SORBONNE UNIVERSITÉ

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS
Centre de la Formation et du Développement des Compétences

ADEAF

ekp ÉCOLE DE KINÉSITHÉRAPIE DE PARIS

ifsi INSTITUT DE FORMATION EN SOINS INFRIMIERS
INSTITUT HOSPITALIER FRANCO-BRITANNIQUE

FONDATION ŒUVRE DE LA CROIX SAINT-SIMON

Fondation LEONIE CHAPTAL

CROIX-ROUGE FRANÇAISE

HEALTH DATA HUB

sesan SERVICE NUMÉRIQUE DE SANTÉ

FEIMA
Fédération des Éditeurs d'Informatique Médicale et paramédicale Ambulatoire

ikigai games for citizens

ESIEE PARIS

ALLIANCE SORBONNE UNIVERSITÉ utc

SFMG le plaisir de comprendre

Relations Médicales® Raphaël Gassin

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

FRANCE 2030

SN@SU
Santé Numérique
Sorbonne Université

# Cybersécurité et Bonnes Pratiques

Plateforme des données de santé

2.1, 2.2, 3.3



Octobre 2025

# Résumé du module

**Niveau débutant**

Ce module (niveau débutant) explique **les bases de la cybersécurité et les bons réflexes** pour protéger les données, en particulier en santé. Il présente les **principales menaces** (phishing, ransomware, virus…), les **bonnes pratiques** à adopter au quotidien (mots de passe, mails, accès, sauvegardes, vigilance) et **quoi faire en cas d'attaque** (alerter, isoler, conserver les preuves, notifier). Il rappelle enfin que la sécurité est **collective** et encadrée par des rôles et ressources (RSSI, DPO, CNIL, CERT Santé).

# Cybersécurité : mais de quoi parle-t-on ?

**Cybersécurité, n.f.**
État d'un système d'information qui **résiste** aux **cyberattaques** et aux **pannes** accidentelles survenant dans le **cyberespace**.

## Définition de l'Union européenne

La cybersécurité recouvre les **activités** nécessaires pour **protéger les réseaux et les systèmes** d'information ainsi que **les utilisateurs** de ces systèmes et les autres personnes exposées aux cybermenaces.

Il est fréquent de voir les termes **cybersécurité** et **sécurité numérique** employés comme des synonymes.

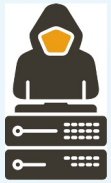
Pourtant, il est communément accepté que **la cybersécurité renvoie à la sécurité des systèmes d'information** tandis que **la sécurité numérique renvoie plus largement à la sécurité des systèmes et des pratiques numériques**.
Ainsi, les bonnes pratiques de sécurité numérique sont aussi bien **techniques** que **comportementales**.

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Cybersécurité : un peu de sémantique

"La cybersécurité est la **pierre angulaire de la transformation numérique** et les besoins dans ce domaine concernent **tous les secteurs** ; elle doit donc être intégrée à un vaste éventail de champs d'action et d'initiatives stratégiques."

*Note de l'ENISA (Agence de l'Union européenne pour la Cybersécurité)*



## Cyberattaque, n.f.

**Ensemble coordonné d'actions** menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur **disponibilité**, à leur **intégrité** ou à leur **confidentialité**.

Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée. Si elle constitue une infraction pénale, on parle de **cybercriminalité**.

## Cyberespace, n.m.

Espace constitué par les **infrastructures interconnectées** relevant des technologies de l'information, et notamment **d'Internet**.

"Perçu comme un **nouveau territoire**, le cyberespace est un espace difficile à définir - et donc à sécuriser - car il repose sur un **ancrage à la fois physique et informationnel**."

*Note de l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information)*

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# Cybersécurité : une vieille histoire…

| | |
|---|---|
| **Antiquité** | **Cyber ⇦ Kubernân (grec) ⇨ Gubernare (lat.) ⇨ Gouverner (fr.)** |
| **2e Guerre mondiale** | Le premier *hacking* de l'Histoire : **Alan Turing déchiffre le code** de la machine allemande *Enigma* grâce à une "bombe cryptologique"… et une **erreur humaine** des nazis ! |
| **Années 60 - 70** | ARPANET (ancêtre d'Internet) connecte des ordinateurs entre eux. Les **premiers messages malicieux** (ancêtres des virus) circulent dans le réseau. Le ver *Creeper* se propage. |
| **Années 80** | Le **piratage de réseaux** se développe. Le virus *Vienna* est décrypté. L'expert allemand en cybersécurité Bernd Fix crée le **premier logiciel antivirus** pour le supprimer. |
| **Années 90** | Les virus se développent à grande échelle. En 1999 et 2000, *Melissa*, *KAK et I Love You* **infectent plus de 10 millions d'ordinateurs** à travers les échanges de fichiers MS **Word** et la messagerie **Outlook**, et rendent inutilisables les fichiers qu'ils contiennent. |
| **Années 2000** | Adoption par l'UE d'une **Convention sur la cybercriminalité**. Naissance des Anonymous, premier collectif de pirates informatiques universellement reconnu. Création de **l'ANSSI**. |
| **Années 2010** | Google victime de l'opération *Aurora* dirigée par la Chine. 3 milliards de comptes Yahoo corrompus par une intrusion. Entrée en application du **RGPD en mai 2018 (Union européenne)**. |
| **Années 2020** | Adoption par l'UE d'une série de **directives cyber**. Multiplication des acteurs publics et privés de la cybervigilance et de la cybersécurité. Explosion de la **cybercriminalité**. |

# Lutter contre les idées reçues pour mieux protéger les données

### Idée reçue n°1

*“Les petites structures comme les cabinets médicaux ou les cliniques ne sont pas des cibles pour les cyberattaques”*

Tout le monde est menacé par les cyberattaques, elles ne sont pas réservées aux grands hôpitaux ! Ce sont même **les petites cliniques qui sont les plus vulnérables,** car elles sont souvent sous-équipées, et les personnels moins formés. Plus largement, toutes les entités manipulant des données sensibles, telles que les données de santé, sont des cibles pour les cybercriminels.

### Idée reçue n°2

*“Notre établissement est conforme au RGPD, on ne risque rien !”*

La conformité aux régulations et aux normes en vigueur est importante, mais elle ne suffit pas à garantir une protection totale. Un établissement de santé peut respecter le RGPD et **en même temps avoir des systèmes obsolètes**, pas mis à jour face aux dernières menaces et exposés aux vulnérabilités…
Ces failles sont à l’origine de 42% des incidents déclarés par les établissements de santé !

