Formation métier — Données de santé & réglementation

Secret professionnel, RGPD, droits du patient, registre et violations, hébergement HDS (BTS : BC4 / C4.7).

Données de santé & réglementation — à lire en premier

> **Référentiel BTS Orthoprothésiste** (arrêté du 27 novembre 2024) — **BC4**, compétence **C4.7** « Accéder aux données de santé numériques dans le respect de la réglementation ». Contribue aussi à **C1.4** « Informer la personne prise en soins et son entourage ».

> **L'essentiel :** une donnée de santé n'appartient pas au professionnel qui la détient. Elle appartient à la personne, et la loi encadre strictement **qui peut y accéder, pourquoi, combien de temps, et où elle est stockée**.

Pourquoi ce livre existe

Le livre *Formation métier — Sécurité numérique* explique **comment** protéger les données. Celui-ci explique **ce que la loi exige**, et **ce à quoi le patient a droit**. Les deux sont indissociables : une mesure de sécurité sans base juridique est arbitraire, une obligation juridique sans mesure technique est un vœu.

Trois régimes se superposent, et c'est leur articulation qui pose difficulté :

Régime	Ce qu'il protège	Texte de référence
Le secret professionnel	Tout ce que le professionnel apprend de la personne, par quelque moyen que ce soit	Code de la santé publique ; article 15 de l'arrêté du 1er février 2011 pour l'orthoprothésiste
Le RGPD et la loi Informatique et Libertés	Le traitement des **données personnelles**	Règlement (UE) 2016/679

Régime	Ce qu'il protège	Texte de référence
Les règles propres aux données de santé	L'**hébergement**, le **partage** et l'**échange** entre professionnels	Code de la santé publique (HDS, équipe de soins)

Le fil conducteur

Toutes les règles de ce livre découlent de trois idées simples :

1. **On n'accède qu'à ce dont on a besoin, pour la personne qu'on prend en soins.** La curiosité n'est pas une finalité légitime.
2. **La personne sait et peut agir.** Elle est informée, elle consulte, elle fait rectifier, elle s'oppose.
3. **Tout laisse une trace.** Les accès sont journalisés ; c'est la contrepartie du droit d'accéder.

Les pages de ce livre

1. **Le secret professionnel et le partage d'informations** — jusqu'où puis-je parler du patient, et à qui.
2. **Le RGPD appliqué au cabinet** — finalités, bases légales, minimisation, durées de conservation.
3. **Les droits du patient sur ses données** — information, accès, rectification, opposition, accès au dossier médical.
4. **Registre, DPO et violations de données** — ce que la structure doit tenir et déclarer.
5. **L'hébergement des données de santé (HDS)** — où sont mes données, et chez qui.
6. **Traçabilité et habilitations dans le logiciel** — la traduction concrète, avec renvois vers WinOrtho.

Ce que ce livre n'est pas

Ce n'est pas un cours de droit, et il ne remplace pas l'avis d'un juriste ni d'un délégué à la protection des données. Il vise le niveau attendu d'un **professionnel bien formé** : savoir ce qui est permis, ce qui ne l'est pas, et **à quel moment il faut demander conseil**.

À retenir

- Trois régimes se superposent : **secret professionnel**, **RGPD**, **règles santé**.
- La donnée appartient à **la personne**, pas au cabinet.
- Trois idées commandent tout : **besoin d'en connaître**, **droits de la personne**, **traçabilité**.

Le secret professionnel et le partage d'informations

> **Référentiel BTS** — **BC4 / C4.7**. Voir aussi **BC1 / C1.5** « Apporter des conseils et une expertise auprès des professionnels de santé ».

> **L'essentiel :** l'orthoprothésiste est **tenu au secret professionnel**. Le secret n'est pas levé parce qu'on parle à un autre soignant : le partage n'est licite que s'il est **nécessaire à la prise en soins** et que le patient en est **informé**.

Objectif

À la fin de cette page, vous savez :

- dire ce que couvre le secret professionnel et qui y est tenu ;
- distinguer **échange** et **partage** d'informations ;
- appliquer la règle du **besoin d'en connaître** dans les situations courantes du cabinet.

Qui est tenu au secret, et sur quoi

L'**article 15 de l'arrêté du 1er février 2011** relatif aux professions de prothésiste et orthésiste pour l'appareillage des personnes handicapées énonce que ces professionnels sont **tenus au secret professionnel**.

