Université de Lille UFR3S-Pharmacie
Année Universitaire 2024/2025

THESE
POUR LE DIPLOME D'ETAT
DE DOCTEUR EN PHARMACIE

Soutenue publiquement le 24 septembre 2025

Par **Mr Arthur Cleuet**

Cybersécurité : Etat des lieux, exigences et bonnes pratiques pour les établissements de santé et les fabricants de dispositifs médicaux.

Membres du jury :

Président :	**Monsieur le Professeur Nicolas BLANCHEMAIN** Professeur des Universités Pharmacotechnie industrielle UFR3S – Pharmacie, Université de Lille.
Directeur de thèse :	**Monsieur Jérémy POROPANE** Directeur associé en Affaires Réglementaires Personne Responsable de la Conformité Réglementaire Biorad – Cressier Suisse
Assesseur(s) :	**Madame le Docteur Morgane MASSE** Maîtresse de Conférence – Praticienne Hospitalière Biopharmacie, Pharmacie galénique et hospitalière UFR3S – Pharmacie, Université de Lille.
	Madame le Docteur Daniela ROMON Coordinatrice Régionale en Matériovigilance et Réactovigilance Hauts-de-France

Université de Lille
UFR3S-Pharmacie
Enseignants et Enseignants-chercheurs
2024-2025

Université de Lille

Président	Régis BORDET
Premier Vice-président	Bertrand DÉCAUDIN
Vice-présidente Formation	Corinne ROBACZEWSKI
Vice-président Recherche	Olivier COLOT
Vice-président Ressources Humaine	Jean-Philippe TRICOIT
Directrice Générale des Services	Anne-Valérie CHIRIS-FABRE

UFR3S

Doyen	Dominique LACROIX
Premier Vice-Doyen, Vice-Doyen RH, SI et Qualité	Hervé HUBERT
Vice-Doyenne Recherche	Karine FAURE
Vice-Doyen Finances et Patrimoine	Emmanuelle LIPKA
Vice-Doyen International	Vincent DERAMECOURT
Vice-Doyen Coordination pluriprofessionnelle et Formations sanitaires	Sébastien D'HARANCY
Vice-Doyenne Formation tout au long de la vie	Caroline LANIER
Vice-Doyen Territoire-Partenariats	Thomas MORGENROTH
Vice-Doyen Santé numérique et Communication	Vincent SOBANSKI
Vice-Doyenne Vie de Campus	Anne-Laure BARBOTIN
Vice-Doyen étudiant	Victor HELENA

Faculté de Pharmacie

Vice - Doyen	Pascal ODOU
Premier Assesseur et Assesseur à la Santé et à l'Accompagnement	Anne GARAT
Assesseur à la Vie de la Faculté et Assesseur aux Ressources et Personnels	Emmanuelle LIPKA
Responsable de l'Administration et du Pilotage	Cyrille PORTA
Représentant étudiant	Honoré GUISE
Chargé de mission 1er cycle	Philippe GERVOIS
Chargée de mission 2eme cycle	Héloïse HENRY
Chargé de mission Accompagnement et Formation à la Recherche	Nicolas WILLAND
Chargé de mission Relations Internationales	Christophe FURMAN
Chargée de Mission Qualité	Marie-Françoise ODOU
Chargé de mission dossier HCERES	Réjane LESTRELIN

Professeurs des Universités - Praticiens Hospitaliers (PU-PH)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	ALLORGE	Delphine	Toxicologie et Santé publique	81
M.	BROUSSEAU	Thierry	Biochimie	82
M.	DÉCAUDIN	Bertrand	Biopharmacie, Pharmacie galénique et hospitalière	81
M.	DINE	Thierry	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
Mme	DUPONT-PRADO	Annabelle	Hématologie	82
Mme	GOFFARD	Anne	Bactériologie - Virologie	82
M.	GRESSIER	Bernard	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
M.	ODOU	Pascal	Biopharmacie, Pharmacie galénique et hospitalière	80
Mme	POULAIN	Stéphanie	Hématologie	82
M.	SIMON	Nicolas	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
M.	STAELS	Bart	Biologie cellulaire	82

Professeurs des Universités (PU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	ALIOUAT	El Moukhtar	Parasitologie - Biologie animale	87
Mme	ALIOUAT	Cécile-Marie	Parasitologie - Biologie animale	87
Mme	AZAROUAL	Nathalie	Biophysique - RMN	85
M.	BERLARBI	Karim	Physiologie	86
M.	BERTIN	Benjamin	Immunologie	87
M.	BLANCHEMAIN	Nicolas	Pharmacotechnie industrielle	85
M.	CARNOY	Christophe	Immunologie	87
M.	CAZIN	Jean-Louis	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	CUNY	Damien	Sciences végétales et fongiques	87

Mme	DELBAERE	Stéphanie	Biophysique - RMN	85
Mme	DEPREZ	Rebecca	Chimie thérapeutique	86
M.	DEPREZ	Benoît	Chimie bio inorganique	85
Mme	DUMONT	Julie	Biologie cellulaire	87
M.	ELATI	Mohamed	Biomathématiques	27
M.	FOLIGNÉ	Benoît	Bactériologie - Virologie	87
Mme	FOULON	Catherine	Chimie analytique	85
M.	GARÇON	Guillaume	Toxicologie et Santé publique	86
M.	GOOSSENS	Jean-François	Chimie analytique	85
M.	HENNEBELLE	Thierry	Pharmacognosie	86
M.	LEBEGUE	Nicolas	Chimie thérapeutique	86
M.	LEMDANI	Mohamed	Biomathématiques	26
Mme	LESTAVEL	Sophie	Biologie cellulaire	87
Mme	LESTRELIN	Réjane	Biologie cellulaire	87
Mme	LIPKA	Emmanuelle	Chimie analytique	85
Mme	MELNYK	Patricia	Chimie physique	85
M.	MILLET	Régis	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	MOREAU	Pierre-Arthur	Sciences végétales et fongiques	87
Mme	MUHR-TAILLEUX	Anne	Biochimie	87
Mme	PERROY	Anne-Catherine	Droit et Economie pharmaceutique	86
Mme	RIVIÈRE	Céline	Pharmacognosie	86
Mme	ROMOND	Marie-Bénédicte	Bactériologie - Virologie	87
Mme	SAHPAZ	Sevser	Pharmacognosie	86
M.	SERGHERAERT	Éric	Droit et Economie pharmaceutique	86
M.	SIEPMANN	Juergen	Pharmacotechnie industrielle	85
Mme	SIEPMANN	Florence	Pharmacotechnie industrielle	85
M.	WILLAND	Nicolas	Chimie organique	86

Maîtres de Conférences - Praticiens Hospitaliers (MCU-PH)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	CUVELIER	Élodie	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
Mme	DANEL	Cécile	Chimie analytique	85
Mme	DEMARET	Julie	Immunologie	82
Mme	GARAT	Anne	Toxicologie et Santé publique	81
Mme	GENAY	Stéphanie	Biopharmacie, Pharmacie galénique et hospitalière	81
Mme	GILLIOT	Sixtine	Biopharmacie, Pharmacie galénique et hospitalière	80
M.	GRZYCH	Guillaume	Biochimie	82
Mme	HENRY	Héloïse	Biopharmacie, Pharmacie galénique et hospitalière	80
M.	LANNOY	Damien	Biopharmacie, Pharmacie galénique et hospitalière	80
Mme	MASSE	Morgane	Biopharmacie, Pharmacie galénique et hospitalière	81
Mme	ODOU	Marie-Françoise	Bactériologie - Virologie	82

Maîtres de Conférences des Universités (MCU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	ANTHÉRIEU	Sébastien	Toxicologie et Santé publique	86
M.	BANTUBUNGI-BLUM	Kadiombo	Biologie cellulaire	87
M.	BERTHET	Jérôme	Biophysique - RMN	85
M	BEDART	Corentin	ICPAL	86
M.	BOCHU	Christophe	Biophysique - RMN	85
M.	BORDAGE	Simon	Pharmacognosie	86
M.	BOSC	Damien	Chimie thérapeutique	86
Mme	BOU KARROUM	Nour	Chimie bioinorganique	
M.	BRIAND	Olivier	Biochimie	87
Mme	CARON-HOUDE	Sandrine	Biologie cellulaire	87
Mme	CARRIÉ	Hélène	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86

Mme	CHABÉ	Magali	Parasitologie - Biologie animale	87
Mme	CHARTON	Julie	Chimie organique	86
M.	CHEVALIER	Dany	Toxicologie et Santé publique	86
Mme	DEMANCHE	Christine	Parasitologie - Biologie animale	87
Mme	DEMARQUILLY	Catherine	Biomathématiques	85
M.	DHIFLI	Wajdi	Biomathématiques	27
M.	EL BAKALI	Jamal	Chimie thérapeutique	86
M.	FARCE	Amaury	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	FLIPO	Marion	Chimie organique	86
M.	FRULEUX	Alexandre	Sciences végétales et fongiques	
M.	FURMAN	Christophe	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	GERVOIS	Philippe	Biochimie	87
Mme	GOOSSENS	Laurence	Institut de Chimie Pharmaceutique Albert Lespagnol	86
Mme	GRAVE	Béatrice	Toxicologie et Santé publique	86
M.	HAMONIER	Julien	Biomathématiques	26
Mme	HAMOUDI-BEN YELLES	Chérifa-Mounira	Pharmacotechnie industrielle	85
Mme	HANNOTHIAUX	Marie-Hélène	Toxicologie et Santé publique	86
Mme	HELLEBOID	Audrey	Physiologie	86
M.	HERMANN	Emmanuel	Immunologie	87
M.	KAMBIA KPAKPAGA	Nicolas	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	KARROUT	Younes	Pharmacotechnie industrielle	85
Mme	LALLOYER	Fanny	Biochimie	87
Mme	LECOEUR	Marie	Chimie analytique	85
Mme	LEHMANN	Hélène	Droit et Economie pharmaceutique	86
Mme	LELEU	Natascha	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	LIBERELLE	Maxime	Biophysique - RMN	
Mme	LOINGEVILLE	Florence	Biomathématiques	26
Mme	MARTIN	Françoise	Physiologie	86
M.	MARTIN MENA	Anthony	Biopharmacie, Pharmacie galénique et hospitalière	

