nominatives = MSSanté.** Jamais de mail personnel, jamais de messagerie grand public.
8. **Je vérifie le destinataire** avant d'envoyer un document. Deux secondes qui évitent une violation de données.
9. **Je ne parle pas d'un patient à voix haute** à l'accueil, au téléphone en salle d'attente, ou en atelier porte ouverte.

Ma vigilance

10. **Message urgent, inattendu, qui demande un identifiant ou un paiement : je ralentis.** Je reviens au canal connu.
11. **Tout changement de RIB se vérifie par téléphone** au numéro que je connais déjà.
12. **Au moindre doute, je le dis tout de suite.** Signaler vite n'est jamais une faute ; se taire aggrave tout.

Les quatre choses que la structure doit avoir

À vérifier une fois, puis chaque année :

☐ Une **sauvegarde 3-2-1**, dont une copie **déconnectée**, **testée** dans les 12 derniers mois.

☐ Une **liste des comptes** à jour, avec désactivation systématique au départ d'un salarié.

☐ Une **fiche réflexe incident** affichée, avec les numéros à appeler.

☐ Un **mode dégradé papier** prêt : planning imprimé chaque soir, formulaires, coordonnées.

Les trois numéros à avoir sous la main

À compléter par l'établissement :

	Nom	Téléphone
Prestataire informatique / éditeur		

	Nom	Téléphone
Responsable sécurité / dirigeant		
Assureur (garantie cyber)		

Ressources publiques : **cybermalveillance.gouv.fr** (diagnostic et assistance), **cnil.fr** (notification de violation de données), **cyberveille-sante.gouv.fr** (CERT Santé).

À retenir

Si vous ne deviez en retenir que trois :

1. **Je verrouille ma session.**
2. **Un mot de passe unique par service, dans un gestionnaire.**
3. **Je ralentis devant l'urgence, et je signale au moindre doute.**