Le secret couvre **tout ce qui est venu à la connaissance du professionnel** dans l'exercice de son activité : ce que le patient a dit, ce qui a été constaté, mais aussi **le simple fait qu'une personne soit suivie au cabinet**, son adresse, ses rendez-vous, son état de santé apparent.

Y sont tenus **tous les membres de l'équipe**, pas seulement les diplômés : secrétaire, technicien d'atelier, apprenti, stagiaire, personnel d'entretien qui passe dans les bureaux. C'est pourquoi la **clause de confidentialité** figure au contrat de travail et que l'engagement est rappelé aux

stagiaires dès leur arrivée.

Le secret **ne cesse pas** : ni à la fin de la prise en charge, ni au départ du salarié, ni au décès du patient.

Échange, partage : deux mots précis

Le code de la santé publique distingue :

- l'**échange** — une transmission **ciblée**, d'un professionnel à un autre professionnel identifié, à propos d'un patient déterminé ;
- le **partage** — la mise à disposition d'informations au sein d'une **équipe de soins** (dossier partagé, DMP).

Dans les deux cas, trois conditions :

1. **La finalité** : l'information doit être **nécessaire à la prise en soins** de la personne. Pas « utile à savoir », pas « intéressant ».
2. **La pertinence** : on transmet ce qui est **strictement nécessaire**, pas le dossier entier.
3. **L'information du patient** : il doit savoir que ces échanges ont lieu, et il peut **s'y opposer**.

Quand le professionnel destinataire **ne fait pas partie de l'équipe de soins**, le **consentement** du patient est requis.

Le besoin d'en connaître, au cabinet

Situation	Licite ?
Écrire au médecin prescripteur pour signaler une intolérance à l'appareil	**Oui** — échange nécessaire à la prise en soins, avec un professionnel identifié, dans l'équipe.
Transmettre au kinésithérapeute qui suit le patient les caractéristiques de l'orthèse délivrée	**Oui**, dans les mêmes conditions.
Demander au technicien d'atelier de préparer un appareil : il voit le nom et les mesures	**Oui** — il participe à la prise en charge, avec l'information dont il a besoin.

Situation	Licite ?
Consulter le dossier d'une voisine, par curiosité	**Non.** Faute grave, et accès tracé.
Répondre au conjoint qui appelle pour savoir si le patient est bien venu	**Non**, sans l'accord du patient — même le fait qu'il soit suivi est couvert.
Envoyer un devis à l'employeur qui finance	**Seulement** avec l'accord explicite du patient, et limité au nécessaire.
Répondre à l'assurance du patient qui demande des pièces	Ce sont **au patient** de transmettre ce qu'il souhaite ; le cabinet ne communique pas directement.
Raconter un cas en formation, sans nom	**Oui**, si le cas est réellement **anonymisé** — attention aux détails qui ré-identifient (pathologie rare, contexte local).
Parler d'un patient dans le couloir, ou à l'accueil avec un tiers à portée d'oreille	**Non.** La confidentialité vaut aussi à l'oral.

Les situations sensibles

- **Le mineur** — l'information est due aux titulaires de l'autorité parentale. L'adolescent peut demander la confidentialité sur certains éléments ; en cas de doute, on en réfère au médecin.
- **Le majeur protégé** — la personne chargée de la mesure de protection a accès dans les limites de sa mission ; la personne reste informée de façon adaptée.
- **La personne de confiance** — désignée par le patient, elle l'accompagne et peut être consultée s'il ne peut plus exprimer sa volonté ; elle n'a pas pour autant accès à tout le dossier.
- **L'aidant présent en consultation** — sa présence suppose l'accord du patient, redemandé s'il y a doute.
- **Après le décès** — les ayants droit peuvent obtenir certaines informations pour des motifs limités (connaître les causes du décès, défendre la mémoire du défunt, faire valoir leurs droits), sauf opposition exprimée de son vivant.

Les conséquences d'une violation

La violation du secret professionnel est une **infraction pénale** (code pénal), indépendamment de toute sanction disciplinaire ou de tout licenciement. Une consultation de dossier sans motif légitime engage la responsabilité de la personne — le journal des accès permet de l'établir.

À retenir

- Le secret couvre **tout**, y compris le fait même d'être suivi au cabinet.
- Il s'impose à **toute l'équipe**, sans limite de temps.
- **Échange** (ciblé) et **partage** (équipe de soins) supposent : **nécessité**, **pertinence**, **information du patient**.
- Hors équipe de soins : **consentement**.
- La confidentialité vaut **à l'oral** autant qu'à l'écrit.