### Idée reçue n°3

*“La cybersécurité, c’est trop compliqué” / “c’est un truc de DSI de haut niveau”*

Non, les outils de cybersécurité sont aujourd’hui faciles d’accès et d’utilisation. Ils sont à la portée de tout responsable d’un système d’information, quelle que soit la taille de l’établissement, et des professionnels de santé eux-mêmes. Et la cybersécurité est aussi une affaire de responsabilité et d’attention collectives : **ce n’est pas très compliqué, mais il faut s’y mettre tous ensemble**…

### Idée reçue n°4

*“J’ai un antivirus sur mon PC, je suis protégé”*

Un **antivirus** installé sur son ordinateur est **nécessaire, mais pas suffisant**. Il ne vous protège pas des réseaux wifi non sécurisés, ni des malwares apportés par certains logiciels, ni du phishing !
*« Et sur Mac, pas besoin d’antivirus »* ?
Sachez que désormais le nombre de menaces détectées par terminal sur les Macs est supérieur au nombre de menaces détectées sur Windows.

### Idée reçue n°5

*“Un site avec un cadenas dans l’adresse, c’est sans risque”*

Google Chrome a retiré le petit cadenas qui apparaissait dans la barre d’adresse des sites internet sécurisés, estimant que **cette icône était trompeuse**. En effet, elle permet de savoir qu’un site utilise le protocole sécurisé HTTPS, mais **ne permet pas de s’assurer qu’il s’agit d’un site légitime et sans danger,** un site d’hameçonnage (phishing) pouvant tout à fait utiliser cette technologie !

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Pourquoi la cybersécurité doit être une priorité ?

## Les violations des données en augmentation constante, en nombre et en coût pour la société

**2022 ⇨ 2023 (France)**

**Attaques par raçongiciel :**

+30%

**Attaques par déni de service :**

+41%

**E-mails de phishing :**

+1265%

(avec intervention de l'IA)

**2023**
**Coût moyen d'une violation de données**

4 **millions €**

(hors paiement de rançons)

**Coût moyen d'une donnée volée**

144 €

(les données sont convoitées parce qu'elles ont une valeur)

**2025**
**Coût projeté de la cybercriminalité pour l'économie mondiale**

9500 **milliards €**

(5 500 milliards € en 2023)

**Quelques chiffres clés**

- **41 milliards d'appareils** dans le monde seront **connectés** à l'Internet des Objets (IoT) en 2025
- 1 entreprise ou institution française sur 2 est victime de cyberattaques au cours d'une année **(+400 % depuis 2020)**

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

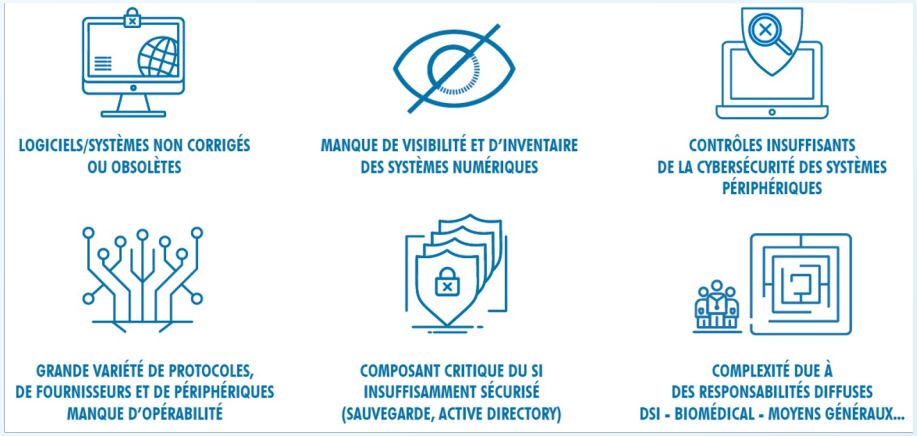
# La cybersécurité en santé c'est quoi ?

## Les activités du secteur santé reposent massivement sur le numérique et ont des impacts directs ou indirects sur la prise en charge des patients

### Des incidents de plus en plus nombreux

Les établissements hospitaliers sont fréquemment touchés par des incidents sur leurs systèmes numériques, comme le révèlent régulièrement les médias : **vol des données** de santé des patients, **blocage des dossiers patient informatisés** (DPI), provocation de **pannes** généralisées (**téléphonie, ascenseurs, climatisation, stérilisation**…) ou plus ciblées (**plateaux techniques**).

### Les vulnérabilités d'une structure de santé




### Le CERT Santé

C'est l'**organisme de cyberveille et de cybersécurité** de l'Agence du Numérique en Santé.

Il a pour missions :

- l'**appui aux établissements de santé** pour le traitement des incidents de cybersécurité
- la **veille sur la menace** de cybersécurité et la sensibilisation de la communauté
- des **audits de cybersurveillance** et des actions de prévention

### Quelques chiffres clés

- **86%** des Français considèrent leurs **données de santé** comme particulièrement **sensibles** (enquête DNS 2024)
- **18%** des notifications de cyberattaques ou cyber-malveillance concernent le **secteur de la santé**
- **2 cyberattaques** ciblent **chaque jour** des établissements de santé (11% des attaques quotidiennes)
- **58% des incidents** signalés par des établissements de santé **ont eu un impact sur les données des patients**
- **24% des signalements** ont donné lieu à un accompagnement par **le CERT Santé**.

# Par conséquent…

La protection des données est une **priorité globale** pour les années à venir

La protection des données de santé nécessite **l'acquisition d'une culture du numérique** et de la cybersécurité chez les professionnels de santé et tous les personnels qui travaillent avec eux

La protection des données est **l'affaire de tous** et de chacun !

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# PLAN

1. Comprendre les menaces, connaître le cadre légal
2. Anticiper pour se protéger
3. Réagir aux agressions

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# La cybercriminalité, ce n'est pas "gratuit" !

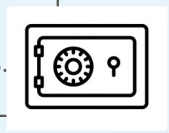
L'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) identifie **4 motifs d'attaques cyber** :

- Le **profit** - cybercriminalité à visée lucrative
- L'**espionnage** - généralement mis en œuvre pour le compte d'un Etat ou d'un concurrent industriel
- La **déstabilisation** - notamment dans le cadre d'activités politiques
- Le **sabotage**

Certains groupes de pirates (hackers "white hat") ont vocation à aider les institutions à détecter les failles et à améliorer leur sécurité. Mais la plupart des pirates cherchent à **capter des données** ou des informations **pour les monnayer** ou les utiliser à des **fins criminelles**.

**Voler des données ou de l'argent**

**Objectif : obtenir des données** personnelles, des informations confidentielles, **arnaquer** directement les personnes.