M.	MENETREY	Quentin	Bactériologie - Virologie	87
M.	MORGENROTH	Thomas	Droit et Economie pharmaceutique	86
Mme	MUSCHERT	Susanne	Pharmacotechnie industrielle	85
Mme	NIKASINOVIC	Lydia	Toxicologie et Santé publique	86
Mme	PINÇON	Claire	Biomathématiques	85
M.	PIVA	Frank	Biochimie	85
Mme	PLATEL	Anne	Toxicologie et Santé publique	86
M.	POURCET	Benoît	Biochimie	87
M.	RAVAUX	Pierre	Biomathématiques / Innovations pédagogiques	85
Mme	RAVEZ	Séverine	Chimie thérapeutique	86
Mme	ROGEL	Anne	Immunologie	
M.	ROSA	Mickaël	Hématologie	87
M.	ROUMY	Vincent	Pharmacognosie	86
Mme	SEBTI	Yasmine	Biochimie	87
Mme	SINGER	Elisabeth	Bactériologie - Virologie	87
Mme	STANDAERT	Annie	Parasitologie - Biologie animale	87
M.	TAGZIRT	Madjid	Hématologie	87
M.	VILLEMAGNE	Baptiste	Chimie organique	86
M.	WELTI	Stéphane	Sciences végétales et fongiques	87
M.	YOUS	Saïd	Chimie thérapeutique	86
M.	ZITOUNI	Djamel	Biomathématiques	85

Professeurs certifiés

Civ.	Nom	Prénom	Service d'enseignement
Mme	FAUQUANT	Soline	Anglais
M.	HUGES	Dominique	Anglais
Mme	KUBIK	Laurence	Anglais
M.	OSTYN	Gaël	Anglais

Professeurs Associés

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	BAILLY	Christian	ICPAL	86
M.	DAO PHAN	Haï Pascal	Chimie thérapeutique	86
M.	DHANANI	Alban	Droit et Economie pharmaceutique	86

Maîtres de Conférences Associés

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M	AYED	Elya	Pharmacie officinale	
M.	COUSEIN	Etienne	Biopharmacie, Pharmacie galénique et hospitalière	
Mme	CUCCHI	Malgorzata	Biomathématiques	85
Mme	DANICOURT	Frédérique	Pharmacie officinale	
Mme	DUPIRE	Fanny	Pharmacie officinale	
M.	DUFOSSEZ	François	Biomathématiques	85
M.	FRIMAT	Bruno	Pharmacologie, Pharmacocinétique et Pharmacie clinique	85
Mme	GEILER	Isabelle	Pharmacie officinale	
M.	GILLOT	François	Droit et Economie pharmaceutique	86
M.	MITOUMBA	Fabrice	Biopharmacie, Pharmacie galénique et hospitalière	86
M.	PELLETIER	Franck	Droit et Economie pharmaceutique	86
M	POTHIER	Jean-Claude	Pharmacie officinale	
Mme	ROGNON	Carole	Pharmacie officinale	

Assistants Hospitalo-Universitaire (AHU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	BOUDRY	Augustin	Biomathématiques	
Mme	DERAMOUDT	Laure	Pharmacologie, Pharmacocinétique et Pharmacie clinique	
M.	GISH	Alexandr	Toxicologie et Santé publique	
Mme	NEGRIER	Laura	Chimie analytique	

Hospitalo-Universitaire (PHU)

	Nom	Prénom	Service d'enseignement	Section CNU
M.	DESVAGES	Maximilien	Hématologie	
Mme	LENSKI	Marie	Toxicologie et Santé publique	

Attachés Temporaires d'Enseignement et de Recherche (ATER)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	BERNARD	Lucie	Physiologie	
Mme	BARBIER	Emeline	Toxicologie	
Mme	COMPAGNE	Nina	Chimie Organique	
Mme	COULON	Audrey	Pharmacologie, Pharmacocinétique et Pharmacie clinique	
M.	DUFOSSEZ	Robin	Chimie physique	
Mme	FERRY	Lise	Biochimie	
M	HASYEOUI	Mohamed	Chimie Organique	
Mme	HENRY	Doriane	Biochimie	
Mme	KOUAGOU	Yolène	Sciences végétales et fongiques	
M	LAURENT	Arthur	Chimie-Physique	
M.	MACKIN MOHAMOUR	Synthia	Biopharmacie, Pharmacie galénique et hospitalière	
Mme	RAAB	Sadia	Physiologie	

Enseignants contractuels

Civ.	Nom	Prénom	Service d'enseignement
Mme	DELOBEAU	Iris	Pharmacie officinale
M	RIVART	Simon	Pharmacie officinale
Mme	SERGEANT	Sophie	Pharmacie officinale
M.	ZANETTI	Sébastien	Biomathématiques

LRU / MAST

Civ.	Nom	Prénom	Service d'enseignement
Mme	FRAPPE	Jade	Pharmacie officinale
M	LATRON-FREMEAU	Pierre-Manuel	Pharmacie officinale
M.	MASCAUT	Daniel	Pharmacologie, Pharmacocinétique et Pharmacie clinique

UFR3S-Pharmacie

L'Université n'entend donner aucune approbation aux opinions émises dans les thèses ; celles-ci sont propres à leurs auteurs.

REMERCIEMENTS

À mon Jury,

Je tiens à exprimer ma plus profonde gratitude aux membres de mon jury, Monsieur Blanchemain, Madame Masse et Madame Romon qui m'ont fait confiance dès le premier jour, lancé ma carrière et posé les fondations de ma formation. Il y a cinq ans, vous m'avez ouvert la porte d'un univers passionnant, m'avez challengé et encouragé à repousser mes limites. Merci pour la confiance que vous m'avez accordée, c'est un véritable honneur pour moi que vous fassiez parti de mon jury.

À mon Directeur de Thèse,

Je tiens à exprimer ma profonde gratitude à mon directeur de thèse, Monsieur Poropane, qui m'a embauché il y a deux ans en plaçant une confiance totale en mes capacités. Jérémy, tu as cru en moi, m'accordant la possibilité de piloter des projets passionnants tout en restant à l'écoute et disponible à chaque étape. Grâce à ton soutien constant et tes conseils avisés, je me suis épanoui professionnellement. J'espère que nous continuerons ensemble à relever les défis à venir.

À mes Collègues,

Je tiens à remercier chaleureusement l'ensemble de mes collègues, et tout particulièrement Marlène et Xiao, pour leur aide précieuse et leurs conseils avisés durant la rédaction de cette thèse. Merci à tous pour les moments passés ensemble dans la bonne humeur, les sessions de relecture et les discussions stimulantes autour d'un café.

À mes Proches,

Je tiens à exprimer ma profonde reconnaissance à ma famille, à ma belle-famille et à mes amis pour leur soutien moral indéfectible depuis tant d'années. Merci pour vos conseils avisés, vos encouragements constants et les moments de joie partagés ensemble qui m'ont permis de garder la motivation tout au long de ce parcours. Votre présence à mes côtés, dans les instants de doute comme dans ceux de réussite, a été une véritable source de force.

A ma chérie qui illumine chaque jour ma vie. Sans toi, rien de tout cela n'aurait été possible. Je manque de mots pour exprimer toute ma gratitude, alors je me contente de te dire merci : merci d'avoir été présente dans mes plus beaux instants comme les plus difficiles, et d'avoir contribué à faire de moi la personne que je suis aujourd'hui.

Je tiens également à dédier ces quelques lignes à mon père, à mes grands-pères et à mon cousin, qui m'ont tout appris et m'ont vu grandir. Même si votre absence a laissé un vide immense, votre mémoire guide chacune de mes démarches et nourrit ma détermination à chaque jour être une meilleure version de moi-même. Je vis chaque jour pour honorer votre héritage et incarner les valeurs que vous m'avez transmise.

« Le succès n'est pas final, l'échec n'est pas fatal : c'est le courage de continuer qui compte. »
W. Churchill

LISTE DES ABRÉVIATIONS

AMF	Authentification multifactorielle
ANSM	Agence Nationale de Sécurité du Médicament et des produits de santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP-HP	Assistance Publique – Hôpitaux de Paris
CE	Conformité Européenne
CERT	Computer Emergency Response Team (Équipe d'intervention en cas d'urgence informatique)
CNIL	Commission Nationale de l'Informatique et des Libertés
CSIRT	Computer Security Incident Response Teams (Équipe de réponse aux incidents de sécurité informatique)
DAST	Dynamic Application Security Testing (analyse dynamique de la sécurité des applications)
DDoS	Distributed Denial of Service (Attaques par Déni de Service Distribué)
DM	Dispositif Médical
DMP	Dossier Médical Partagé
DPO	Délégué à la protection des données
ECCG	Commission européenne ou du Groupe européen de certification
EDS	Entrepôt de données de santé
ENISA	European Union Agency for Cybersecurity (Agence de l'Union Européenne pour la Cybersécurité)
EOL	End of Life (Fin de Vie)
EOS	End of Support (Fin de Support)
FBI	Federal Bureau of Investigation (Bureau fédéral d'enquête)
FDA	Food Drug Administration (Agence américaine des produits alimentaires et médicamenteux)
IA	Intelligence Artificielle
IEC	International Electrotechnical Commission (Commission électrotechnique Internationale)
IMDRF	International Medical Device Regulators Forum (orum international des régulateurs des dispositifs médicaux)
IoMT	Internet of Medical Things (Internet des Objets Médicaux)
IRM	Imagerie par Résonnance Magnétique
ISO	International Organization for Standardization (Organisation internationale de normalization)
IVDR	In Vitro Diagnostic Regulation (Règlement sur les dispositifs médicaux de diagnostic in vitro)
MDCG	Medical Device Coordination Group (Groupe de coordination des dispositifs médicaux)
MDR	Medical Device Regulation (Règlement sur les dispositifs médicaux)
NHS	National Health Service (Service national de santé)
NIS	Network and Information System (sécurité des réseaux et des systèmes d'information)
NMPA	National Medical Products Administration (Administration nationale des produits médicaux de la Chine)
PMDA	Pharmaceuticals and Medical Devices Agency (Agence des produits pharmaceutiques et des dispositifs médicaux du Japon)
R&D	Recherche et Développement
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsable de la Sécurité des Systèmes d'Information
SaMD	Software as a Medical Device (logiciel en tant que dispositif médical)
SAST	Static Application Security Testing (analyse statique de la sécurité des applications)
SBOM	Software Bill of Materials (nomenclature logicielle)
SMQ	Système de Management de la Qualité
SMSI	Système de Management de la Sécurité de l'Information
SOUP	Software of Unknown Provenance (logiciel d'origine inconnue)
TIC	Technologies de l'Information et de la Communication
UE	Union Européenne

Table des matières

Table des figures

INTRODUCTION

Dans un monde de plus en plus numérique et interconnecté, la cybersécurité doit devenir une préoccupation majeure pour le secteur de la santé. En effet, bien que les technologies modernes soient aujourd'hui indispensables aux soins, elles présentent aussi un nombre important de vulnérabilités, faisant des acteurs de la santé des cibles privilégiées pour les cyberattaques.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) estime qu'entre 2022 et 2023, 86% des incidents signalés concernaient des établissements de santé (1).