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 1er 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** .

Les droits du patient sur ses données

> **Référentiel BTS — BC4 / C4.7**. Contribue à **BC1 / C1.4** « Informer la personne prise en soins et son entourage ».

> **L'essentiel :** le patient a le droit de **savoir**, de **voir**, de **faire corriger** et, dans certains cas, de **s'opposer**. Le cabinet doit répondre **dans un délai d'un mois**, et savoir **vérifier l'identité** du demandeur avant de transmettre quoi que ce soit.

Objectif

À la fin de cette page, vous savez :

- énoncer les droits d'une personne sur ses données ;
- traiter une demande d'accès au dossier, de bout en bout ;
- rédiger et placer la **mention d'information** du cabinet.

1. Le droit d'être informé

C'est le droit premier : il conditionne tous les autres. Le patient doit savoir, **au moment de la collecte**, ce qu'on fait de ses données.

La **mention d'information** du cabinet indique, en termes compréhensibles :

- **qui** est responsable de traitement (raison sociale, coordonnées) ;
- **pourquoi** les données sont recueillies (prise en soins, facturation, télétransmission) ;
- **quelles** catégories de données, et leur caractère obligatoire ou facultatif ;
- **qui** y a accès (l'équipe, l'Assurance Maladie, la mutuelle en tiers payant, l'hébergeur) ;
- **combien de temps** elles sont conservées ;

- **quels droits** la personne a, et **comment les exercer** ;
- l'existence éventuelle d'un **DPO**, et le droit de **réclamation auprès de la CNIL**.

Où la placer : **affichée en salle d'attente**, **remise ou signalée à l'ouverture du dossier**, et disponible sur le site du cabinet s'il existe. Une phrase orale ne suffit pas.

2. Le droit d'accès — et l'accès au dossier

Toute personne peut demander **communication des informations la concernant**. Deux fondements se croisent : le droit d'accès du RGPD, et le droit d'accès au **dossier médical** du code de la santé publique.

La procédure, pas à pas :

1. **Enregistrer la demande** et sa date — le délai court à partir de là.
2. **Vérifier l'identité** du demandeur. C'est une étape de sécurité, pas un obstacle : transmettre un dossier à un imposteur est une violation de données. Une copie de pièce d'identité est légitime.
3. **Vérifier la qualité** : le patient lui-même ? le titulaire de l'autorité parentale ? un majeur protégé et son représentant ? un ayant droit après décès (motif limité à justifier) ? un mandataire (mandat écrit) ?
4. **Constituer le dossier** : identité et administratif, anamnèse, dossier technique, descriptif de l'appareil, comptes rendus. Les **notes personnelles de travail**, non formalisées et non partagées, n'ont pas à être communiquées.
5. **Répondre sous un mois** (prolongeable en cas de demande complexe, en informant la personne). Le code de la santé publique prévoit par ailleurs un **délai de réflexion de 48 heures** avant communication du dossier médical, et des délais propres selon l'ancienneté des informations.
6. **Remettre** : consultation sur place gratuite, ou copie. Les **frais de copie** peuvent être facturés au coût réel, sans excéder le coût de reproduction et d'envoi.
7. **Tracer** la demande et la réponse.

> ⚠ Cas fréquent en cabinet : le conjoint, l'enfant ou l'employeur qui demande « le dossier ». La réponse par défaut est **non** : c'est au patient de demander, et à lui de transmettre ensuite ce qu'il veut.

3. Le droit de rectification

Le patient peut faire **corriger une donnée inexacte** : orthographe du nom, date de naissance, adresse, mutuelle.

Attention à la limite : on rectifie une **donnée factuelle erronée**. On ne supprime pas rétroactivement une **observation professionnelle** parce qu'elle déplaît. Si le patient conteste une appréciation, on **consigne sa contestation** au dossier — on ne réécrit pas l'histoire.

4. Le droit d'opposition et la limitation

- **Opposition** : possible pour les traitements fondés sur l'intérêt légitime ou le consentement — newsletter, enquête, photos en communication. **Pas** pour le dossier de soins ni la facturation, qui reposent sur des obligations légales.
- **Opposition au partage** : le patient peut refuser que ses informations soient partagées avec un professionnel donné, ou masquer un document dans son DMP.
- **Limitation** : geler temporairement un traitement, le temps d'examiner une contestation.