**Bloquer le fonctionnement des systèmes d'information**

**Objectif :** mettre en place un chantage pour **obtenir de l'argent** en échange d'un déblocage

**S'approprier les systèmes et les ordinateurs**

**Objectif :** détourner des appareils et **les utiliser pour commettre d'autres attaques**

**Mais comment les pirates s'y prennent-ils ?**

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# Des techniques “anciennes” toujours en vigueur…

### Les attaques par déni de service (DDOS)

**Sur-sollicitent** un serveur par une multitude de **demandes de connexions simultanées,** qui le rendent inaccessible

### Les vers, virus, trojan

**S’introduisent** dans un système d’information pour y délivrer une information conduisant à sa **mise hors service,** ou pour lui faire réaliser des **actions inadéquates**

### Les intrusions par force brute

Permettent d’**entrer dans un système** d’information en utilisant une gigantesque série de tentatives successives afin de **“casser” un code**

## Elles continuent de faire des dégâts

En 2023, les intrusions dans les sites internet des entreprises et les piratages de comptes “à l’ancienne” ont représenté 23% des cyberattaques en France.

Les faux ordres de virement et défiguration de sites ont augmenté de plus de 60% par rapport à 2022.
Les attaques par déni de service ont augmenté de 41%.

# …de nouvelles attaques toujours plus “créatives”…

## L’Union européenne identifie l’apparition de nouvelles familles de menaces :

Elles utilisent des techniques sophistiquées de **blocage des systèmes** ou de **verrouillage des bases** de données, ou s’appuient sur la **crédulité** et la confiance des internautes, pour des attaques pouvant notamment **conduire à une violation de données personnelles au sens du RGPD**.
L’agence de l’UE pour la cybersécurité (ENISA) les a listées pour **organiser la prévention** et aider les entreprises et les institutions à apporter des réponses à ces nouvelles menaces.

| Le phishing | Les ransomwares | Les logiciels malveillants | La désinformation | Le minage clandestin |
|---|---|---|---|---|
| Utilise l’email ou le sms pour proposer un “service” apparemment avantageux, ou usurper l’identité d’une autorité connue (banque, assurance), afin de conduire l’internaute à confier des données personnelles | Verrouillent l’accès à la base de données d’une entreprise ou d’une institution, et demande le paiement d’une rançon pour la débloquer | Endommagent volontairement une infrastructure pour la détruire ou la paralyser ; ou installe un système permettant d’accéder aux données sans autorisation | Utilise massivement des canaux de communication apparemment légitime (réseaux sociaux) pour publier des informations déformées ou de fausses nouvelles | Infiltre un ordinateur ou un téléphone afin de produire de la cryptomonnaie à l’insu du propriétaire de l’appareil |

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# …et des menaces plus diffuses sur les personnes

### La cybermalveillance

Diffusion de fausses informations par un canal numérique, visant à nuire à une personne (parfois à une entreprise ou une institution) en la dénigrant ou en la représentant négativement

### Le cyberharcèlement

Forme de harcèlement moral par le biais d'un support numérique : dénigrement, rumeurs, publication de photos ou vidéos compromettantes, etc.

### La cyberviolence

Degré extrême du cyberharcèlement, pouvant inclure des injures notamment racistes ou sexistes, des intimidations, des menaces, voire l'usurpation d'identité

## Elles sont sévèrement punies et font l'objet d'une vigilance accrue de la part des pouvoirs publics

Ces menaces informelles peuvent dégrader l'identité numérique des personnes, nuire à leur santé, leur réputation et leur causer d'importants traumatismes.
Les infractions sont punies de 2 à 5 ans d'emprisonnement et de 12 000 € à 75 000 € d'amende.

Deux sites internet dédiés permettent d'identifier ces menaces, de connaître le comportement à adopter pour les éviter ou les combattre, et de signaler des faits :

**cybermalveillance.gouv.fr & internet-signalement.gouv.fr**

# Protéger les personnes, mais pas seulement…

La cybersécurité se donne pour **objet prioritaire** de **protéger les personnes physiques**. La cybervigilance et la cybersécurité doivent créer un **environnement numérique suffisamment sûr** afin de préserver les personnes :

- De tout **accès frauduleux à leurs données personnelles protégées par le RGPD**, ainsi que de toute **modification ou suppression** de ces données sans autorisation
- Des **atteintes à leur "identité numérique"** et à leur réputation
- Des **atteintes à leur intégrité psychique voire physique** (suite à un chantage, une intimidation ou des menaces par exemple)
- Des **atteintes à leur situation économique** et financière (cyberattaques conduisant à un vol, un détournement d'argent, une escroquerie…)

**La cybersécurité protège aussi les entreprises et les institutions publiques et privées :**

## Leur système d'information (SI)

La cybersécurité **protège les machines**, **contrôle les accès** au SI et **assure l'intégrité** des systèmes et des réseaux.

## Leurs données

La cybersécurité i**nterdit les pénétrations frauduleuses** dans les bases de données, et protège ainsi à la fois l'entreprise / institution et ses clients / usagers.

## Leur économie

La cybersécurité garantit la pérennité et la sécurité économique de l'entreprise / institution, qui **dépend aujourd'hui fortement de son SI et de ses données**…

# Un cadre juridique européen universel : le RGPD

Le RGPD est le **cadre général de protection** des données personnelles, sur tout le **territoire de l'UE**.
Il définit précisément la notion de **données à caractère personnel, y compris les données de santé**.
Il pose des **contraintes fortes pour en assurer la sécurité**.

**_Les données de santé_ selon le Règlement général sur la protection des données (RGPD) - Art. 4. 15 :**

« *Les* ***données à caractère personnel relatives à la santé physique ou mentale****, passée, présente ou future, d'une personne physique, y compris la prestation de services de soins de santé,* ***qui révèlent des informations sur l'état de santé*** *de cette personne* »

**Une sécurité renforcée sur les données de santé**

- Le traitement des données de santé est par principe interdit, il faut pouvoir justifier d'une exception du RGPD pour pouvoir traiter les données de santé (ex. recherche scientifique, ou consentement explicite)
- La finalité du traitement des données de santé peut être l'intérêt public (ex. soin, recherche)
- Les données doivent faire l'objet de mesures de sécurité renforcées
- La durée de conservation doit être limitée au temps strictement nécessaire pour réaliser l'objectif
- La conservation des données (spécifiquement pour la France) doit être assurée par un hébergeur certifié "HDS", selon un référentiel émis par l'Agence du Numérique en Santé

# Des compléments réglementaires européens #1 : la législation dédiée à la protection des données

Depuis 2018, l'Union européenne a complété le RGPD par des directives et des règlements destinés à assurer un niveau élevé commun de cybersécurité et à encadrer certains traitements de données et la mise en oeuvre de certains systèmes particuliers.

