

Cybersécurité en santé

Notre mission commune

Protéger ensemble l'intégrité et la confidentialité des données patients

HÔPITAUX Paris

Saint-Joseph

Marie-Lannelongue



Le paysage des menaces cyber dans la santé

Le secteur de la santé est devenu l'une des **cibles privilégiées** des cybercriminels. Les établissements hospitaliers subissent des attaques quotidiennes, avec des conséquences parfois dramatiques pour la **continuité des soins**.

300%

Hausse des cyberattaques

Augmentation des incidents en 5 ans dans les hôpitaux français

21

Jours d'indisponibilité

Durée moyenne de paralysie après un ransomware réussi

1/3

Établissements touchés

Des hôpitaux européens ont subi une cyberattaque majeure

Depuis le début de l'année, 243 incidents de sécurité dans des établissements de santé.

AUX Paris

Joseph

-Lannelongue



Les données de santé : un trésor convoité

Pourquoi nos données sont si précieuses ?

Les **dossiers médicaux** contiennent des informations complètes et permanentes : identité, pathologies, traitements, coordonnées bancaires. Sur le marché noir, un dossier médical vaut 10 à 50 fois plus qu'une carte bancaire.

- Usurpation d'identité
- Fraude à l'assurance maladie
- Chantage et extorsion

Les conséquences d'une fuite

Une violation de données peut avoir des **impacts dévastateurs** et durables pour les patients comme pour l'établissement.

- Atteinte à la vie privée des patients
- Perte de confiance envers l'hôpital

Tarification moyenne :

- Carte de crédit unitaire : 3-8 €
- Dossier patient : 50-100 €



Réglementations et obligations légales

Le cadre juridique protégeant les données de santé est particulièrement strict en France et en Europe. Notre responsabilité collective est engagée à chaque manipulation de données concernant les patients.

RGPD

Règlement Général sur la Protection des Données

- Renforcement du droit des personnes
- Impose des obligations aux entités qui traitent des données personnelles
- CNIL : Sanctions jusqu'à 4% du CA mondial ou 20M€
- Notification d'une fuite de données sous 72h

NIS 2

Network and Information Security Directive 2

- Renforcement des obligations de sécurité
- Obligations cyber opérationnelles
- Sanctions jusqu'à 2% du CA Mondial ou 10 M€
- Obligation de signalement des incidents de sécurité

Secret médical

Article 226-13 du Code pénal

- Obligation générale et absolue
- Sanction pénale : 1 an de prison et 15 000€ d'amende
- Sanction civile : dommages - intérêts
- Responsabilité personnelle

Règles d'accès au dossier médical

- Règles d'accès au dossier d'un patient

- > Le secret médical

- ~ Couvre toutes les informations que le professionnel de santé a sur vous : état de santé (diagnostic, traitement...), identité, ce que le patient a confié, ce que le professionnel a vu, entendu, compris...

- > Le RGPD

- ~ Données de santé : catégories particulières Article 9

- ~ Traitement encadré

- ~ Obligation du Responsable de traitement : Analyse d'impact, information sur les finalités des traitements, limitation de la collecte, respect de la durée de conservation, niveau de sécurité hébergement, sécuriser les échanges (messagerie sécurisée), recherche MR.

- > Le code de la santé publique

- ~ Secret des informations, Art. L1110-4

Dossier patient
Pas d'accès

Patient hors prise en charge

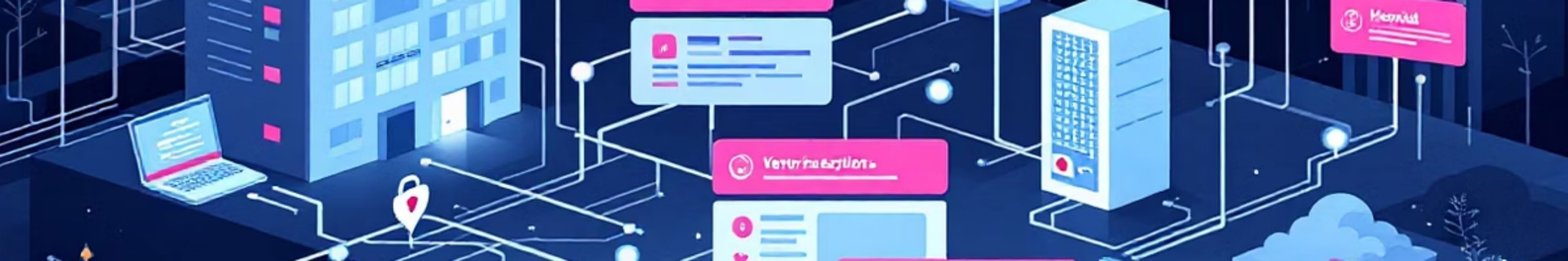
Collègue

Personne de son entourage familial

Faute

et violation du secret professionnel





Les principales vulnérabilités dans notre environnement

Facteur humain

90% des incidents de sécurité impliquent une erreur humaine. Phishing, mots de passe faibles, partage de comptes, ou négligence dans la manipulation des données.