Aujourd'hui, la réalité est que les établissements de santé et les fabricants de dispositifs médicaux sont confrontés à des menaces croissantes et de plus en plus sophistiquées. Celles-ci peuvent se manifester par des vols de données, des suppressions ou corruptions de données et même par le piratage de dispositifs médicaux, causant des préjudices importants pour les patients (2).

Les cyberattaques mettent donc en péril non seulement la santé des patients mais aussi la confidentialité d'informations médicales sensibles et entraînent également de graves préjudices financiers et réputationnels pour les acteurs de la santé.

La cyberattaque de l'hôpital d'Armentières en 2024, n'est qu'un exemple parmi les événements récents. Largement couverte par les médias, c'est lors de cette attaque que des cybercriminels ont pu voler et divulguer les données de santé de 300'000 patients, obligeant l'établissement à fermer son service des urgences pendant plusieurs jours (3).

Parallèlement, les dispositifs médicaux continuent eux aussi leur évolution. Alors qu'ils étaient initialement autonomes, ils sont maintenant interconnectés et souvent intégrés aux réseaux des établissements de santé.

Cette interconnexion, bien que permettant une meilleure efficacité, une réduction des erreurs ou encore une surveillance à distance, a aussi apporté son lot de nouvelles vulnérabilités (4). Medtronic, un des leaders dans la conception et la distribution de dispositifs médicaux, faisait par exemple état en 2022, de failles pouvant impacter ses modèles de pompes à insuline MiniMed 600. Les cybercriminels pouvaient ainsi obtenir un accès non autorisé à ces pompes et augmenter ou diminuer le dosage d'insuline administré avec des conséquences potentiellement sévères pour les patients (5).

Face à cette réalité, exacerbée par le contexte géopolitique global, les acteurs de la santé s'efforcent de suivre le rythme effréné de l'évolution des menaces et de se conformer aux exigences pour sécuriser leurs systèmes d'information.

Pour les établissements de santé, secteur déjà éprouvé par un manque de financement et de personnel, cela représente une charge supplémentaire conséquente.

Les fabricants de dispositifs médicaux, de leur côté, tâchent d'intégrer des fonctions de cybersécurité dans leurs produits et de maintenir une documentation technique solide démontrant la conformité des dispositifs vis-à-vis d'exigences réglementaires croissantes.

Pour les gouvernements, dont le secteur de la santé est considéré comme critique, la cybersécurité doit être une priorité pour deux raisons principales. La première est d'apporter le soutien nécessaire aux acteurs de la santé afin qu'ils répondent aux besoins. La seconde est de permettre à la population de continuer à accéder à des soins de qualité tout en garantissant la confidentialité de leurs données.

Le pharmacien, quant à lui, est un partenaire indispensable pour la mise en œuvre de la cybersécurité dans le secteur de la santé. Avec son rôle transversal et sa présence dans les établissements de santé, les officines, l'industrie pharmaceutique, les fabricants de dispositifs médicaux et également dans les organismes de régulation, il est l'un des acteurs principaux pour une intégration réussie des pratiques de sécurité.

Cette thèse d'exercice a pour objet de dresser un état des lieux synthétique des menaces pesant sur les établissements de santé et les fabricants de dispositifs médicaux, en évaluant leurs répercussions sur la sécurité des patients, l'intégrité des données et la continuité des opérations, puis d'exposer les exigences de cybersécurité définies par les référentiels législatifs et normatifs de l'Union européenne. Elle propose enfin une analyse des solutions et perspectives visant à réduire ces risques, en soulignant la nécessité d'adopter une stratégie proactive et collaborative pour renforcer la résilience du secteur sanitaire.

Au-delà de la démonstration de l'actualité du sujet, cette thèse d'exercice a pour vocation de mettre en exergue son caractère insuffisamment appréhendé et pourtant crucial, soulignant l'urgence de reconnaître et de traiter la cybermenace avec la rigueur scientifique et opérationnelle qu'elle mérite.

PARTIE 1 : CYBERSÉCURITÉ ET SECTEUR DE LA SANTÉ : ETAT DES LIEUX

1.1 DÉFINITION ET CHIFFRES CLÉS

L'ANSSI définit la cybersécurité comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles » (6).

Une cyberattaque est quant à elle « l'atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants » (6).

Les établissements de santé et les fabricants de dispositifs médicaux sont quant à eux définis dans le règlement (UE) 2017/745 relatif aux dispositifs médicaux.

Un établissement de santé étant défini comme « une entité ayant pour mission première de prendre en charge ou de soigner des patients ou d'œuvrer en faveur de la santé publique » (7).

Le fabricant de dispositif médical comme « une personne physique ou morale qui fabrique ou remet à neuf un dispositif ou fait concevoir, fabriquer ou remettre à neuf un dispositif, et commercialise ce dispositif sous son nom ou sous sa marque » (7).

Les chiffres relatifs à la cybersécurité pour le secteur de la santé sont alarmants. La période 2021-2023, marquée par la pandémie COVID-19 ainsi que la pré-invasion de l'Ukraine, a été particulièrement marquée par le nombre de cyberattaques dirigées contre l'Europe.

Entre janvier 2021 et mars 2023, l'Agence de l'Union Européenne pour la Cybersécurité (ENISA) a pris l'initiative d'analyser 215 incidents de cybersécurité signalés publiquement dans des structures du secteur de la santé (hôpitaux, laboratoires, mutuelles, organismes publics ou industries pharmaceutiques) au sein de l'Union européenne (figure 1) (8).

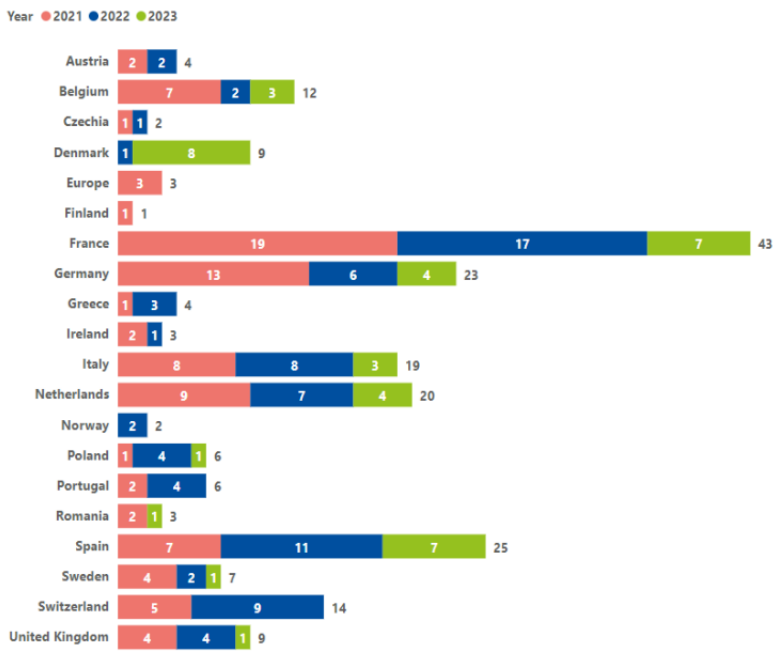


***Figure 1** : Nombre d'incidents pour les années 2021/2022/2023 (8)*

La figure 1 met en avant un nombre d'incidents globalement stable entre 2021 et 2022, avec une légère tendance à la hausse sur le premier trimestre 2023.

La France, avec 43 incidents signalés sur les 215 incidents analysés, se place en tête, devant l'Espagne et l'Allemagne, reflet à la fois de son parc d'établissements et de sa propension à déclarer les incidents (8). Cela représente toutefois en moyenne plus d'un incident grave par mois sur la période étudiée.

Ces chiffres inquiétants ont été confirmés par l'observatoire des signalements de l'Agence Numérique en Santé publié en 2024. En effet, le nombre total d'incidents déclarés (**749 signalements**) a fortement augmenté par rapport à 2023 (**581 signalements**). Le nombre d'incidents ayant un impact sur la prise en charge des patients est en augmentation par rapport à 2023 (de 13%). En effet, **230 signalements** reçus en 2024 indiquent que les établissements ont été contraints de passer en mode dégradé ou d'interrompre la prise en charge des patients soit 31% des signalements reçus(9).

La répartition des incidents entre les différentes organisations est également présentée dans le rapport de l'ENISA :

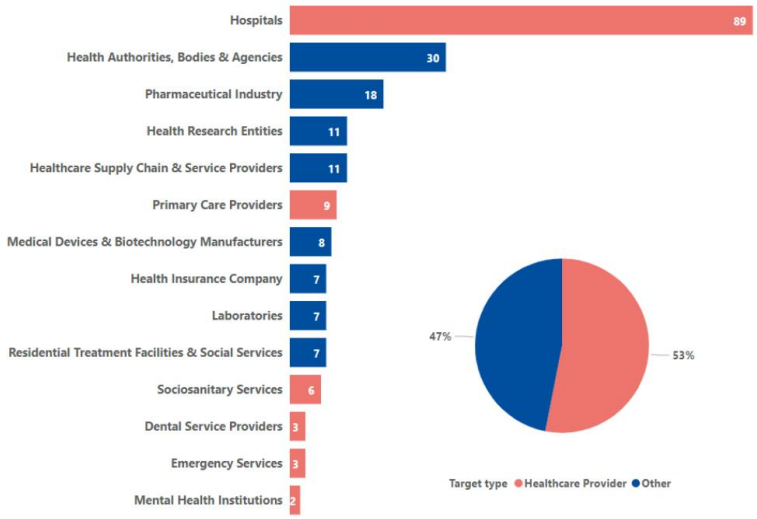


***Figure 2** : Nombre d'incidents par type d'entité* (8)

La figure 2 démontre que les établissements de santé sont particulièrement touchés avec 53% du nombre total d'incidents.

Les hôpitaux européens sont particulièrement impactés avec 89 incidents reportés sur la période et représentent donc la première cible pour les cybercriminels. Les autorités/organismes de santé et les industries pharmaceutiques complètent le podium (8).

