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.

Revision #4
Created 2026-09-15 17:24:34 UTC by Antoine
Updated 2026-09-16 07:03:22 UTC by Antoine