Union européenne

## Data act

Le Règlement européen sur les données (Data Act) a pour but de **construire une économie** européenne de la donnée **respectueuse des libertés et des droits** fondamentaux.
Il encadre notamment l'interopérabilité des données à l'échelle européenne.

## Digital Services Act (DSA)

La législation européenne sur les services numériques vise à renforcer le contrôle démocratique et la surveillance des grandes plateformes.

Il dispose que **ce qui est illégal hors ligne est illégal en ligne.**

## AI act

L'AI Act est la première réglementation qui fixe un cadre légal spécifique et dédié à l'intelligence artificielle.
L'AI Act impose notamment de réaliser une **étude d'impact pour tout nouveau projet d'IA** et interdit les usages de l'IA jugés "inacceptables".

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Des compléments réglementaires européens #2 : la législation dédiée à la protection des données

Avec la directive NIS2, l'Union européenne vise à **améliorer la cybersécurité et la résilience** des réseaux et des systèmes d'information sur son territoire.
Cette nouvelle version de la directive NIS complète le règlement de 2019 sur la cybersécurité.

## La directive "Network and Information Security"

La directive NIS 2 entrée en vigueur en 2024 succède à la NIS 1 qui datait de 2013. Elle est la pierre angulaire de la lutte contre la cybercriminalité en Europe.
Elle impose aux entreprises et aux institutions publiques **d'adopter des mesures de protection strictes**, en fonction de leur "niveau de criticité".
600 "entités essentielles" et plus de 20 000 "entités importantes" sont concernées, notamment dans le secteur de la santé (tous les établissements hospitaliers français, par exemple).

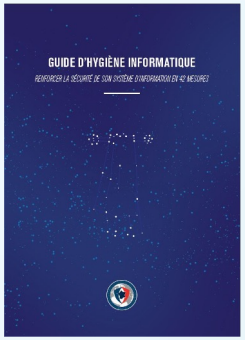
## Le Règlement sur la cybersécurité, relatif à l'ENISA

Le règlement sur la cybersécurité « vise à atteindre un niveau élevé de cybersécurité, de cyber-résilience et de confiance dans l'UE. »

- Il renforce le rôle de l'Agence de l'Union européenne pour la cybersécurité (ENISA)
- Il fixe un cadre européen commun pour les systèmes de certification de la cybersécurité
- Il permet de soutenir les institutions et autorités nationales pour l'amélioration de la cybersécurité
- Il promeut le **renforcement et l'amélioration de la prévention, de la détection et de l'analyse des cybermenaces** à l'échelle européenne.

# Des corpus et des guides spécifiques à la santé pour la mise en œuvre de la cybersécurité #1

Pour permettre à tous les acteurs de la santé de s'y retrouver dans les obligations et les bonnes pratiques en cybersécurité, l'ANSSI a élaboré un "Guide d'hygiène" à suivre.
Il complète et documente la PGSSI-S.




## Le Guide d'hygiène informatique

Il est conçu comme une **feuille de route** qui accompagne les **responsables de la sécurité des systèmes d'information**, dans tous les types d'entité.

Il présente **42 mesures essentielles pour assurer la sécurité du système d'information** et les moyens de les mettre en oeuvre. Elles constituent le socle minimum à respecter pour protéger les informations de la structure.
Il s'appuie sur autant **d'outils pratiques** aidant à la compréhension des mesures à prendre.

## La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

Élaborée par l'Agence du Numérique en Santé (ANS), la PGSSI-S constitue un corpus documentaire qui **encadre les règles spécifiques de sécurité pour l'e-santé** :

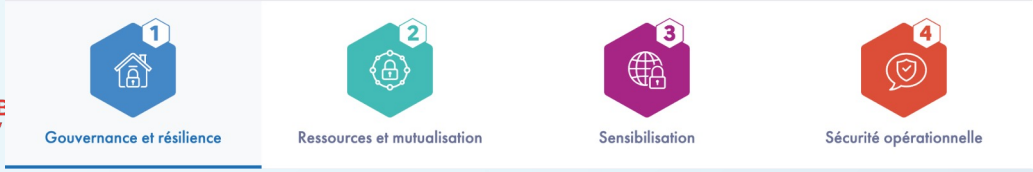
- Elle s'applique dès lors que des données de santé sont utilisées
- Elle s'applique au service public et au privé : les professionnels de santé, les secteurs médico-social et social, les établissements de soins et les offreurs de services
- Elle encadre notamment **l'identification électronique et l'authentification des patients** à travers un **Référentiel des Moyens d'Identification Électronique** (Identité Nationale de Santé, Application Carte Vitale…).

# Des corpus et des guides spécifiques à la santé pour la mise en oeuvre de la cybersécurité #2

Malgré un encadrement de mieux en mieux documenté, de plus en plus complet et unifié à l'échelle européenne, les acteurs de la santé se trouvent encore parfois dans des situations qu'ils ne savent pas résoudre. Des programmes et des référentiels les aident à s'y retrouver.

## Cybersécurité accélération et Résilience des Établissements (CaRE)

Bonnes pratiques, aide à la réponse à incident, mise en œuvre d'une main courante ou d'un relevé d'actions, gestion de la crise cyber : l'ANS a déployé un **programme permettant aux établissements de santé de répondre concrètement à l'augmentation de la cybermenace**, de gérer efficacement les événements cyber, et de structurer la gouvernance de la cybersécurité entre acteurs nationaux, régionaux et locaux.
Le programme se déploie selon 4 axes :




## Le groupe de travail APSSIS - AFIB pour les dispositifs médicaux connectés

L'Association française des ingénieurs biomédicaux (AFIB) a mis en place un groupe de travail spécifique avec l'Association pour la sécurité des systèmes d'information de Santé (APSSIS), qui fédère l'écosystème de la SSI en santé.

Le groupe a publié un **référentiel sous la forme d'un questionnaire joint aux cahiers des charges** des appels d'offres de dispositifs médicaux connectés.

Il compte **32 objectifs de sécurité** et 48 questions fermées concernant différents aspects de la sécurité en santé : techniques, juridiques (RGPD, certifications, etc.) et de gouvernance.

