

Veille : L'Évolution de la Protection des Données de Santé face à l'IA Médicale (2025-2026)

Sommaire

1. **Les Nouvelles Règles (2025)** : Ce que la loi oblige les hôpitaux et les IA à faire.
 2. **Où sont stockées vos données ?** : L'importance de garder les données en Europe (Souveraineté).
 3. **Les Nouvelles Menaces** : Comment les pirates utilisent l'IA pour attaquer.
 4. **Les Solutions Techniques** : Comment les techniciens protègent le système.
 5. **Calendrier** : Les dates clés pour être en règle
-

1. Les "Gendarmes" et les Lois (Le Cadre)

En 2025, trois grandes autorités renforcent les contrôles :

- **La HAS (Haute Autorité de Santé)** : C'est l'organisme qui donne des "notes de qualité" aux hôpitaux. En 2025, si un hôpital utilise une IA pour aider un médecin à diagnostiquer une maladie, il doit prouver que l'IA ne se trompe pas et qu'elle ne rejette pas certains patients (ce qu'on appelle les **biais**).
- **L'AI Act (Loi Européenne sur l'IA)** : C'est le "code de la route" de l'intelligence artificielle en Europe. Il interdit les IA dangereuses (qui manipulent les gens) et oblige les IA médicales à être très surveillées.
- **La CNIL** : Le gendarme de la vie privée. Elle autorise l'utilisation de vos données pour entraîner des IA, mais seulement si c'est très sécurisé et que vous êtes informés.

2. Le "Coffre-Fort" des données (HDS et Souveraineté)

Pour stocker des dossiers médicaux, on ne peut pas utiliser n'importe quel serveur. Il faut une autorisation spéciale : la **certification HDS** (Hébergeur de Données de Santé).

- **HDS version 2.0** : C'est la nouvelle règle de 2025. Elle oblige désormais à ce que les données de santé des Français soient **stockées physiquement en Europe**.
- **Pourquoi ?** Pour éviter que des lois étrangères (comme le *Cloud Act* américain) ne permettent à des gouvernements hors-Europe de regarder nos dossiers médicaux. C'est ce qu'on appelle la **Souveraineté**.

- **Les géants (Google, Microsoft) :** Ils ont dû modifier leurs installations pour obtenir ce "diplôme" HDS v2.0 et prouver qu'ils respectent nos règles.

3. La guerre entre IA : Pirates contre Défenseurs

En 2025-2026, la cybercriminalité change de visage :

- **Vols de données :** Les pirates ne se contentent plus de bloquer les ordinateurs des hôpitaux (Ransomware), ils volent les dossiers pour faire chanter les patients.
- **L'IA malveillante :** Les pirates utilisent des IA pour créer des emails de piège (Phishing) parfaits ou imiter la voix d'un directeur d'hôpital pour demander des virements (Deepfakes).
- **La menace "Quantique" :** On s'inquiète des futurs ordinateurs super-puissants capables de casser tous les mots de passe actuels. On commence déjà à créer de nouveaux codes (Cryptographie Post-Quantique).

4. Les solutions des techniciens (SISSR)

Pour protéger tout ça, les spécialistes utilisent des méthodes précises :

- **MFA (Authentification Multi-Facteurs) :** C'est quand on vous demande un code sur votre téléphone en plus de votre mot de passe. C'est obligatoire pour tous les soignants.
- **Zéro Trust (Confiance Zéro) :** Un principe simple : on ne fait confiance à personne par défaut. Même si vous êtes déjà connecté au réseau de l'hôpital, on vérifie votre identité

à chaque étape.

- **Apprentissage Fédéré** : Une technique géniale pour l'IA. Au lieu d'envoyer toutes les données des patients vers un gros serveur central (dangereux en cas de vol), l'IA "apprend" directement dans chaque hôpital et ne partage que son savoir, pas les noms des patients.

5. Dates clés à retenir

Février 2025 : Début des règles européennes sur l'IA.

Août 2025 : Surveillance renforcée des IA qui font des diagnostics.

16 Mai 2026 : Date limite. Tous les hébergeurs de données de santé doivent avoir le nouveau diplôme (HDS v2.0) sous peine d'être illégaux.

Petit Lexique pour comprendre les sigles :

ANS : Agence du Numérique en Santé (ceux qui pilotent l'informatique médicale en France).

HDS : Le "label" obligatoire pour stocker des données de santé.

IA Générative : Une IA capable de créer du texte ou des images (comme ChatGPT).

RGPD : La loi qui protège vos données personnelles (nom, adresse, santé).

GPU : Des composants informatiques très puissants nécessaires pour faire tourner l'IA.