5. L'effacement — et pourquoi il est le plus souvent refusé

Le « droit à l'oubli » **ne s'applique pas** aux données que le cabinet doit conserver au titre d'une obligation légale : dossier de prise en soins, pièces comptables et de facturation.

La bonne réponse à un patient qui demande la suppression de son dossier n'est donc pas « non » tout court, mais : *« Je ne peux pas supprimer votre dossier de soins, la loi m'impose de le conserver ; en revanche je peux retirer vos coordonnées de nos envois, supprimer vos photos utilisées en communication, et restreindre les accès. »*

6. La portabilité

Droit de récupérer ses données dans un format lisible par machine, et de les faire transmettre à un autre responsable. Il s'applique aux données fournies par la personne, sur la base du consentement ou d'un contrat — donc **d'une portée limitée** pour un dossier de soins. En pratique, le transfert vers un confrère passe par la communication du dossier, à la demande du patient.

Répondre : les réflexes

Réflexe	Pourquoi
Dater et enregistrer la demande	Le délai d'un mois est opposable
Vérifier l'identité et la qualité	Éviter de créer soi-même une violation de données
Ne pas demander plus que nécessaire pour vérifier	Une pièce d'identité suffit ; pas de justificatif du motif
Répondre par écrit, même pour refuser	Un refus se motive et mentionne le recours CNIL
Transmettre par un canal sûr	MSSanté, remise en main propre, courrier recommandé — pas un mail ordinaire
Ne rien facturer au-delà du coût réel de reproduction	Le droit d'accès est gratuit

À retenir

- Six droits : **information, accès, rectification, opposition, limitation, portabilité** — et un droit d'effacement **largement neutralisé** par les obligations de conservation.
- **Un mois** pour répondre ; demande **datée et tracée**.
- **Vérifier l'identité et la qualité** avant toute transmission.
- Le patient demande **lui-même** : ni le conjoint, ni l'employeur, ni l'assurance à sa place.
- On rectifie un **fait**, pas une **observation professionnelle** : la contestation se consigne.

Registre, DPO et violations de données

> **Référentiel BTS — BC4 / C4.7**. Voir aussi **BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** trois obligations concrètes pèsent sur la structure — **tenir un registre** de ses traitements, **désigner un DPO** lorsque c'est requis, et **documenter puis notifier** les violations de données.

Objectif

À la fin de cette page, vous savez :

- dire ce que contient un registre des traitements et comment le construire ;
- savoir quand un **DPO** est obligatoire et ce qu'il fait ;
- qualifier une **violation de données** et déclencher la bonne réaction.

1. Le registre des traitements

C'est la pièce maîtresse de la « responsabilité » : le document qui permet de **prouver** qu'on sait ce qu'on fait des données. Il est demandé en premier en cas de contrôle de la CNIL.

Une ligne par traitement. Pour un cabinet d'orthoprothèse, la liste tient en une dizaine de lignes :

Traitement	Finalité	Personnes	Données	Destinataires	Durée
Dossier patient	Prise en soins, suivi de l'appareillage	Patients	Identité, INS, santé, mesures, modèles 3D, photos	Équipe, prescripteur	Voir politique d'archivage

Traitement	Finalité	Personnes	Données	Destinataires	Durée
Facturation / télétransmission	Facturer, être remboursé	Patients	Identité, NIR, droits, codes LPP	AMO, AMC, SCOR	Durée légale comptable
Rendez-vous	Organiser l'activité	Patients	Identité, coordonnées	Équipe	Durée du suivi
Gestion du personnel	Paie, contrats, planning	Salariés	Identité, contrat, paie	Comptable, URSSAF	Durées légales sociales
Fournisseurs / achats	Commandes, comptabilité	Contacts pro	Coordonnées professionnelles	Comptable	10 ans (pièces)
Recrutement	Sélectionner	Candidats	CV, lettre	Dirigeant	Quelques mois
Vidéosurveillance (si présente)	Sécurité des locaux	Patients, salariés, visiteurs	Images	Dirigeant, forces de l'ordre sur réquisition	Quelques semaines

À chaque ligne, on ajoute utilement : la **base légale**, les **mesures de sécurité**, et les éventuels **transferts hors Union européenne**.

Le registre **vit** : on le met à jour à chaque nouveau logiciel, nouveau prestataire, nouvel usage. Un registre écrit une fois en 2019 et jamais rouvert ne prouve rien.