# PLAN

1. Comprendre les menaces, connaître le cadre légal
2. Anticiper pour se protéger
3. Réagir aux agressions

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# Mesures physiques : protéger les lieux

### Sécuriser l'accès aux locaux

- Délimiter le niveau de sécurité des différentes zones d'un bâtiment et définir les procédures d'accès (moyens d'authentification) en fonction de la sensibilité
- Tenir à jour une liste des personnes
- Conserver une trace des accès

### Sécuriser les matériels

- Tenir à jour un inventaire des matériels informatiques
- Prévoir une redondance matérielle des unités de stockage de données
- Protéger les postes légers ou nomades par un câble physique
- Chiffrer les données stockées sur les postes nomades
- Limiter drastiquement l'utilisation des clés USB ; chiffrer les données sur tous les supports amovibles

## ▲ En quoi cela protège les données ?

➔ Les mesures de sécurité physiques limitent le risque que des personnes non autorisées n'accèdent physiquement aux données à caractère personnel

➔ Elles limitent le risque que des données soient dérobées par le vol d'un matériel

➔ En cas d'incident, elles permettent d'identifier les causes, notamment par la traçabilité qu'elles établissent (liste des personnes autorisées, authentification des collaborateurs et visiteurs, trace des accès, alerte en cas d'effraction, etc.).

# Mesures logiques : protéger les systèmes

### Contrôler l'accès logique aux données

- Créer et gérer les profils d'utilisateurs et leurs droits
- Créer des identifiants uniques pour les personnes qui doivent se connecter
- Associer un mot de passe unique à chaque compte, et gérer une politique de mots de passe rigoureuse
- Limiter le nombre et l'usage des comptes "administrateurs"
- Journaliser les accès

### Lutter contre les logiciels malveillants

- Installer un antivirus bien configuré et mis à jour en continu
- S'assurer que les utilisateurs ne peuvent pas désactiver l'antivirus
- Mettre en œuvre des mesures complémentaires de filtrage : pare-feu, proxy…
- Installer un programme de lutte contre les logiciels espions (anti-spyware)
- Centraliser les événements de sécurité

### Sécuriser les canaux

- Etablir et tenir à jour une cartographie détaillée du réseau, incluant tous les accès à internet
- Surveiller l'activité réseau
- Interdire le raccordement d'équipements informatiques non maîtrisés
- Limiter la prise en main à distance des matériels informatiques
- Mettre en place une authentification forte pour les utilisateurs accédant à distance au système d'information interne

## ▲ En quoi cela protège les données ?

➔ Le contrôle des accès **limite le risque que des personnes non autorisées entrent** dans le système par voie électronique et sans effraction constatable…

➔ Les moyens de lutte anti logiciels **protègent** les postes de travail et les serveurs - donc les données - **contre les codes malveillants**

➔ La surveillance des canaux informatiques **diminue la possibilité qu'ils soient exploités**, directement ou indirectement, pour porter atteinte aux données.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# Mesures organisationnelles et gouvernance : faire vivre la cybersécurité dans l'entreprise

### Organiser la politique de protection de la vie privée

- Définir et mettre en place une organisation pour diriger et contrôler la sécurité et la protection des données
- Créer une base documentaire formalisant les objectifs cyber
- Intégrer la politique de protection dès la conception des projets (*Privacy by design*)
- Concevoir un Plan de Continuité / Reprise d'Activité (PCA - PRA)

### Gérer les personnels

- Déployer un plan encadrant les mesures de sensibilisation des personnels :
  - dès l'arrivée en fonction
  - tout au long de l'activité
- Prévoir une procédure décrivant les mesures prises au départ des personnels accédant aux données (suppression de compte, restitution d'appareils nomades, etc.)

### Gérer les risques et les incidents

- Définir et rédiger une politique de maîtrise des risques portant sur les droits et libertés des personnes
- Concevoir une organisation opérationnelle permettant de détecter et de traiter les événements liés à la cybersécurité
- Développer une culture de l'information et de la transparence vis-à-vis des usagers lors des incidents

## 🔺En quoi cela protège les données ?

➔ L'organisation et la documentation de la politique de protection de la vie privée fixe un **cadre adéquat pour permettre le pilotage** de la sécurisation des données

➔ Une gouvernance transparente des questions de cybersécurité **diminue le risque que des personnes aux compétences inadéquates accèdent aux données** et leur portent atteinte.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# Le facteur humain, premier rempart

Dans 85% des cas, la réussite d'une cyberattaque est due à une erreur humaine : une inattention, un clic malencontreux, ou simplement une session restée ouverte…

## On ne surfe pas n'importe où

Votre institution vous protège en vous empêchant de vous rendre sur des sites peu sûrs ou sur des réseaux sociaux ouverts lorsque vous êtes connecté à votre environnement de travail.
Si ce n'est pas le cas, vous devez le faire par vous-même, afin de limiter les risques d'introduire un virus dans le système d'information.

## On oublie sa date de naissance

Un mot de passe ne doit JAMAIS utiliser des chiffres qui se suivent, des mots simples, votre date de naissance… Cette règle paraît évidente, mais en 2022 les deux mots de passe les plus courants étaient encore :
- motdepasse
- 123456

## On ne clique pas sur tout ce qui bouge

94% des logiciels malveillants sont délivrés par email. Ne cliquez jamais sur un lien sans regarder ce qui s'affiche en laissant quelques secondes votre pointeur dessus ; et n'ouvrez pas un mail sans regarder le nom de l'expéditeur (celui qui s'affiche entre <--->)

## On ferme toutes les portes derrière soi


Lorsque vous quittez votre ordinateur, ne laissez jamais la session en cours ouverte : mettez l'appareil en veille, afin qu'aucune personne non autorisée ne soit tentée d'y regarder.

## On ne prête pas son login

Votre login et le mot passe associé représentent votre clé unique pour entrer dans le système. Les prêter à un tiers, même "pour une fois", vous fait courir deux risques :
- qu'il les réutilise ultérieurement pour se connecter à un système auquel il n'a pas accès normalement
- que vous soyez tenu pour responsable en cas d'incident causé par ce tiers…

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Les rôles-clés de l'organisation : des référents à consulter, des référentiels à suivre

**Pour renforcer encore la cybersécurité en entreprise ou dans les établissements de santé, des référents sont souvent présents. Ils jouent généralement un rôle d'information et de conseil.**

### Le DPO

La désignation d'un **Délégué à la Protection des Données est obligatoire** dans tout établissement de santé, et plus largement dans toute entité traitant des données de santé.
Il joue un rôle de conseil et d'orientation, forme les équipes aux bonnes pratiques en cybersécurité, et fait l'interface avec les partenaires publics et privés, ainsi qu'avec la CNIL.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

### La CNIL

La Commission Nationale pour l'Informatique et les Libertés dispose d'un **service dédié à la santé**. Ses conseillers sont disponibles sur rendez-vous téléphoniques. Leur rôle est d'**accompagner les établissements**, notamment à travers le DPO, dans la construction de nouveaux projets impliquant des données de santé, et dans l'**analyse de risques** liés.

