gbna santé

# Sensibilisation à la sécurité du Système d'Information

**Réunion Cadres** le **14/10/2025**

**Florian RIGAUD** et **Alexis TIGOULET**

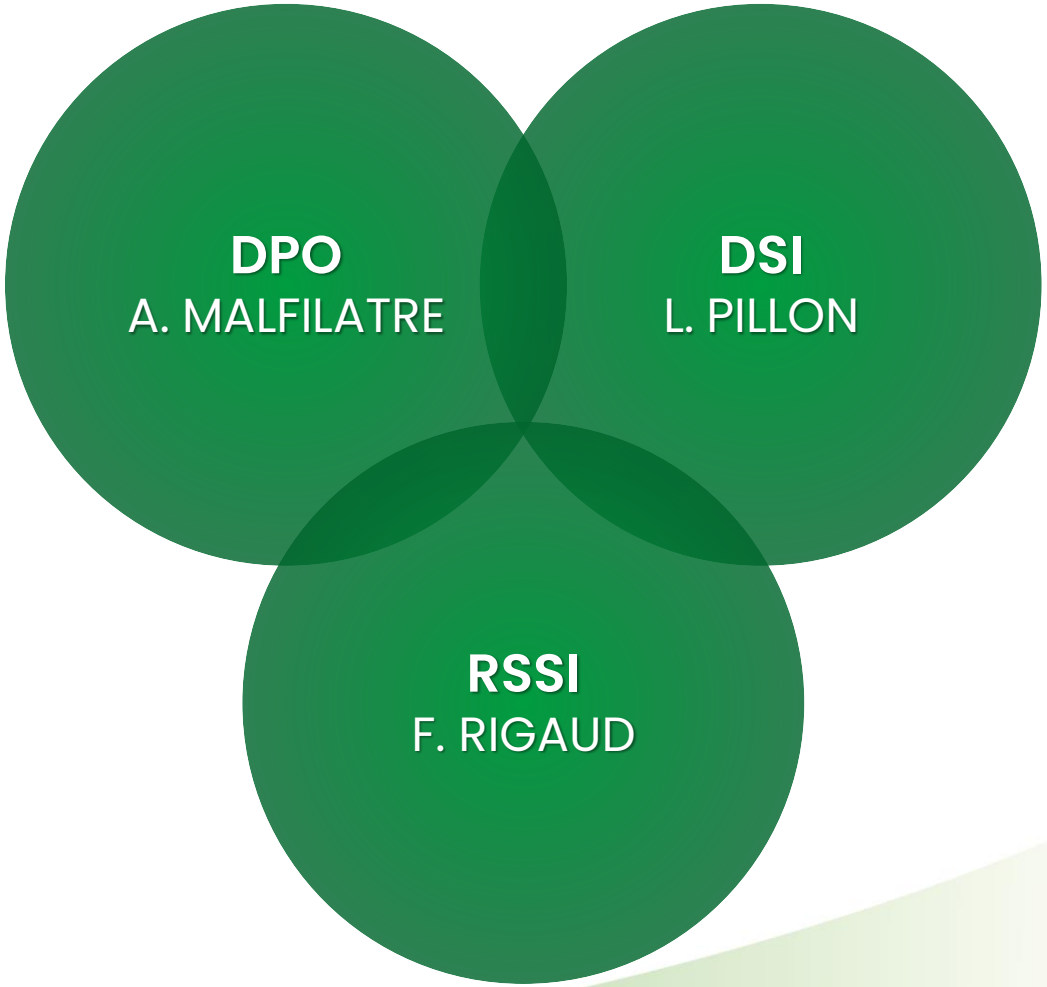
Prendre soin de la vie et de la santé de la population

# Sommaire

- La sécurité du système d'information hospitalier
- Des cybermenaces en constante évolution
- Adopter les bons réflexes
- Questions ?

# Vos interlocuteurs cybersécurité

› **DSI** : Directeur du Système d'Information
› **DPO** : Délégué à la protection des données
› **RSSI** : Responsable de la Sécurité du Système d'Information