2. Le délégué à la protection des données (DPO)

Obligatoire notamment lorsque l'activité principale conduit à un **traitement à grande échelle de données sensibles**. Pour un cabinet d'orthoprothèse de quelques personnes, la désignation n'est en général **pas obligatoire** — mais elle est **recommandée**, et une structure plus importante, un réseau ou un groupe d'établissements relèvera souvent de l'obligation.

Le DPO peut être **interne** ou **externe** (mutualisé entre plusieurs structures, ce qui est fréquent et économique). Il **informe et conseille**, **contrôle** le respect des règles, **coopère avec la CNIL** et sert de **point de contact** pour les personnes.

Il n'est **pas** le responsable de traitement : la responsabilité reste au dirigeant. Et il doit disposer des moyens et de l'indépendance nécessaires — on ne nomme pas DPO la personne qui décide des traitements.

Quand il n'y a pas de DPO, il faut malgré tout **désigner un référent** identifié dans l'équipe. Sinon, personne ne tient le registre et personne ne répond aux demandes.

3. L'analyse d'impact (AIPD)

Une **analyse d'impact relative à la protection des données** est requise lorsqu'un traitement est susceptible d'engendrer un **risque élevé** pour les personnes — ce qui vise notamment les traitements **à grande échelle** de données de santé.

Un cabinet de taille modeste n'y est généralement pas tenu pour son dossier patient courant, mais la question se pose sérieusement en cas de **nouveau dispositif** : plateforme de télésuivi, base de modèles 3D mutualisée, outil d'analyse de marche connecté, recherche. En cas de doute : la CNIL publie des listes de traitements nécessitant ou non une AIPD.

4. Les violations de données

Définition : une violation, c'est toute atteinte à la **confidentialité** (accès ou divulgation non autorisés), à l'**intégrité** (altération) ou à la **disponibilité** (perte, destruction) de données personnelles — **accidentelle ou illicite**.

Le mot important est **accidentelle** : il n'y a pas besoin d'un pirate.

Événement	Violation ?	Type
Compte rendu envoyé au mauvais patient	Oui	Confidentialité
Ordinateur portable non chiffré volé	Oui	Confidentialité
Rançongiciel chiffrant les dossiers	Oui	Disponibilité (+ confidentialité si exfiltration)
Classeur de dossiers papier perdu	Oui	Confidentialité
Serveur en panne, données intactes, restaurées en 2 h	Non (incident technique)	—
Salarié consultant un dossier sans motif	Oui	Confidentialité
Suppression accidentelle sans sauvegarde	Oui	Disponibilité

Ce qu'il faut faire

1. **Documenter toutes les violations** dans un **registre des violations** — y compris celles qu'on ne notifie pas. Ce registre doit pouvoir être présenté à la CNIL.
2. **Évaluer le risque** pour les personnes : nature des données (santé = risque élevé par défaut), nombre de personnes, facilité d'identification, conséquences possibles.

3. **Notifier la CNIL sous 72 h** dès lors que le risque n'est pas négligeable. En cas de retard, motiver. Une notification peut être complétée ensuite.
4. **Informer les personnes concernées sans délai** si le risque est **élevé** : leur dire ce qui s'est passé, quelles données, quelles conséquences possibles, ce qu'elles peuvent faire, et qui contacter.
5. **Prendre les mesures correctives**, et les consigner.

Le registre des violations note pour chaque événement : date de survenue et de découverte, nature, données et personnes touchées, conséquences, mesures prises, décision de notifier ou non **et sa justification**.

À retenir

- **Registre des traitements** : une ligne par traitement, mis à jour, présentable à tout moment.
- **DPO** : souvent non obligatoire en petit cabinet, toujours utile ; à défaut, un **référent désigné**.
- **AIPD** : pour les traitements à risque élevé — à examiner avant tout nouveau dispositif.
- **Violation** = confidentialité, intégrité **ou** disponibilité, y compris par accident.
- **Toutes** les violations se documentent ; celles à risque se notifient à la **CNIL sous 72 h** ; celles à risque **élevé** s'annoncent **aux patients**.

L'hébergement des données de santé (HDS)

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

> **L'essentiel :** dès qu'un **tiers** héberge des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins, il doit être **certifié HDS**. Ce n'est pas une option commerciale : c'est une obligation légale, et c'est au cabinet de la vérifier.