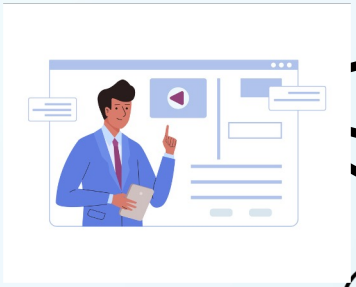
### Le RSSI

Dans la plupart des établissements de santé, vous pouvez faire appel au Responsable de la Sécurité des Systèmes d'Information. Rattaché généralement à Direction des Systèmes d'Information ou à la Direction Informatique, il **doit être consulté pour tout projet induisant un risque cyber**, même mineur.

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# La formation, une assurance-vie pour la cyber

**Toute personne, toute équipe concernée par des traitements de données doit se former en continu à la cybersécurité,** afin de rester informée de l'état de l'art, d'exercer et de renouveler ses réflexes et sa vigilance… Cette formation concerne aussi bien les établissements que les professionnels de santé libéraux.



**Dans les grandes entreprises et établissements de santé, des formations internes dédiées à la protection des données et à la sécurité informatique sont régulièrement organisées.**

**Si ce n'est pas le cas, vous pouvez le demander auprès de votre RSSI ou de la DRH de votre établissement. Le Centre de formation de l'ANSSI (CFSSI) propose des formations dispensées par ses experts pour les agents des trois fonctions publiques.**

**Le DPO, obligatoire dans les entités traitant des données de santé, doit mettre en œuvre chaque année une session de sensibilisation à la protection des données personnelles**

**Le MOOC de la CNIL**

La CNIL propose une formation en ligne de 5 h pour mieux comprendre et savoir gérer les questions liées aux données personnelles. Elle est gratuite et se déroule en 5 modules : le RGPD, les grands principes, les responsabilités, les outils de la conformité - et un module thématique pour les collectivités territoriales.

**Les ateliers du HDH**

Le Health Data Hub propose des formations accessibles en ligne et sous forme de webinaires sur le sujet des données de santé. De nombreux thèmes sont abordés : le SNDS, les entrepôts de données, les données de santé-environnement, etc.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

https://atelier-rgpd.cnil.fr/login/index.php

https://www.health-data-hub.fr/formations

# PLAN

1. Comprendre les menaces, connaître le cadre légal
2. Anticiper pour se protéger
3. Réagir aux agressions

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# L'établissement est attaqué … Que s'est-il passé ?


*Hervé travaille au service RH d'un petit* ***établissement hospitalier****. Il a reçu un* ***email du Ministère de la Santé*** *l'informant que les personnels de santé publique allaient obtenir une prime exceptionnelle !*
***Il a cliqué sur le lien*** *"Savoir si vos équipes sont éligibles"…*

Lorsque Hervé clique sur le lien, il se rend sur un site qui active en réalité un ransomware, **un logiciel qui s'installe instantanément dans son système**

*Il avait pourtant confiance car tout semblait indiquer qu'il s'agissait réellement d'un mail du ministère :*
***logo,***
***adresse mail,***
***signature du ministre…***

Hervé n'a **pas prêté attention à l'URL** qui apparaissait en surimpression sous le pointeur de sa souris, juste avant qu'il ne clique : **www.ransom$€$.ru**

A quelques bureaux de celui d'Hervé, Célia, responsable des admissions, ne parvient plus à ouvrir les dossiers patients. Elle a beau tenter de s'identifier, le serveur lui renvoie "mot de passe erroné".
Sur tous les ordinateurs de l'hôpital, une fenêtre s'affiche avec un compte à rebours et un message très inquiétant :

*L'accès à vos données a été bloqué. Elles seront effacées dans 23h59:00.*
*Vous devez verser 100 000 € à l'adresse indiquée …*

Le ransomware, en s'installant dans le système de l'établissement via le réseau auquel Hervé est connecté, a **bloqué l'accès à toutes les données patients** !

Heureusement, les données avaient été sauvegardées en copie dans plusieurs serveurs. Cette précaution a permis de ne pas avoir à verser de rançon aux pirates, qui n'ont eu accès qu'à un serveur…

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# J’ai été attaqué ? Les gestes qui sauvent #1

Une cyberattaque provoque toujours un moment de grande tension, même si on est bien préparé. Quels sont les premiers gestes à accomplir ? Comment gérer les “premiers secours” ?

1

**Mettre l’organisation en état d’alerte.**

La première action à conduire est d’**alerter le support informatique**, puis tous les acteurs de l’organisation, afin que chacun s’assure de ne pas aggraver la situation. Si l’organisation a consigné des mesures de crise dans des notes internes, celles-ci doivent être de nouveau communiquées à tous ses membres.

2

**Isoler les systèmes.**

L’équipe technique, sous la responsabilité du DSI et/ou du RSSI, doit avant tout protéger les données des actions malveillantes. Elle doit **isoler le SI et les bases de données des réseaux** (internet et local) afin de limiter la poursuite de l’incident, notamment s’il s’agit d’une intrusion.

3

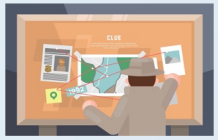
**Constituer une équipe de crise.**

Les personnes qui vont piloter la gestion de crise, contrer l’attaque et en corriger les conséquences doivent être **parfaitement coordonnées** : composantes technique, RH, juridique, financière, communication…

C’est souvent le DPO qui joue le rôle pivot, mais ce peut être aussi un dirigeant ou le RSSI.

4

**Conserver les preuves.**



Il est indispensable de constituer un dossier de preuve qui **documente l’incident** : traces d’effraction (physiques ou numériques), logs, état du système horodaté… Ces preuves serviront pour instruire une plainte si nécessaire.

Ces “**premiers secours**” sont vitaux. Plus vous réagissez **vite**, avec **sang-froid** et **de façon adéquate**, moins l’attaque risquera de vous affecter gravement.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

# J’ai été attaqué ? Les gestes qui sauvent #2

Les premiers instants passés, l’organisation est en place.
Il faut maintenant gérer la crise.