La figure 3 expose la nature des menaces, les ransomwares occupants la première place (54%), suivi des menaces liées aux données (46%) et des intrusions (13%) (8):

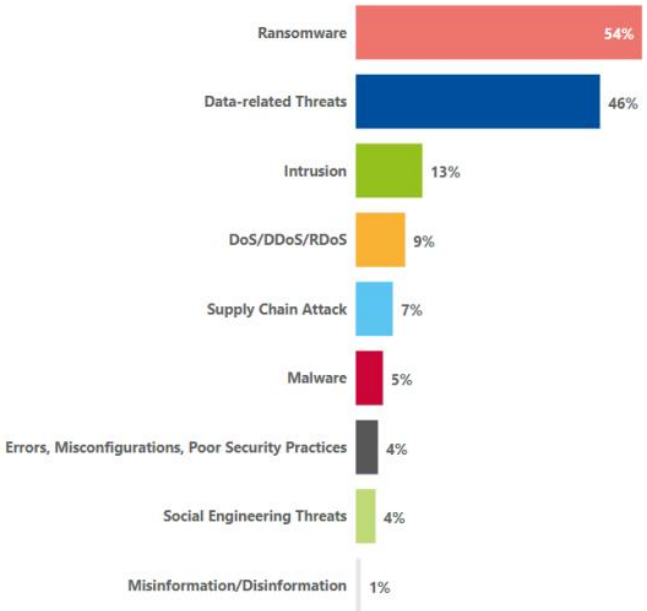


***Figure 3** : Natures des menaces dans le secteur de la santé de janvier 2021 à Mars 2023* (8)

NB : Dans la figure ci-dessus, le cumul des pourcentages atteignant une valeur supérieure à 100% s'explique par le fait qu'un incident peut être classé dans plusieurs catégories de menace.

Les natures des cyberattaques sont hétérogènes et il convient de présenter les principaux types de cyberattaques, des plus courantes aux menaces émergentes, et d'analyser leurs conséquences pour les établissements de santé, les fabricants de dispositifs médicaux, et la prise en charge des patients.

1.2 VUE D'ENSEMBLE DES CYBERATTAQUES ET LEUR CONSÉQUENCES

Les cyberattaques ciblant le secteur de la santé reposent sur des méthodes et des points d'entrée très variés, renforcées par l'essor de l'intelligence artificielle et l'interconnexion croissante des systèmes de soins. Comprendre ces vecteurs et les possibilités de cyberattaques est indispensable pour anticiper et atténuer les menaces.

1.2.1 Vecteurs et surfaces d'attaque

Un vecteur d'attaque est la « méthode ou la combinaison de méthodes que les cybercriminels utilisent pour pénétrer ou s'infiltrer dans le réseau d'une victime » (10).

La surface d'attaque est « le nombre de tous les points possibles pour lequel un utilisateur non autorisé peut accéder à un système et extraire des données ». La surface d'attaque se résume donc par la somme des vecteurs d'attaque (11).

Les deux notions sont liées, le vecteur d'attaque étant la méthode qu'un cybercriminel utilise pour obtenir **un** accès alors que la surface d'attaque est **l'ensemble** de l'espace et des potentiels accès.

Limiter la surface d'attaque facilite grandement la protection : moins de portes ouvertes signifiant moins de risques d'intrusion.

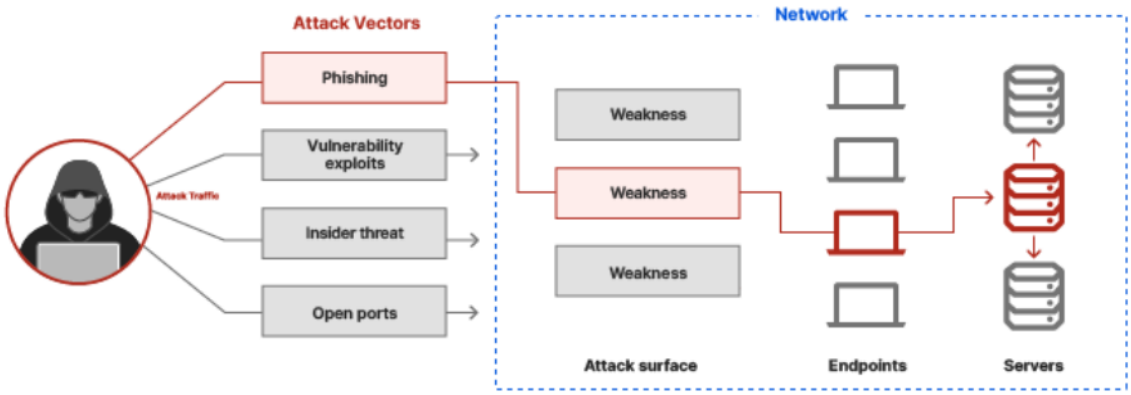


***Figure 4** : Le parcours d'un vecteur d'attaque dans une infrastructure cible (10)*

Les vecteurs d'attaques les plus connus sont les suivants (12) :

- **Phishing** :

  Hameçonnage en français, consiste à voler des informations comme le mot de passe ou le nom d'un utilisateur. Le cybercriminel peut ainsi utiliser ces données pour s'introduire dans un réseau.

  Ce vecteur d'attaque fait partie d'un groupe plus large appelé les attaques par ingénierie sociale qui exploitent une erreur ou le comportement humain dans le but d'accéder à des informations ou à des services.

  Cela peut être par l'envoi de courriels ou messages imitant un interlocuteur connu pour inciter l'utilisateur à communiquer ses identifiants ou à exécuter un logiciel malveillant.

  Il s'agit du vecteur d'attaque le plus connu et le plus couramment utilisé (13).
- **Menace d'initié** :

  Divulgation volontaire ou accidentelle de données sensibles par un employé ou prestataire disposant d'un accès légitime. L'employé peut par exemple être menacé ou soudoyé par le cybercriminel pour qu'il fournisse un accès (12). Des employés malveillants peuvent également agir d'eux-mêmes, par mécontentement envers leur employeur par exemple.
- **Malware** :

  Logiciel malveillant (virus, ver, cheval de Troie, ransomware) conçu pour exécuter un programme non autorisé ayant un impact négatif sur la confidentialité, l'intégrité ou la disponibilité d'un système (13).
- **Pièce jointe au courriel** :

  Fichier infecté transmis par courriel, exécutant un code malveillant à l'ouverture. Les cybercriminels peuvent usurper l'identité d'une agence gouvernementale ou d'un proche afin de mettre en œuvre plus facilement ce type d'attaque (12).
- **Absence de chiffrement** :

  Exploitation de données non chiffrées, interceptées en transit ou accessibles sur des systèmes mal protégés (12).
- **Exploitation de vulnérabilité** :

  Utilisation de failles non corrigées dans des logiciels ou matériels pour obtenir un accès non autorisé (12).
- **Attaque basée sur le navigateur** :

  Injection de code malveillant dans un site ou redirection vers une fausse page, afin de compromettre les comptes ou télécharger un malware (12).

Le vecteur d'attaque représente, d'une certaine façon, la carte de visite du cybercriminel. Il est donc essentiel de connaître les différents vecteurs d'attaque et de se tenir constamment informé (10).

Ces vecteurs peuvent être combinés pour déjouer les dispositifs de sécurité et tromper davantage les utilisateurs. Il importe de distinguer la méthode d'intrusion (vecteur) de l'action malveillante elle-même (cyberattaque).

1.2.2 Cyberattaques répandues

L'ANSSI distingue quatre grandes catégories de menaces pesant sur les systèmes de santé. Les attaques à finalité lucrative constituent la plus fréquente et revêtent plusieurs formes, détaillées ci-après (1):

1.2.2.1 Les menaces à finalité lucrative

Les attaques motivées par le gain financier sont particulièrement utilisées contre les établissements de santé et les fabricants de dispositifs médicaux.

- **Ransomware** :
  Ou rançongiciels en français, ces logiciels malveillants chiffrent les données ou bloquent l'accès aux services, paralysant souvent des mois de fonctionnement avant de réclamer une rançon. Les cybercriminels collectent parfois les données à l'insu de la victime pendant plusieurs semaines, puis combinent chiffrement, extorsion et menace de publication sur le darknet (internet clandestin) si la rançon n'est pas versée (13).
  Cette attaque se caractérise généralement par l'indisponibilité de certaines données ou services et un ralentissement voire un arrêt des activités (1).
- **Exfiltration de données à des fins de revente** :
  Les données médicales, personnelles et de paiement sont captées puis vendues sur des forums ou sur le darknet (internet clandestin). Leur valeur réside dans le potentiel de revente direct, l'usurpation d'identité ou le lancement d'attaques ultérieures contre les patients et les organisations concernées (1).
- **Compromissions à des fins de fraude** :
  Une compromission de données est « un incident de sécurité durant lequel des informations appartenant à une entité sont dérobées, reproduites, consultées ou divulguées illégalement par une personne ou un groupe non autorisé » (14).
  La compromission permet donc par exemple de monter des fraudes (ouverture de comptes bancaires, demandes de prêts, obtention de pièces d'identité).

1.2.2.2 Les menaces à finalité d'espionnage

Les attaques à finalité d'espionnage visent principalement le vol de données sensibles (personnelles, médicales) et d'informations de recherche (brevets, protocoles cliniques).

Elles sont souvent orchestrées par des groupes sponsorisés par des États ou des organisations disposant de moyens financiers et techniques importants. L'objectif est de compenser des retards en R&D, de réduire le coût des programmes de recherche pharmaceutique ou d'obtenir un avantage concurrentiel dans le développement de nouveaux traitements (1).

Les opérations d'espionnage ont considérablement augmenté durant la pandémie de Covid-19. Un exemple emblématique est l'arrestation à Milan, en juillet 2025, de Xu Zewei, accusé par le FBI d'avoir participé à des cyberattaques visant les travaux de recherche sur les vaccins anti-Covid menés à l'Université du Texas (15).

Ce type d'incident illustre le risque que fait peser l'espionnage sur l'innovation médicale, la souveraineté sanitaire et souligne l'impératif d'installer une surveillance renforcée des accès à la R&D.

1.2.2.3 Les menaces à finalité de déstabilisation

Les menaces à finalité de déstabilisation sont le plus souvent portées par des groupes hacktivistes, contraction de « hacker » et « activiste », ce sont des militants numériques dont l'objectif est de déstabiliser ses cibles (16). Le secteur de la santé, de par la criticité de ses services, constitue une cible privilégiée : dégrader son fonctionnement revient à ébranler la population et, par ricochet, l'État.

Ces attaques de déstabilisation surviennent souvent à l'occasion d'événements politiques ou sociaux majeurs (conflits, manifestations, publications de rapports sensibles) (1).

Plusieurs types d'attaques sont employés à cette fin :

- **Attaques par déni de service distribué (ou attaques DDoS)** :
  Ces campagnes visent à saturer les ressources réseau ou serveurs d'un service critique (site web, centre d'appels, application interne) en inondant la cible de requêtes simultanées (17). La conséquence est l'indisponibilité des services nécessitant ces ressources pendant parfois plusieurs heures.

Par exemple, l'envoi massif de faux appels aux services d'urgences peut bloquer l'ensemble du standard, empêchant les véritables appels de secours d'aboutir.