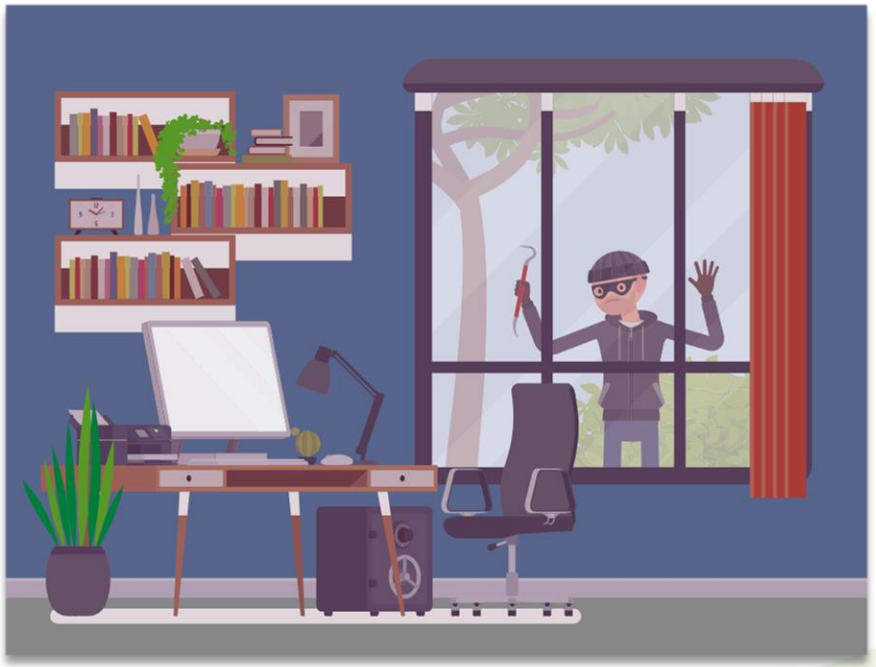
# La sécurité du Système d'Information Hospitalier (SIH)

Pour notre vie privée, ou nos activités professionnelles, nous avons tous recours à l'outil informatique et à Internet au quotidien.

## Les risques informatiques sont présents partout.

### À la maison…

- Je ne laisse pas les clés sur la porte du domicile.
- Je ne laisse pas les fenêtres ouvertes alors que je suis absent du domicile.
- Je ne laisse pas en évidence des objets de valeur en présence d'étrangers.
- Je ne laisse pas entrer n'importe qui chez moi.



**Au travail comme à son domicile la sécurité c'est une question de bon sens !**

# La sécurité du Système d'Information Hospitalier (SIH)

## Pourquoi protéger le SIH de GBNA ?


Parce que **les missions de l'établissement ne doivent pas être compromises** par une atteinte au Système d'Information (**Ouverture H24 7/7 jours**)

Car les informations de notre Système d'Information sont **sensibles et confidentielles avec une valeur marchande forte**


Enfin **pour éviter des conséquences graves sur les patients ou nos collaborateurs** en raison de la perte d'intégrité des informations

# Qu'est-ce qu'une cybermenace ?

## Des menaces omniprésentes


### Les erreurs

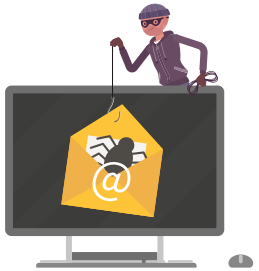
- Erreur de manipulation
- Erreur de saisie
- Erreur de configuration


### Les accidents

- Accident environnemental
- Rupture de service
- Coupure réseau
- Panne d'équipements
- Saturation de ressources
- Perte accidentelle de données


### Les actes non malveillants

- Utilisation de logiciels sans licence
- Mauvais usages



### Les malveillances

- Vandalisme, vol & sabotage
- Fuite d'information / divulgation
- Effacement volontaire de données
- Abus de droits
- Cybercriminalité
- Intrusion sur le SI

# Des cybermenaces en constante évolution

## Face aux cybermenaces, les collaborateurs sont le 1er rempart !

De nombreuses vulnérabilités peuvent être exploitées pour **nuire à la sécurité de nos systèmes et de nos métiers…**

Nos **mesures de protection techniques** (pare-feu, antivirus, limitation des droits, sauvegardes, double authentification etc.) vous offrent une protection.

**Cependant votre vigilance reste notre première défense.**

# Des cybermenaces en constante évolution

**Septembre 2025**

Communiqué de presse

## Une cyberattaque dirigée contre les données d'identité des patients des hôpitaux publics de la région

En fin de semaine dernière, le groupement régional d'appui au développement de la e-santé (GRADes) Hauts-de-France a constaté - en lien avec les autorités nationales et l'agence régionale de santé Hauts-de-France - qu'une cyberattaque avait été menée contre les serveurs sur lesquels sont hébergées des données d'identité de patients d'hôpitaux publics de la région. Plusieurs régions de France sont concernées à des degrés différents par cette attaque. Le ou les pirates ont pu s'introduire dans les serveurs partagés par les centres hospitaliers des Hauts-de-France en usurpant l'identité d'un professionnel de santé.