Objectif

À la fin de cette page, vous savez :

- dire quand la certification HDS est requise ;
- vérifier qu'un prestataire l'est réellement ;
- lister ce qu'un contrat d'hébergement doit prévoir.

Le principe

Le code de la santé publique impose que l'hébergement de données de santé à caractère personnel, **pour le compte d'un tiers**, soit assuré par un hébergeur **certifié HDS** (Hébergeur de Données de Santé). La certification est délivrée par un organisme accrédité, après audit, et porte sur des activités précises (mise à disposition d'infrastructure, d'infogérance, de sauvegarde, d'administration…).

Quand c'est requis :

- le **logiciel métier est en ligne** (mode SaaS) et les dossiers sont chez l'éditeur ou son hébergeur ;

- les **sauvegardes** partent chez un prestataire externe ;
- les **modèles 3D**, photos cliniques ou fichiers de CAO sont stockés sur un service tiers ;
- une **plateforme de télésoin** ou de suivi conserve des données patients ;
- l'**infogérance** du serveur du cabinet est confiée à un prestataire qui y accède.

Quand ce n'est pas requis : le cabinet qui héberge **ses propres** données sur **son propre** serveur, dans ses locaux, n'a pas à être certifié pour lui-même. Il reste évidemment tenu à la sécurité et à toutes les autres obligations.

Vérifier, ne pas croire sur parole

« Nos serveurs sont en France » n'est pas « nous sommes certifiés HDS ». Deux vérifications simples :

1. **Demander le certificat HDS** — un document nominatif, avec un périmètre, une date de validité et l'organisme certificateur. Vérifier que le **périmètre couvre bien** la prestation qui vous concerne.
2. **Consulter la liste publique des hébergeurs certifiés** publiée par l'Agence du Numérique en Santé.

Attention aux chaînes de sous-traitance : l'éditeur de votre logiciel peut ne pas être hébergeur lui-même et s'appuyer sur un prestataire. C'est alors **ce prestataire** qui doit être certifié, et le contrat doit le nommer.

Ce que le contrat doit prévoir

Le contrat avec l'hébergeur (ou l'éditeur) est un **contrat de sous-traitance** au sens du RGPD. Il doit préciser au minimum :

Point	Ce qu'on vérifie
Objet et durée	Quelles données, pour quel service, combien de temps
Certification HDS	Référence du certificat et périmètre couvert
Localisation	Où sont physiquement les données ; **transferts hors UE** encadrés ou absents
Sous-traitants ultérieurs	Liste, et obligation d'information avant tout changement
Sécurité	Chiffrement, contrôle des accès, journalisation
Sauvegardes	Fréquence, rétention, **délai de restauration garanti**
Confidentialité	Engagement du personnel de l'hébergeur ; pas d'accès hors nécessité technique

Point	Ce qu'on vérifie
Incidents	Obligation d'informer le cabinet **sans délai** en cas de violation
Audit	Droit pour le cabinet de demander des éléments de preuve
Réversibilité	**Format**, **délai** et **coût** de restitution des données en fin de contrat ; suppression certifiée ensuite
Fin d'activité de l'éditeur	Ce qu'il advient des données si le prestataire disparaît

> **La réversibilité est le point le plus souvent négligé et le plus coûteux.** Un cabinet qui ne peut pas récupérer ses dossiers dans un format exploitable est captif — et en difficulté le jour où il doit changer de logiciel, ou si l'éditeur cesse son activité.

Et le cloud grand public ?

Non. Un service de stockage grand public n'est pas certifié HDS, ses conditions générales ne constituent pas un contrat de sous-traitance conforme, et la localisation des données y est rarement maîtrisée.

Le raccourci « je mets juste les scans 3D sur mon espace personnel » est une **double faute** : hébergement non conforme **et** usage de matériel ou de compte personnel (voir *Formation métier — Sécurité numérique*).

Responsabilité : qui répond de quoi

- Le **cabinet** reste **responsable de traitement**. C'est lui qui décide, lui qui informe les patients, lui qui répond à la CNIL.
- L'**hébergeur** et l'**éditeur** sont **sous-traitants** : ils ne traitent que sur instruction, et engagent leur propre responsabilité s'ils sortent de ce cadre ou manquent à la sécurité.

Externaliser ne transfère pas la responsabilité. Cela la **partage**, à condition que le contrat soit écrit.