- **Exfiltration de données à des fins de divulgation publique** :
  L'objectif ici n'est plus la revente des données, mais leur publication pour choquer l'opinion ou porter atteinte à la réputation d'une institution (1).
  Des informations sensibles (dossiers de personnalités, rapports internes sur la gestion d'une crise sanitaire) sont diffusées sur des sites publics ou des forums du darknet. L'Agence mondiale antidopage a, par exemple, vu fuiter les dossiers médicaux de sportifs de haut niveau – parmi lesquels Chris Froome et Simone Biles – dans une opération visant à décrédibiliser l'institution (18).

1.2.2.4 Le sabotage

Les attaques utilisées à des fins de sabotage regroupent certaines mentionnées ci-dessus. Ici, c'est l'objectif qui diffère étant donné que les attaques à finalité de sabotage visent exclusivement à priver un système d'information ou un équipement médical de toute fonctionnalité, sans objectif financier ni divulgation de données (1).

Ces attaques peuvent provoquer pannes généralisées, retards de soins et erreurs médicales, avec un impact direct sur la sécurité des patients.

Toutes les cyberattaques résumées ci-dessus, bien qu'elles soient les plus courantes, ne représentent pas la totalité de l'arsenal dont disposent les cybercriminels. Le secteur de la santé doit en effet se préparer aux nouvelles menaces qui émergent avec le développement de l'Intelligence Artificielle.

1.2.3 Cyberattaques émergentes

Aujourd'hui, notre environnement de santé s'appuie de plus en plus sur le cloud et du réseau de dispositifs médicaux connectés générant chaque seconde d'importants volumes de données médicales et administratives (13). Parallèlement, l'apprentissage automatique et l'Intelligence Artificielle (IA) se diffusent dans nos outils de diagnostic, de suivi des patients et de gestion des flux.

L'adoption de ces technologies ouvre la porte à de nouvelles vulnérabilités. L'IA ne se limite pas à renforcer nos défenses ; elle offre également aux cybercriminels des capacités d'automatisation et d'adaptation de leurs attaques.

L'utilisation de deepfakes est un exemple des nouvelles possibilités qu'offre l'IA dans la manipulation des victimes. Le mécanisme de deepfake dans le cadre de la santé

fait référence à l'utilisation de l'Intelligence Artificielle pour créer de fausses images, enregistrements audio ou des clips vidéos particulièrement réalistes (19).

Dans un contexte hospitalier, un cybercriminel pourrait :

- Générer une vidéo d'un directeur d'hôpital ordonnant l'arrêt immédiat des interventions chirurgicales en cours, provoquant la panique et la suspension des blocs opératoires.
- Cloner la voix d'un praticien pour téléphoner à un service de soins à domicile et modifier les prescriptions médicamenteuses d'un patient, avec un risque grave pour sa sécurité.

Cette technique s'attaque au socle de la relation de confiance patient-soignant : le moindre doute sur l'authenticité des communications peut compromettre la prise en charge et ralentir le parcours de soins.

Fort de cet inventaire des vecteurs, familles de menaces et scénarios émergents, il est désormais indispensable d'évaluer les impacts concrets de ces cyberattaques.

1.2.4 Conséquences des cyberattaques pour les acteurs de la santé

Les hôpitaux et, plus largement, les établissements de santé constituent la cible privilégiée des cybercriminels, comme le montre le chapitre 1.1 (8).

Cette situation tient d'une part à la sensibilité et à la valeur des données médicales qu'ils manipulent (cf. chap. 1.3.2), et d'autre part à la forte visibilité de leur activité : toute interruption de service y est immédiatement médiatisée, alors que des incidents similaires peuvent passer inaperçus dans d'autres secteurs.

Ainsi, bien que les conséquences présentées dans ce chapitre soient particulièrement ciblées vers les établissements de santé, elles sont tout autant applicables aux fabricants de dispositifs médicaux ou toute autre entité disposant d'un système d'information vulnérable.

1.2.4.1 Conséquences opérationnelles

Les établissements de santé prennent en charge de la vie des patients 24h/24 et 7j/7 ; ils ne peuvent donc ni interrompre les soins, ni refuser des patients. Leurs systèmes d'information et leurs réseaux informatiques doivent donc être constamment fonctionnels.

Dans le cas contraire, la perturbation des services de santé amène à des situations où les opérations doivent être annulées, où l'admission des patients est plus lente et

moins efficace et où le réacheminement des patients vers d'autres hôpitaux est nécessaire (6). L'interruption des services et la perturbation des soins dans les établissements de santés peuvent se traduire également par un accès aux dossiers médicaux plus difficile, un dysfonctionnement des équipements ou encore la perturbation des rendez-vous et des plannings (6).

L'étude de l'Institut Ponemon publiée en 2023 sur l'impact des ransomwares sur la sécurité des patients démontre que ces attaques entraînent une augmentation significative des complications liées aux procédures médicales (20).

Il a été estimé que pour 53% des personnes interrogées dans des organisations ayant subi une attaque par ransomware, celles-ci ont entraîné une perturbation des soins aux patients, l'événement le plus néfaste étant l'augmentation du nombre de patients transférés ou détournés vers un autre établissement (20).

Une enquête complémentaire auprès de 653 professionnels de l'informatique et de la sécurité révèle une hausse d'environ 28 % du taux de mortalité dans les établissements touchés par un rançongiciel (21).

1.2.4.2 Conséquences financières directes

Les conséquences financières directes peuvent être multiples, comprenant entre autres (21) :

- Les pertes de revenus liées aux facteurs suivants :
    - Indisponibilité du système : interruption des flux de soins et de facturation par exemple.
    - Inactivité des utilisateurs : baisse de productivité liée aux temps d'arrêt ou aux lenteurs des applications.
    - Durée de remise en état : période pendant laquelle l'activité reste dégradée, avant retour à un fonctionnement normal.
- Les coûts de réparation en lien avec l'endommagement ou le vol des actifs et de l'infrastructure informatiques avec le remplacement ou restauration des équipements (serveurs, postes de travail, dispositifs connectés) endommagés par exemple.
- Les activités de remédiation et d'assistance technique, y compris les enquêtes médico-légales, les activités de réponse aux incidents, le service d'assistance et la fourniture de services aux patients.
- Paiement éventuel de rançon avec le montant versé aux attaquants pour obtenir la clé de déchiffrement ou la remise en service des systèmes.

Aux Etats-Unis, il a été estimé que les atteintes à la sécurité des données dans les hôpitaux peuvent coûter jusqu'à 7 millions de dollars, y compris les amendes, les litiges et l'atteinte à la réputation. L'intervention et le nettoyage peuvent à eux seuls coûter des centaines de milliers de dollars (22).

Selon une étude du Ponemon Institute, c'est la perte de chiffre d'affaires liée à l'interruption des opérations courantes qui pèse le plus lourd, avec un coût moyen estimé à 1,3 million de dollars par incident pour les établissements de santé américains (21).

1.2.4.3 Conséquences réputationnelles

Outre les impacts directs sur les opérations et les finances, une cyberattaque porte un préjudice durable à l'image des établissements de santé et des fabricants de dispositifs médicaux. Cette altération de réputation se manifeste à plusieurs niveaux (23) :

- **Perte de confiance** :
  Une cyberattaque réussie est le reflet de l'incapacité à protéger les données des patients. Elle entraîne donc une perte de confiance significative de la part des patients qui peut se traduire par une méfiance envers le système de santé nuisant à l'adhésion aux parcours de soins et aux programmes de prévention (23).
- **Couverture médiatique négative** :
  Les incidents critiques, notamment lorsqu'ils impliquent des grands hôpitaux ou des fabricants renommés, font l'objet d'une large diffusion dans les médias. Cette exposition renforce la défiance des patients et des partenaires, et suscite des interrogations sur la gouvernance et la résilience de l'organisation (23).
- **Actions en bourse et pertes financières associées** :
  Pour les entreprises cotées (laboratoires, fabricants de dispositifs), l'annonce d'une violation de données ou d'une attaque par rançongiciel entraîne souvent une chute spectaculaire du cours de bourse (23). Les investisseurs peuvent redouter d'autres incidents et exiger des stratégies de cybersécurité renforcées avant de rétablir leur confiance.
- **Perte d'opportunités commerciales** :
  L'érosion de la crédibilité entraîne parfois la renonciation de partenaires potentiels : hôpitaux, laboratoires de recherche ou organismes de financement préfèrent collaborer avec des acteurs perçus comme plus sûrs, ce qui freine le développement de nouveaux projets et l'accès à des marchés (23).

- **Moral des équipes et attractivité** :

  Le personnel, déjà soumis à une forte pression, ressent un sentiment d'insécurité et de frustration lorsqu'une attaque révèle des lacunes dans les systèmes de protection. En outre, la publicité négative entourant une cyberattaque peut rendre difficile l'attraction des meilleurs talents, car les candidats potentiels peuvent hésiter à rejoindre une entreprise dont la réputation est ternie (23).

- **Actions en justice et sanctions :**

  Les impacts juridiques et réglementaires sont également à prendre en compte et notamment la responsabilité associée à l'absence de mesures de cybersécurité adéquates en cas de violation de données. Par exemple, si un patient subit un préjudice qui aurait pu être évité si l'établissement de santé ou le fabricant n'avaient pas négligé sa sécurité informatique, ce patient ne manquerait pas d'intenter de lourdes actions en justice (23).

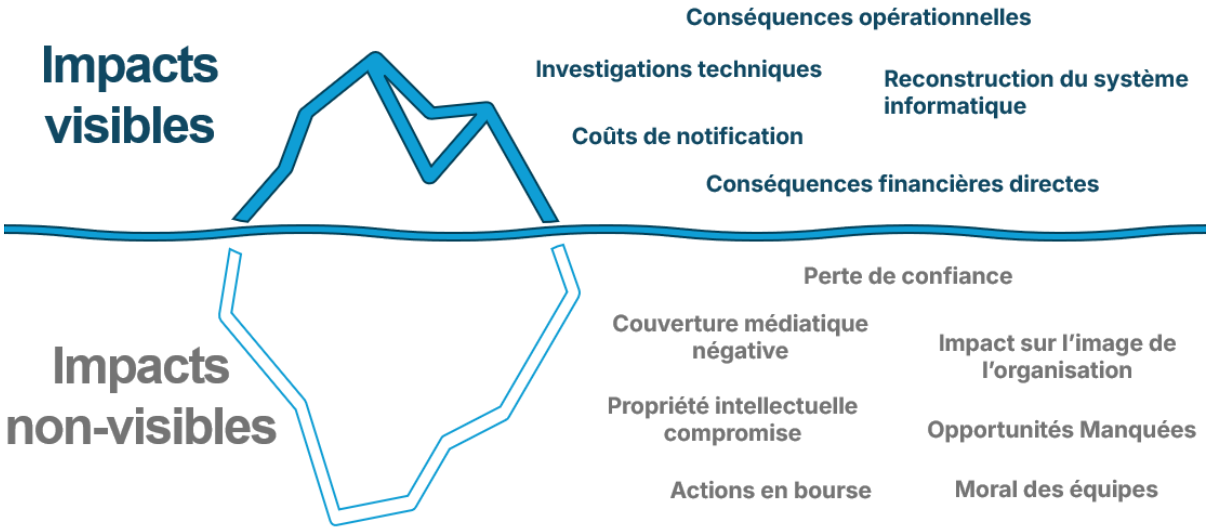


***Figure 5** : Cyberattaque : l'iceberg des impacts*

1.3 CYBERSÉCURITÉ ET ÉTABLISSEMENTS DE SANTÉ

1.3.1 Transformation numérique des systèmes médicaux : coordination des soins et enjeux de cybersécurité

Les données de santé constituent un pilier du parcours de soins. Toute vulnérabilité affectant cette ressource menace non seulement les systèmes d'information des établissements, mais aussi la qualité et la sécurité des soins, et par conséquent la santé des patients.