**1. Activer les solutions de secours :** pour pouvoir continuer d’assurer les services, vous devez mettre en route votre **plan de continuité et/ou de reprise d’activité (PCA / PRA).**

**2. Déclarez le sinistre :**

- effectuez rapidement les démarches **auprès de votre assureur**, et aussi **de votre banque** si des informations permettant des transferts de fonds ont été volées ;
- **notifiez la violation à la CNIL dans les 72h** suivant la prise de connaissance si elle présente un risque pour les personnes ; notifier les personnes concernées si ce risque est élevé ;
- faites remonter l’incident à **votre Groupement Régional d’Appui au Développement de la e-Santé (GRADeS) et à l’ARS.**

**3. Portez plainte :** fournissez **au commissariat ou à la gendarmerie** toutes les preuves en votre possession.

**4. Identifiez l’origine de l’attaque :** lancez une enquête afin de comprendre le mécanisme de l’incident et de **pouvoir corriger vos éventuelles failles.**

**5. Gérez votre communication :** informez **vos patients et autres administrés ou clients**, vos partenaires, et l’ensemble de vos collaborateurs. **Soyez transparents**, ne minimisez pas, mais fournissez aussi toutes les informations sur les solutions que vous mettez en place pour résoudre la crise.

# J'ai été attaqué ? Les gestes qui sauvent #3

Une fois l'attaque maîtrisée et dépassée, il est indispensable d'en tirer les leçons
**pour améliorer son niveau de cybersécurité et de cybervigilance**

## Sécurisation et réorganisation cyber

- ➔ Ne conduisez **aucune action sur les données dont vous avez la charge** sans être assuré (auprès de votre RSSI ou votre service informatique) :
  - ◆ que les failles ont toutes été repérées et sécurisées
  - ◆ que les vulnérabilités ont été corrigées
- ➔ Assurez une **remise en service progressive** et contrôlée du système d'information
- ➔ Vérifiez qu'une surveillance étroite du fonctionnement des systèmes est assurée par les services compétents, afin de **détecter toute reprise de l'incident** ou nouvelle attaque

*Vous pouvez **solliciter l'aide du CERT Santé** (Computer Emergency Response Team) à tout moment de la crise. Ce service a été créé par l'ANS pour venir en appui des acteurs de la santé dans la réponse aux incidents de cybersécurité.*

## Modification et optimisation des plans

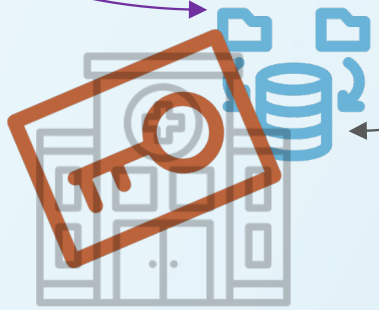
- ➔ Tirez les enseignements de l'attaque et des raisons pour lesquelles elle a pu se dérouler
- ➔ Listez les points qui **n'ont pas (ou qui ont mal) fonctionné** dans votre gestion de crise :
  - ◆ les 24 premières heures
  - ◆ l'activation des PCA-PRA
- ➔ Modifiez et optimisez **tout ce qui vous a semblé défaillant**, insuffisamment performant, difficile à mettre en œuvre…

*Une cyberattaque peut générer **d'importants risques psychosociaux** dans une organisation : sentiment de sidération, d'incompétence, de culpabilité. N'hésitez pas à solliciter votre DRH pour prendre en compte ce risque et l'accompagner.*

# Détecter les incidents de cybersécurité en santé

## Le médecin libéral

Pour son cabinet de ville, le médecin libéral gère des **logiciels métiers, qui sont autant de points d'entrée pour les cybermenaces** ; et les données de ses patients, qui doivent être sécurisées de façon draconienne.
Pour lui, la **détection précoce des incidents** est vitale !
Il doit pour cela :
- installer des **outils performants** sur son système d'information (antivirus, anti-malware, logiciel de nettoyage)
- respecter une hygiène rigoureuse quant à ses **mots de passe**, sa **navigation** sur internet, la gestion de ses **emails**, etc.
- bien sûr, s'interdire d'échanger des informations patient sur les **réseaux sociaux**...



## L'agent d'une entité de recherche

Dans une entité de recherche, les agents (ARCs, médecins investigateurs...) **manipulent** quotidiennement de très **nombreuses données**. Il est crucial qu'ils soient attentifs à toute situation anormale : dysfonctionnement d'un système, d'une base de données, accès impossible ou corrompu...
En cas de **doute**, ils doivent signaler la **situation suspecte** au référent ou au **support informatique** / numérique, afin qu'ils examinent le cas et que des mesures de prévention soient prises le plus rapidement possible.

## Le médecin hospitalier

La structure de **l'établissement de santé** est une sécurité pour le médecin hospitalier : elle **gère la cybersécurité** pour son compte...
Pour autant, le médecin travaillant en établissement peut être directement confronté à une cyberattaque et se trouver en **première ligne**. S'il constate un problème sur des données ou un comportement étrange du système d'information qu'il utilise, il doit en **informer sans délai le RSSI et/ou le DPO** de l'établissement !

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Prévenir les risques sur sa réputation… et sur l'image des patients !

## Attention à *toutes* vos publications sur les réseaux sociaux

Même si les réseaux sociaux sont un bon moyen de construire son image de professionnel de santé, il est vital de ne pas y publier n'importe quoi !

- Lorsque vos patients publient un avis, répondez courtoisement, même si vous êtes mis en cause !
- Ne donnez pas d'informations personnelles pouvant vous exposer
- Ne publiez pas de contenus tombant sous le coup de la loi : diffamation, incitation à la haine, propos discriminatoires…
- Ne publiez pas de photos protégées par le droit d'auteur.

Attention : les patients savent vous chercher sur les réseaux… et **les publications de vos comptes personnels (Facebook, Instagram, etc.) seront facilement assimilées à vos comptes et à votre activité professionnelle !**

## Protégez la vie privée de vos patients

L'utilisation rigoureuse des outils de communication est aussi importante pour préserver la vie privée et l'image des patients.

- **Ne parlez pas de vos patients sur les réseaux sociaux**, même de façon anonyme. Ce qui est "non identifiant" pour vous ne le sera pas forcément pour quelqu'un qui lira votre propos et qui pourra reconnaître dans le "cas" que vous présentez son voisin, son cousin ou son collègue.
- **Utilisez les services d'une messagerie sécurisée de santé (MSS)** pour toute communication comportant des données de santé au sens du RGPD (diagnostic, compte-rendu, documents d'imagerie, résultats d'analyses, etc.). Ces informations n'ont pas leur place sur Gmail, ni sur X !
- **Ne demandez pas à ChatGPT de vous rédiger un compte-rendu !** Les logiciels métiers des professionnels de santé disposent désormais de service d'IA qui vous permettent d'enregistrer votre consultation et de mettre en forme votre compte-rendu ; ils sont sécurisés, alors que les IA génératives tout public stockent les informations que vous leur fournissez… et les réutilisent pour leur apprentissage, ce qui peut les conduire à révéler des informations sensibles…

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

# Des obligations spécifiques pour le responsable de traitement de données de santé

Le responsable d'un traitement de données de santé, quel qu'il soit, doit mettre en œuvre certaines mesures spécifiques pour protéger les personnes concernées par le traitement. Ses sous-traitants et ses partenaires sont eux aussi concernés.