À retenir

- Hébergement de données de santé **par un tiers** ⇒ **certification HDS obligatoire**.

- On **demande le certificat** et on vérifie son **périmètre** — « serveurs en France » ne suffit pas.
- Le contrat couvre : localisation, sécurité, sauvegardes, incidents, audit, **réversibilité**.
- **Jamais** de données de santé sur un cloud grand public.
- Le cabinet reste **responsable de traitement**, quoi qu'il externalise.

Traçabilité et habilitations dans le logiciel

> **Référentiel BTS — BC4 / C4.7**. Page de mise en pratique, avec renvois vers les écrans de WinOrtho.

> **L'essentiel :** deux mécanismes traduisent la réglementation dans le logiciel — les **habilitations** (qui a le droit de voir quoi) et la **journalisation** (qui a effectivement fait quoi, et quand). Sans eux, aucune des obligations précédentes n'est démontrable.

Objectif

À la fin de cette page, vous savez :

- définir un profil d'habilitation à partir d'un rôle ;
- lire un journal d'activité et en tirer une conclusion ;
- situer ces éléments dans WinOrtho.

1. Les habilitations

Une habilitation répond à la question : *de quoi cette personne a-t-elle besoin pour faire son travail ?* — et à rien d'autre. C'est le **principe du moindre privilège**, transposé au logiciel métier.

Méthode en quatre étapes :

1. **Lister les rôles** réels de la structure, pas les personnes : orthoprothésiste, technicien, secrétariat, gestion, direction, apprenti.
2. **Pour chaque rôle, lister les opérations nécessaires** : consulter / créer / modifier / supprimer / exporter, par domaine (patients, PEC, facturation, stock, atelier, paramétrage).

3. **Créer un profil par rôle**, et y rattacher les personnes — jamais l'inverse.
4. **Revoir la liste au moins une fois par an**, et à chaque arrivée, changement de poste ou départ.

Les points de vigilance :

- Le droit d'**exporter** ou d'imprimer en masse mérite plus d'attention que le droit de consulter : c'est par là que partent les fuites volumineuses.
- Le droit de **supprimer** doit être rare et tracé.
- Les **comptes d'administration** ne servent qu'à administrer.
- Un **apprenti ou stagiaire** a un compte nominatif, restreint, et **désactivé à la fin du stage**.
- Un **compte générique** partagé annule toute traçabilité : c'est le défaut le plus grave.

2. La journalisation

Le journal enregistre **qui**, **quand**, **quoi**. C'est la contrepartie du droit d'accès aux données : parce que les professionnels peuvent consulter les dossiers, il faut pouvoir vérifier que ces consultations étaient légitimes.

Un journal sert à trois choses :

- **répondre au patient** qui demande qui a consulté son dossier ;
- **établir les faits** après un incident (violation, suspicion de consultation indue) ;
- **dissuader** — savoir que tout est tracé change les comportements.

Encore faut-il qu'il soit **exploité** : un journal que personne ne regarde jamais ne dissuade personne. Une revue périodique, même sommaire — quelques sondages par trimestre, et systématiquement après un événement — suffit à le rendre réel.

> ⚠ Le journal contient lui-même des données personnelles (celles des salariés). Il a donc une **durée de conservation** définie, un **accès restreint**, et il ne peut pas être détourné en outil de surveillance permanente de l'activité des employés : son usage doit être annoncé à l'équipe, et proportionné.

3. Dans WinOrtho

Notion	Où la voir	Support détaillé

Comptes et profils utilisateurs	Écran **Préférences**	*Formation logiciel — Système* → **Préférences**
Journal d'activité (qui a fait quoi, quand)	Écran **Journal d'activité**	*Formation logiciel — Direction* → **Journal d'activité**
Exports de données	Écran **Exports**	*Formation logiciel — Direction* → **Exports**
Documents du dossier patient	Onglet Documents de la prise en charge	*Formation logiciel — Général* → **Prises en charge**
Données de droits et de mutuelle	Fiche patient	*Formation logiciel — Général* → **Patients**

À retenir

- **Habilitations** = le droit d'accéder ; **journal** = la preuve de ce qui a été fait.
- On crée des **profils par rôle**, et on y rattache les personnes.
- **Export** et **suppression** sont les droits les plus sensibles.
- Un **compte partagé détruit la traçabilité** — et donc la conformité.
- Le journal doit être **relu** pour servir à quelque chose, et reste lui-même encadré.