Systemes obsolètes

De nombreux équipements médicaux utilisent des **exploitation non mis à jour**, créant des failles exploitables.

Connexions non sécurisées

Wi-Fi publics, accès distants mal configurés, et appareils personnels connectés au réseau hospitalier multiplient les **d'entrées potentiels**.

Supports amovibles

Clés USB, disques externes et smartphones peuvent servir de supports de malwares ou servir à exfiltrer des données hors de l'établissement.



Attaques par ransomware : cas réels et impacts

Les ransomwares sont devenus la menace n°1 pour les établissements de santé. Ces logiciels malveillants chiffrent l'ensemble des données et systèmes, paralysant totalement l'activité hospitalière.

CH d'Armentières (2024)

Coût 3 M€ suite à la cyberattaque. Fuite des coordonnées bancaires de 230 000 patients. 95% des postes de travail touchés, en plus des serveurs. Fermeture des urgences.

1

Hôpital privé de la Loire - St Etienne (2025)

Cyberattaque majeure. Un hacker a volé 530 000 dossiers de patients & 45 000 pièces d'identité.

2

3

4

CH Cannes (2024)

Chiffrement des données demande de rançon en échange de la clé de déchiffrement. Les services paralysés. Les services paralysés.

Plan de crise déclenché

CH Pontarlier (2025)

Ransomware de type Cryptolocker. Chiffrement d'une partie des données.

L'hôpital a coupé son réseau

Impact critique : Les cyberattaques sur les hôpitaux peuvent mettre des vies en danger.

Interventions reportées, urgences redirigées, accès aux dossiers impossible.



Bonnes pratiques au quotidien

Vos gestes de protection essentiels

La sécurité numérique repose sur des réflexes simple adopter systématiquement dans votre pratique quotidien

Mots de passe robustes : 12 caractères minimum (chiffres, maj, min)

Vigilance emails : sécurité.informatique@ghpsj.fr

Verrouillage/déconnexion systématique de votre session

Supports externes : professionnels

Ne partagez pas vos codes applicatifs : votre signature

IA : ChatGPT non autorisé sur le réseau → Copilot suite Mic

Vers l'extérieur : messagerie Bluefiles, demande au 11 ou



Signalement d'incidents : réagir rapidement

Chaque minute compte lors d'un incident de sécurité. Un signalement rapide permet de limiter les dégâts et de protéger les données des patients. Ne jamais hésiter à alerter, même pour un simple doute.

01 Identifier le problème

Email suspect, comportement anormal du système, accès non autorisé, perte de matériel, ou toute anomalie inhabituelle

03 Alerter immédiatement


Contactez le service informatique ou le RSSI sans délai. Documentez ce que vous avez observé avec précision

02 Ne pas agir seul

Ne tentez pas de résoudre le problème vous-même. N'ouvrez pas de pièces jointes suspectes. Déconnectez l'appareil du réseau mais ne pas l'éteindre

04 Suivre les instructions

Coopérez pleinement avec l'équipe de sécurité. Fournissez tous les détails demandés. Préservez les preuves

 **Principe fondamental** : Il vaut mieux signaler à tort qu'ignorer une vraie menace. Aucune alerte légitime ne sera jugée négativement.

securite.informatique@ghpsj.fr
service informatique -> 11 (HPSJ), 3300 (HML)
Hors HNO -> Administrateur de garde /

Votre rôle d'interne : garant de la sécurité numérique

En tant qu'interne, vous êtes en première ligne de la protection des données patients.

Votre vigilance quotidienne et votre exemplarité sont essentielles pour maintenir la confiance dans notre système de santé.



Responsabilité individuelle

Chaque professionnel est personnellement responsable des données qu'il consulte et manipule. Le secret médical s'étend au numérique.



Culture collective

Partagez les bonnes pratiques avec vos collègues. La sécurité est l'affaire de tous, pas seulement de l'informatique.



Formation continue

Restez informés des nouvelles menaces et techniques. Participez aux sessions de sensibilisation proposées par l'établissement. Consultez

« La cybersécurité n'est pas une contrainte technique, c'est une extension du serment d'Hippocrate à l'ère numérique : d'abord, ne pas nuire aux données de nos patients. »

l'actu RGPD du DPO [Ensemble GHPSJ](#)



OBLIGATOIRE → e-learning

- « MOOC RGPD et secteur santé 2024 »
~ 4 niveaux / QUIZ Final → 30 minutes de formation
- [Tableau de bord | GHPSJ Formations \(mooct.fr\)](https://mooct.fr)

Mes Cours



MOOC RGPD & secteur santé 2025

Démarré - 1 janv. 2025



Reprendre le cours