1.3.1.1 Numérisation des données de santé : opportunités cliniques et nouveaux enjeux de sécurité

La numérisation est le processus de conversion d'informations d'un format analogique (comme un document papier, une image, une bande sonore, etc.) à un format numérique, c'est-à-dire, en données représentées par des nombres que les ordinateurs peuvent traiter (24).

A l'ère du numérique, ce processus a permis (25):

- Une amélioration de la prise en charge et de la coordination entre professionnels.
- Une rationalisation des flux administratifs et opérationnels.
- Un accès facilité aux données pour la recherche et l'innovation thérapeutique.

La pandémie de COVID-19 a accéléré ce mouvement vers la dématérialisation, avec un recours massif à la télésanté et aux outils de suivi à distance pour maintenir la continuité des soins en situation de crise (26).

En effet, la numérisation des données peut être utilisée de manière responsable et innovante comme illustré dans deux exemples très concrets mis en place en France :

Le Dossier Médical Partagé (27) :	DMP DOSSIER MÉDICAL PARTAGÉ
Objectif : mutualiser et centraliser les informations médicales pour l'ensemble des acteurs de santé, en ville comme à l'hôpital. Fonctions : accès instantané aux antécédents, résultats d'examens, traitements en cours, directives anticipées. Bénéfices : suivi optimal des maladies chroniques, réduction des prescriptions redondantes, prévention des interactions médicamenteuses.	
L'application Covidom (28) :	covidom
Public : patients à domicile atteints de forme légère à modérée de COVID-19.	

Fonctions : questionnaire quotidien sur les symptômes, alertant un centre de suivi en cas de dégradation de l'état de santé.
Bénéfices : orientation rapide vers un rendez-vous médical ou vers un service d'urgence, collecte de données agrégées pour la recherche universitaire avec consentement des patients.

Les dossiers de santé numériques renferment aujourd'hui des informations particulièrement sensibles (29) :

- **Informations médicales et administratives** :
  - Identité : nom, prénom, date de naissance.
  - Antécédents médicaux, résultats de laboratoire, suivi psychiatrique.
- **Informations financières** :
  - Numéros de carte bancaire et de compte.
- **Informations d'identification personnelle** :
  - Numéro de sécurité sociale, adresse e-mail, numéro de téléphone.
- **Propriété intellectuelle** :
  - Données de recherche, protocoles cliniques, innovations technologiques.

Face à l'importance et à la sensibilité de ces données, la question de leur usage, de leur protection et des risques inhérents devient cruciale.

Un article du Lancet publié en 2021 soulignait cette défiance vis-à-vis de la « santé digitale » lorsque le National Health Service (NHS) a demandé aux médecins anglais de regrouper et de transmettre les antécédents médicaux de leurs patients vers le système numérique centralisé. Les professionnels pointaient alors (26) :

- L'absence de véritable anonymisation des données.
- Le flou sur les modalités d'utilisation et de partage.
- Le manque de précisions concernant les autorisations d'accès et le consentement des patients.

La protection des informations patients ne date pas de l'ère numérique, elle existait déjà pour les archives papier. Cependant, le passage au numérique redéfinit les menaces et étend considérablement la surface d'attaque (4) :

- **Accéder à distance :**

Un pirate peut cibler un hôpital situé à des milliers de kilomètres, compliquant l'identification et la poursuite judiciaire.

- **Accéder et voler les données de façon « invisible » :**
  Contrairement au vol physique de dossiers, l'extraction de données peut rester indétectable pendant des semaines, voire des mois.
- **Centralisation des dossiers** :
  Le Dossier Médical Partagé regroupe en un point unique des informations jadis éparpillées, offrant une « mine » complète en cas de compromission.
- **Accéder à une quantité de données beaucoup plus importante** :
  Là où la disparition ou le vol d'un carton papier affectait quelques dizaines ou centaines de patients, une seule intrusion informatique peut exposer plusieurs centaines de milliers de dossiers à la fois.

La centralisation et la diversité des menaces soulignent une réalité incontournable : la sécurité des données de santé ne se joue plus uniquement au niveau de chaque système pris isolément. La multiplication des échanges entre hôpitaux, cabinets libéraux, laboratoires, fabricants de dispositifs médicaux et plateformes cloud complexifie encore la protection de ces informations stratégiques.

1.3.1.2 L'interconnexion des systèmes médicaux : entre coordination des soins et exposition aux risques

L'interconnexion est définie par la CNIL comme « la mise en relation automatisée d'informations provenant de fichiers ou de traitements qui étaient au préalable distincts » (30).

Autrefois centrés sur la gestion administrative et financière, les systèmes d'information hospitaliers reposaient sur des dossiers papier dont l'isolement limitait considérablement les risques de compromission. Avec la montée en puissance de la numérisation, ces silos se sont progressivement connectés (31) :

- Réseaux locaux et services cloud : partage des données patients entre services internes et externes.
- Internet des objets médicaux (IoMT) : réseau de dispositifs médicaux connectés à Internet qui collectent et transmettent des données de santé. Ils incluent les wearables, les implants, les appareils de diagnostic et les logiciels qui permettent le suivi à distance des patients, l'amélioration des résultats, et la réduction des coûts.

- Dossiers médicaux électroniques et télémédecine : échanges sécurisés entre établissements et professionnels libéraux.
- Intelligence artificielle : exploitation d'ensembles de données pour la reconnaissance d'images, la prédiction de risques ou l'aide à la décision.

L'objectif de cette interconnexion est double : optimiser la coordination des soins et accroître l'efficacité opérationnelle. Par exemple, un laboratoire peut envoyer directement un résultat sanguin à l'hôpital, tandis qu'un fabricant de dispositifs assure la maintenance à distance de ses équipements via un accès protégé au système d'information de l'établissement (31).

Cependant, cette ouverture vers l'extérieur augmente la surface d'attaque et fait émerger de nouvelles vulnérabilités. Si elle améliore la qualité des soins, elle expose aussi les hôpitaux à des cybermenaces susceptibles de divulguer des données sensibles, de perturber l'activité clinique, voire de mettre en danger la sécurité des patients (32).

Les établissements de santé, du fait de la sensibilité et la valeur de leurs données, sont particulièrement prisés par les attaquants. Il est donc pertinent de s'interroger sur les facteurs qui en font une cible privilégiée.

1.3.2 Des établissements de santé particulièrement ciblés

Il est contre-intuitif d'imaginer des attaques visant des hôpitaux, perçus comme des sanctuaires protégés. Le droit international humanitaire, et notamment les Conventions de Genève, stipule que « Les hôpitaux civils organisés pour donner des soins aux blessés, aux malades, aux infirmes et aux femmes en couches ne pourront, en aucune circonstance, être l'objet d'attaques; ils seront, en tout temps, respectés et protégés » (33).

Aucun établissement de santé n'a été construit dans l'objectif initial d'assurer la cybersécurité, le soin des patients ayant toujours été la priorité. Pourtant de nombreux facteurs font qu'ils représentent une cible pour les cybercriminels.

1.3.2.1 Les données de santé au cœur de l'enjeu

Plusieurs caractéristiques confèrent aux données de santé une attractivité particulière :

- **La valeur financière des données de santé** :

  La principale motivation des cybercriminels quand il s'agit d'exploiter des vulnérabilités de systèmes informatiques est la motivation financière (8). Les

dossiers médicaux se vendent jusqu'à dix fois plus cher que les données bancaires sur le darknet, et le coût de la gestion d'une violation dans le secteur de la santé est environ trois fois supérieur à la moyenne des autres industries (34).

Au-delà du vol pur, l'accès à ces données facilite l'usurpation d'identité, la fraude, l'extorsion et le chantage (8). Confrontés à l'urgence de rétablir leurs systèmes, les hôpitaux sont souvent prêts à verser des rançons élevées pour reprendre l'accès à leurs services cliniques (35).

- **Le caractère immuable des données de santé** :

Contrairement aux données financières, qu'on peut simplement réinitialiser (nouvelle carte, nouveau numéro…), les informations médicales (antécédents, données personnelles) sont définitives. Leur compromission constitue donc une menace irréversible pour la vie privée des patients (36).

- **Le nombre d'employés ayant accès aux données de santé** :

Un grand nombre de professionnels (médecins, infirmiers, pharmaciens, personnel administratif) nécessite un accès régulier aux dossiers. Chaque employé représente un point d'entrée potentiel que les attaquants peuvent exploiter (36).

- **La quantité de données stockées** :

Les données sont stockées en grande quantité et pendant une période très importante dans les établissements de santé. Par exemple, l'Entrepôt de Données de Santé (EDS) de l'AP-HP (Assistance Publique – Hôpitaux de Paris) recense les données de 19 millions de patients distincts, centralisant ainsi un vivier considérable pour les cybercriminels (37).

La richesse et la sensibilité des données de santé expliquent en grande partie l'attrait des cybercriminels. Mais ce n'est pas le seul facteur : c'est aussi la complexité même des systèmes d'information hospitaliers qui multiplie les failles exploitables.

1.3.2.2 Des systèmes d'information particulièrement complexes

Un rapport de la Cour des Comptes publié en 2024 souligne la fragilité et la complexité croissante des systèmes d'information des établissements de santé. Certains grands centres hospitaliers peuvent aujourd'hui compter jusqu'à 1 000 applications métiers distinctes, un nombre sans équivalent dans les autres secteurs d'activité (31).

La figure 6 ci-dessous illustre la diversité et l'étendue des solutions logicielles déployées au sein d'un centre hospitalier (38).