**Août 2025**

**Grande distribution**

## Auchan à nouveau victime d'une cyberattaque, des «centaines de milliers» de données personnelles piratées

Le joyau de l'empire Mulliez a subi un «acte de cyber malveillance sur une partie des données personnelles de ses clients associées aux comptes de fidélité», a annoncé jeudi l'enseigne. Les mots de passe et données bancaires ne sont toutefois pas concernés.

**Juillet 2025**

PIXELS • SÉCURITÉ INFORMATIQUE

## France Travail ciblé par un piratage, les données de 340 000 demandeurs d'emploi concernées

Parmi les éléments consultés par les pirates se trouvent les « noms et prénoms, dates de naissance, identifiants France Travail, adresses mail et postale et numéros de téléphone », précise l'organisme. Ce dernier avait déjà été visé par une cyberattaque en 2024.

# Adopter les bons réflexes


**Respecter les règles**

## Je respecte le règlement et la législation

Un acte malveillant ou une erreur peut avoir des impacts significatifs sur les collaborateurs, les patients et les activités de GBNA.

**Les règles mises en place sont là pour assurer la protection du SI de GBNA** tout en permettant aux collaborateurs de travailler dans de bonnes conditions.

**Pour l'échange de données de santé, j'utilise une messagerie sécurisée (MSSANTÉ)**

2

# J'agis en professionnel

**Seuls les professionnels de santé impliqués dans la prise en charge directe du patient** peuvent consulter les données de santé de ce patient.

**Les collaborateurs s'interdisent de consulter des informations** pour lesquelles ni leur rôle ni leur champ de compétence ne leur donnent de droits particuliers.

**Utiliser le SI à des fins professionnelles**

# Adopter les bons réflexes

3

**Rester vigilant en toute circonstance**

## Je suis prudent avec l'utilisation de ma messagerie

**Les mails sont susceptibles de contenir des menaces** (virus, ransomware, phishing) et ne garantissent pas l'identité du destinataire.

**Je vérifie systématiquement l'identité de l'expéditeur**, j'évite d'ouvrir les pièces jointes suspectes et n'hésite pas en cas de doute à transférer un mail suspect à :

support@gbna-sante.fr

## Je me méfie des supports amovibles inconnus

**L'utilisation de supports externes inconnus (clés USB, disques durs externes, etc.) est formellement interdite.**

Cela concerne particulièrement les supports trouvés dans les lieux publics. En outre, il faut également éviter l'utilisation de supports amovibles personnels.

# Adopter les bons réflexes

## Je protège mes mots de passe et ne les communique pas

Mes identifiants de connexion sont personnels, les confier à une autre personne met en péril les données et applications auxquelles j'ai accès (ex : vol, suppression, falsification de données, fraude)

**Je suis responsable de toutes les actions réalisées avec mon compte.**

Il est également **déconseillé** de noter mes identifiants sur des supports non sécurités (ex : post-it, fichier Excel, etc.)


## Protéger son identité et ses équipements numériques

# Adopter les bons réflexes


## Protéger les données de l'établissement

## Je protège les données personnelles

L'utilisation de données à caractère personnel qu'il s'agisse de données appartenant à des collaborateurs ou toute autre personne physique est **strictement encadrée par la loi et doit être respecté sous peine d'amendes.**

**Un délégué à la protection des données (DPO) a été nommé** pour apporter un support dans les projets traitant des données à caractère personnel.

Je ne laisse pas de documents papier confidentiels ou d'équipements (PC, téléphone, supports de données, etc.) **sans surveillance.**

# Adopter les bons réflexes

## Je communique de manière prudente sur les réseaux sociaux

Les réseaux sociaux sont des outils utiles pour partager de l'information rapidement, toutefois attention aux informations partagées.

**Il est interdit de diffuser des informations dommageables pour GBNA ainsi que tout contenu confidentiel.**


**Communiquer avec prudence sur les réseaux sociaux**

# Adopter les bons réflexes

**Alerter au plus vite le service informatique**

## J'alerte au plus vite en cas d'incident

### En cas d'incident cybersécurité

- Débrancher le poste du réseau (Ethernet et Wifi)
- Ne pas éteindre !
- Contacter le 05 57 22 58 20 / support@gbna-sante.fr
- Récupérer les supports USB ayant eu un contact récent avec le poste.

# Conclusion et questions

**Chaque collaborateur est un acteur de la sureté et la sécurité du Système d'Information.**

Il s'agit donc d'adopter des comportements adaptés face aux risques de malveillances ou de maladresses.

**En cas de doute, n'hésitez pas à contacter le centre d'appel de la DSIH**

**Contactez le 05 57 22 58 20**
**ou**
**support@gbna-sante.fr**