### Certification HDS

La conservation des données de santé, notamment dans le cadre de l'utilisation pour le soin, doit obligatoirement être assurée par un hébergeur certifié HDS.
Les médecins de ville sont exemptés de cette obligation s'ils hébergent les données en propre (mais pas s'ils ont recours à un prestataire).

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

### Analyse d'impact

Tout traitement de données de santé doit préalablement faire l'objet d'une analyse d'impact (AIPD) pour évaluer le risque portant sur les personnes concernées (les patients).
Cette analyse doit être communiquée à la CNIL si elle montre un risque élevé pour les personnes.

dpo

### Désignation d'un DPO

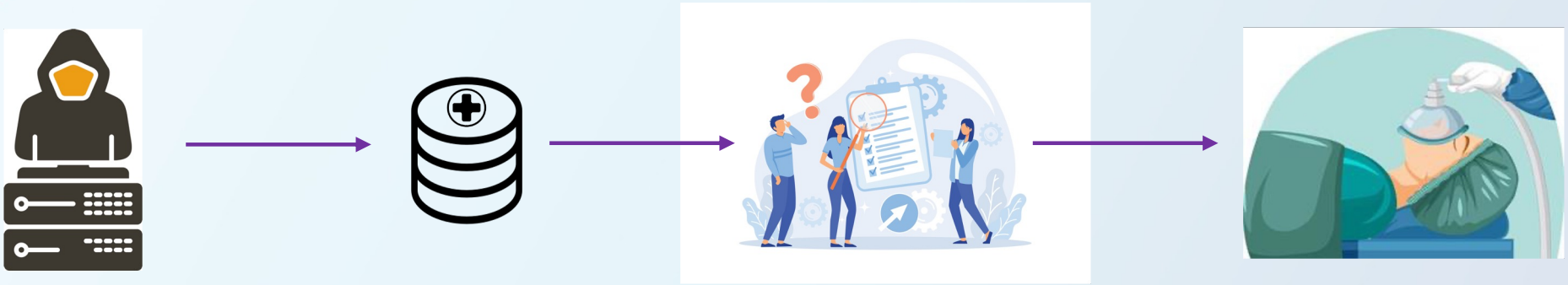
Toute organisation exploitant des données de santé, que ce soit comme responsable de traitement ou comme sous-traitant, doit désigner un Délégué à la Protection des Données, interne ou externe.
Le DPO ne doit pas être un dirigeant de l'entité. Il peut être certifié par un organisme.

Comme toute entité traitant des données personnelles, le responsable de traitement de données de santé et ses sous-traitants doivent :

- **consigner chaque traitement** dans un registre, en indiquant sa finalité, ses destinataires, la durée de conservation des données
- **tenir une documentation complémentaire** sur ses sous-traitants, les consentements obtenus, les incidents et violations constatés…
- **informer les personnes concernées** lorsqu'un incident de cybersécurité portant sur leurs données leur fait courir un risque particulier

SORBONNE UNIVERSITÉ

# Mauvaise prise en charge, réaction trop lente : des conséquences grave pour les patients…



**Un incident de sécurité passé inaperçu sur une base de données ?**

**Une cyberattaque  prise en charge trop lentement ?**

**Une menace insuffisamment prise au sérieux ?**

**Ce sont les personnes concernées - le plus souvent les patients - qui en subissent les conséquences les plus graves !**

**Données volées ou accédées frauduleusement :**
risque de chantage, d'usurpation d'identité, d'identification illégale à des fins de privation d'un droit ou du bénéfice d'un service (de santé, d'assurance, etc.)

**Données modifiées de façon non autorisée :**
risque de modification inopportune ou d'arrêt d'un traitement, d'erreur médicale, de perte de chance (dans le cadre d'une recherche interventionnelle)…

**Données détruites :**
risque de perte d'accès à un dossier médical ou à un traitement, de perte de chance (dans le cadre d'une recherche interventionnelle)…

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

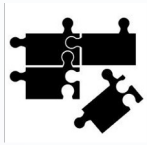
# En conclusion


# TAKE HOME MESSAGES La vigilance numérique est un tout…

**Cybersécurité, cyber-vigilance, cyber-hygiène :** ces concepts sont étroitement liés et nécessitent une **approche globale, collective et continue**

**Il est indispensable d'être préparé et formé :** les exercices d'anticipation et de simulation du programme CaRE, le MOOC de la CNIL, les formations de l'ANSSI, les conseils du CERT Santé sont des aides précieuses qui doivent être sollicitées.

**La cybersécurité dans une organisation, c'est l'affaire de tous :** chacun doit participer à la promotion d'une culture partagée de la sécurité. Cette attitude est d'autant plus nécessaire dans les organisations qui traitent des données de santé, particulièrement sensibles. Elle nécessite de mettre en œuvre et d'étudier des scénarios pratiques, des cas d'usage, pour une appropriation collective de cette culture.



**La menace sur les données de santé vient souvent de l'extérieur des établissements, mais aussi parfois de l'intérieur :** il est indispensable de penser en continu les questions d'accès aux données, de les documenter et de mettre en place les protocoles qui permettent de limiter le risque à son minimum.

**La sécurité numérique se construit dans une approche par le risque :** il est indispensable d'entretenir des analyses de risque et de les faire évoluer de façon continue pour maintenir un niveau supérieur de cybersécurité.

SORBONNE UNIVERSITÉ

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS
Centre de la Formation et du Développement des Compétences

ADERE

ekp ÉCOLE DE KINÉSITHÉRAPIE DE PARIS

ifsi INSTITUT DE FORMATION EN SOINS INFIRMIERS
INSTITUT HOSPITALIER FRANCO-BRITANNIQUE

FONDATION ŒUVRE DE LA CROIX SAINT-SIMON

Léonie Chaptal

CROIX-ROUGE FRANÇAISE

HDH HEALTH DATA HUB

sesan SERVICE NUMÉRIQUE DE SANTÉ

FEIMA
Fédération des Éditeurs d'Informatique Médicale et paramédicale Ambulatoire

ikigai games for citizens

ESIEE PARIS

ALLIANCE SORBONNE UNIVERSITÉ utc

SFMG le plaisir de comprendre

Relations Médicales® Raphaël Gassin

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

FRANCE 2030

# SN@SU
## Santé Numérique Sorbonne Université

*Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre **de France 2030** portant la référence ANR-23-CMAS-0001*