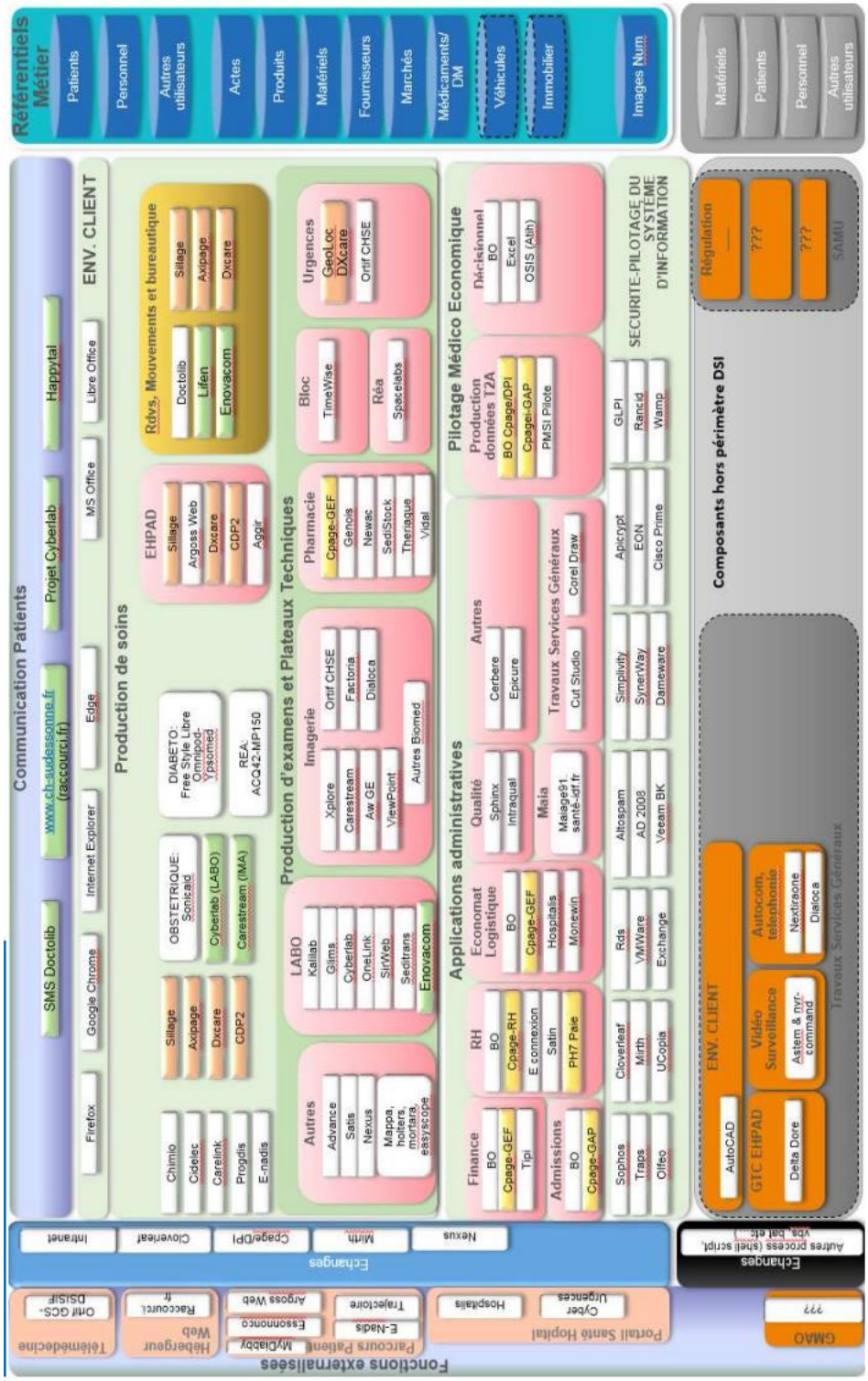


***Figure 6** : Cartographie simplifiée des applications au Centre Hospitalier Sud Essonne (37)*

Les caractéristiques qui font la singularité — et la vulnérabilité — des SI hospitaliers se déclinent ainsi :

- **La diversité des acteurs** (38):
  - Services cliniques (imagerie, bloc opératoire, soins intensifs…).
  - Pôles supports (pharmacie, finances, ressources humaines…).

    - Activités non cliniques (recherche, formation, comptabilité…). Chaque nouvelle spécialité introduit ses propres applications et configurations, augmentant la surface d'attaque.
- **Le nombre d'application** (38):
    - Plus de 50 illustrées sur la seule figure 6.
    - Collecte, stockage, analyse et partage des données. Chacune d'elles représente un vecteur potentiel de vulnérabilité.

À cette complexité s'ajoute l'obsolescence des systèmes d'exploitation et le manque de mises à jour régulières. Par exemple, en 2016, 9 établissements sur 10 utilisaient encore Windows XP, dont le support officiel avait cessé en 2014 (39).

1.3.2.3 Des dispositifs médicaux connectés toujours plus nombreux

L'essor des dispositifs médicaux connectés améliore la prise en charge des patients, mais multiplie également les points d'entrée pour les cybercriminels. Aux États-Unis, un hôpital compte en moyenne entre 10 et 15 dispositifs connectés par lit, soit près de 15 000 appareils pour un établissement de 1 000 lits (40).

Ces dispositifs sont souvent accessibles à tous (prescription, achat en ligne), ce qui facilite leur étude et la découverte de vulnérabilités potentielles. Une faille dans un seul appareil peut suffire à compromettre l'ensemble du réseau interne et exposer des données sensibles (41).

La mise à jour régulière des dispositifs médicaux est essentielle pour corriger les failles de sécurité. Or, les équipements sont souvent en service 24/7, et l'application de correctifs les rend temporairement indisponibles, un obstacle majeur à la maintenance sécuritaire (40). De plus, de nombreux hôpitaux ne disposent pas d'un inventaire exhaustif et à jour de tous les dispositifs connectés, compliquant la mise en place de mesures de défense adéquates (40).

Par ailleurs, le recours aux appareils personnels par le personnel soignant (smartphones, tablettes) pour accéder à distance aux données patients augmente les risques, car ces terminaux ne sont pas toujours équipés de solutions de détection des dispositifs compromis (35).

Il est compréhensible que les soignants privilégient la continuité des soins à la cybersécurité. Toutefois, une faille exploitée peut avoir des conséquences directes sur

la qualité et la sécurité des soins, pouvant, dans les situations les plus critiques, mettre la vie des patients en danger.

1.3.3 Etudes de cas

1.3.3.1 Le cas du centre hospitalier Sud-Francilien

Le 20 août 2022, le Centre Hospitalier Sud-Francilien a été victime d'une attaque par rançongiciel qui a paralysé, en une seule nuit, l'ensemble de ses logiciels métiers, systèmes de stockage, imagerie et admission des patients. Cette intrusion a également affecté les services de messagerie, de pharmacie et de comptabilité, déstabilisant l'organisation clinique et administrative (42).

Confronté à la gravité de la situation, l'hôpital a déclenché son plan blanc, malgré l'indisponibilité de son système de rappel informatisé. Des procédures manuelles ont été mises en place pour gérer les paiements fournisseurs et les approvisionnements, notamment par l'émission d'ordres de paiement papier (42).

Peu après l'attaque, le groupe de hackers russophones LockBit 3.0 a menacé de publier les données de 1,5 million de patients et membres du personnel, exigeant une rançon de 10 millions d'euros. Refusant de céder à la demande, l'établissement a vu les données diffusées le 25 septembre 2022 (42). Les informations publiées comprenaient :

- Numéros de sécurité sociale et données administratives.
- Comptes rendus d'examens (anatomopathologie, radiologie, laboratoires).

La gestion de crise et la remise en état des systèmes ont coûté près de 9 millions d'euros, dont 1 million dédié à l'envoi de notifications aux patients et au personnel concernés (31).

1.3.3.2 Le cas du centre de psychothérapie Vastaamo

En 2020, le centre de psychothérapie finlandais Vastaamo a subi une compromission massive de ses dossiers médicaux électroniques, touchant des milliers de patients et révélant des failles majeures dans la protection des données de santé mentale (43).

- **Intrusion et extorsion** :
  Un cybercriminel a accédé aux dossiers sensibles du service de psychothérapie, puis a commencé par faire chanter l'établissement pour obtenir une rançon. Par la suite, il a directement menacé les patients, leur réclamant 200 € sous peine de publication de leurs échanges confidentiels avec les thérapeutes (43).

- **Impacts humains et psychologiques** :
  La menace de divulgation a provoqué une détresse aiguë chez de nombreux patients, fragilisant leur santé mentale et celle de leurs proches. À ce jour, un suicide a été directement attribué à la fuite d'un de ces dossiers de psychothérapie (43).
- **Manquements dans la détection et la notification** :
  Il ressort qu'au moins deux brèches antérieures, survenues en 2018 et 2019, n'ont pas été signalées. Ce défaut de vigilance et de transparence a aggravé l'étendue du préjudice (43).
- **Sanctions et conséquences financières** :

Le non-respect des obligations de notification au titre du Règlement Général sur la Protection des Données (RGPD) a conduit à une amende administrative de 608'000 € pour négligence et dissimulation des incidents (44).

- **Effondrement de la structure** :
  Accablé par les indemnisations judiciaires, les sanctions réglementaires et la perte de confiance des patients, le centre Vastaamo a fait faillite en 2021 (44).

Cet exemple souligne la criticité de mettre en place, dès la conception des services, des mesures robustes de cybersécurité et de gestion des incidents, en particulier dans les secteurs où la confidentialité est fondamentale.

1.4 CYBERSÉCURITÉ ET FABRICANTS DE DISPOSITIFS MÉDICAUX

1.4.1 L'environnement des dispositifs médicaux

Le nombre de dispositifs médicaux n'a cessé de croître depuis les dernières années. En 2015, MedTech Europe (Association professionnelle européenne des industries des technologies médicales) estimait à plus de 500 000 le nombre de catégories de dispositifs médicaux commercialisés, contre environ 20 000 molécules pharmaceutiques (45).

Les dispositifs médicaux couvrent un large spectre, des articles de consommation à faible risque (lunettes, pansements, seringues) aux équipements connectés.

Dans le cadre de cette thèse, l'attention sera principalement portée sur les dispositifs médicaux **connectés**, c'est-à-dire ceux intégrés à des réseaux de communication permettant l'échange de données en temps réel. Cette approche exclut volontairement les dispositifs **numériques non connectés**, qui, bien qu'ils puissent embarquer des

technologies informatiques (comme les logiciels embarqués ou les interfaces numériques), ne présentent pas les mêmes enjeux en matière de cybersécurité.

Les dispositifs médicaux connectés font partie de l'Internet des Objets Médicaux (IoMT), un réseau de dispositifs médicaux connectés à Internet qui collectent et transmettent des données de santé.

Ces dispositifs peuvent être :

- Des objets de suivi basiques, tels que les trackers d'activité.
- Des systèmes complexes, comme les dossiers médicaux électroniques, les implants cardiaques et les pompes à insuline.
- Des plateformes de surveillance à distance, intégrées à la télémédecine pour le suivi continu des patients chroniques (46).

L'essor des applications mobiles et du haut débit a démocratisé l'accès à ces technologies : les patients peuvent désormais gérer leur traitement et communiquer leurs données de santé en temps réel, sans se déplacer (47).

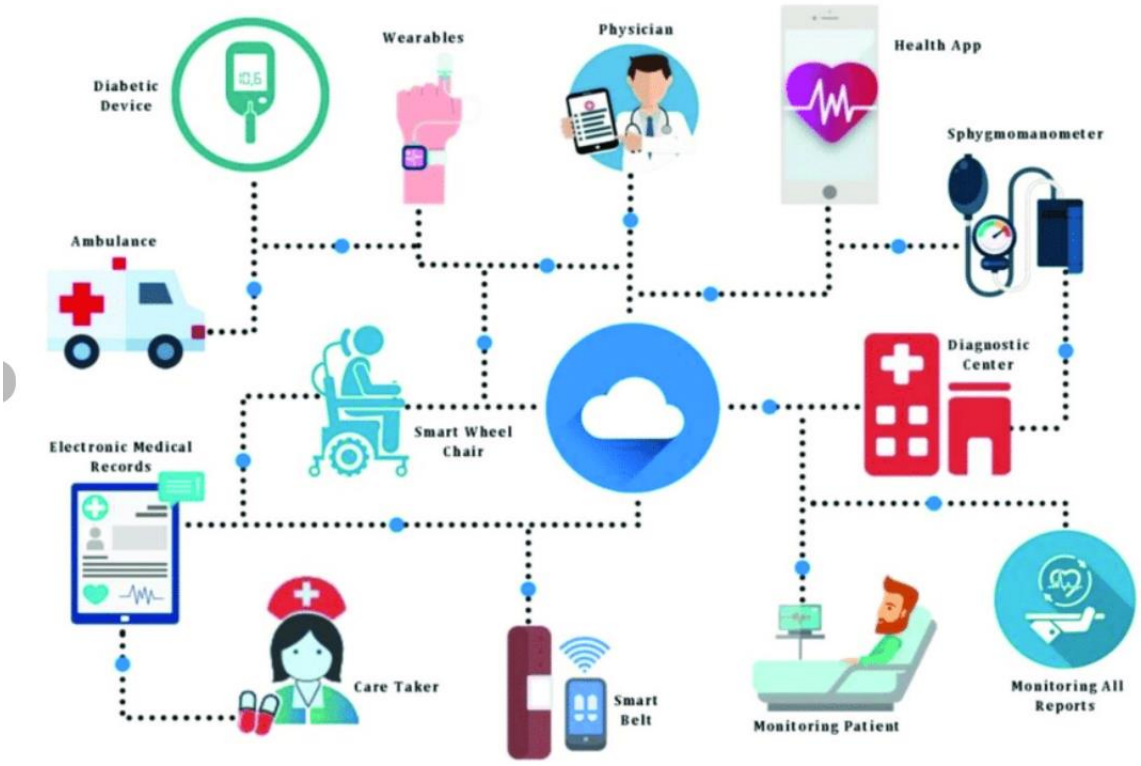


***Figure 7** : Environnement des dispositifs médicaux connectés*

Les dispositifs médicaux connectés offrent de nombreux bénéfices (47) :

- Amélioration de l'efficacité et réduction des erreurs médicamenteuses.
- Automatisation de la surveillance et ajustements à distance des traitements.

- Diminution des coûts par la prévention et la gestion proactive des pathologies chroniques.

Pourtant, leur intégration aux systèmes d'information cliniques ouvre de nouvelles portes aux cyberattaques. La disponibilité, l'intégrité et la confidentialité des données de santé sont vitales et une intrusion peut altérer les décisions thérapeutiques ou corrompre le fonctionnement des appareils (48).

Des soins retardés ou un diagnostic erroné dus à un scanner défectueux peuvent facilement entraîner une perte des fonctions motrices, des lésions cérébrales, voire la mort (48).

Par exemple, une salle d'urgence dépend de la fiabilité d'un scanner pour diagnostiquer un accident vasculaire cérébral. Un dispositif compromis ou indisponible peut retarder la prise en charge, entraînant des séquelles neurologiques irréversibles, voire le décès.

La montée en puissance des dispositifs médicaux connectés, si elle révolutionne la prise en charge des patients, ouvre également la porte à des vulnérabilités critiques.

1.4.2 Des dispositifs médicaux vulnérables

Le problème de la vulnérabilité de la cybersécurité associée aux dispositifs médicaux est constitué de facteurs multiples :

1.4.2.1 Vulnérabilités des dispositifs médicaux connectés : enjeux de sécurité et risques cliniques

La migration des dispositifs médicaux, autrefois isolés, vers des objets connectés optimise le suivi des patients et personnalise les protocoles de traitement. Cependant, cette transition introduit de nouvelles failles (49) :

- La plupart des dispositifs IoMT manquent de mécanismes de sécurité robustes (authentification, chiffrement), ce qui les rend particulièrement sensibles aux intrusions.
- La prolifération de ces équipements élargit la surface d'attaque, compliquant la gouvernance et la supervision des mises à jour.
- Une brèche dans un appareil peut compromettre l'intégralité du réseau hospitalier, menaçant non seulement les données mais la sécurité même des patients.

Ces vulnérabilités affectent la disponibilité des dispositifs et l'intégrité des données cliniques. Bien que des failles aient toujours existé au sein des systèmes médicaux, leur exposition à un écosystème de menaces globalisé justifie l'augmentation du niveau de risque (50).

Des incidents réels démontrent que la compromission de dispositifs implantables n'est plus de la science-fiction. Des pompes à insuline et stimulateurs cardiaques ont déjà été détournés, illustrant la criticité de ces enjeux (50).

Une étude de deux ans menée dans un établissement américain a mis en évidence les failles suivantes (51):

- Pompes à perfusion manipulables à distance pour ajuster arbitrairement le dosage administré.
- Défibrillateurs implantables Bluetooth pouvant être détourner pour envoyer des chocs inappropriés ou bloquer une thérapie essentielle.
- Accès non autorisé aux radiographies, compromettant la confidentialité des examens.
- Modification des paramètres de stockage des réfrigérateurs de sang et de médicaments.
- Altération des dossiers médicaux numériques, induisant des erreurs de diagnostic et de prescription.
- Mise hors service de dispositifs critiques, paralysant des unités entières.
- Failles dans les services web intégrés, dues à des communications non authentifiées et non chiffrées, exploitables à distance depuis n'importe où dans le monde.

La mise en exergue des vulnérabilités des objets connectés révèle un défi tout aussi crucial : la persistance en service de dispositifs anciens, ou « legacy devices ».

1.4.2.2 Les dispositifs médicaux obsolètes : un maillon faible dans la cybersécurité

De nombreux dispositifs médicaux encore en service n'ont pas été conçus pour faire face aux menaces actuelles de cybersécurité. Ils reposent souvent sur des logiciels et systèmes d'exploitation obsolètes, générant des points d'entrée vulnérables pour les attaquants (52).

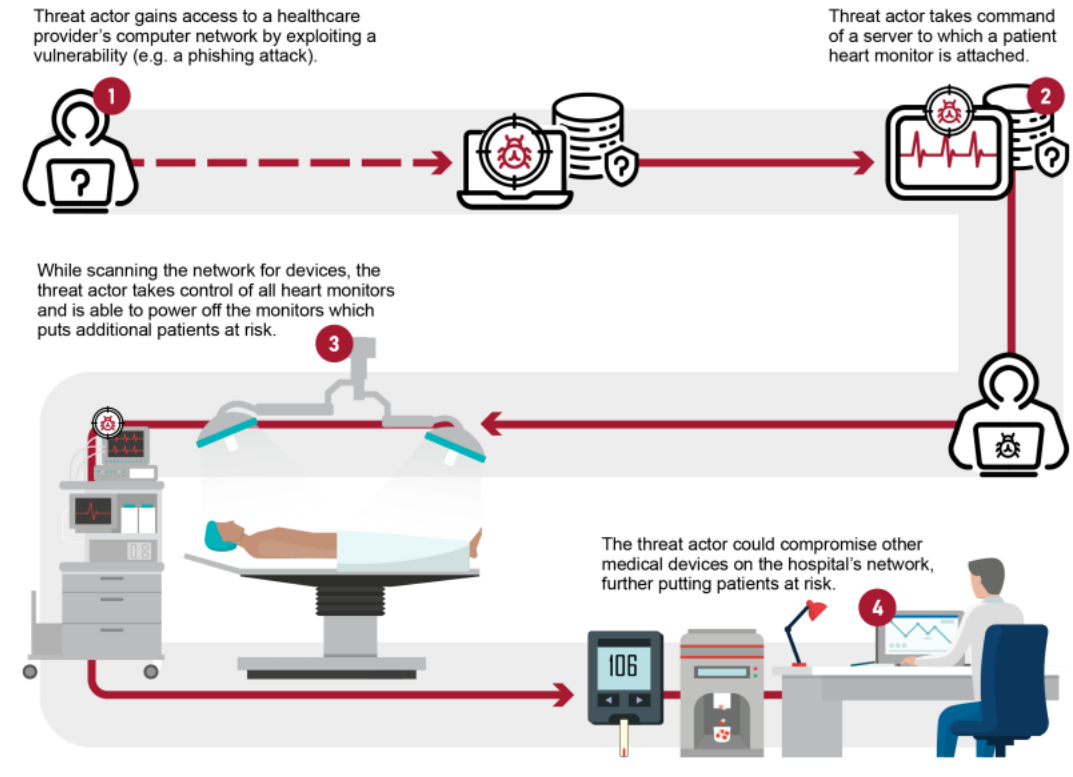
Selon l'IMDRF (International Medical Device Regulators Forum), un dispositif est qualifié de « legacy device » lorsqu'il ne peut pas être raisonnablement protégé contre les menaces actuelles en matière de cybersécurité (53).

Plusieurs facteurs expliquent cette impossibilité :

- Conception initiale sans prise en compte des exigences de sécurité (authentification, chiffrement) (52).
- Absence de mises à jour logicielles et d'assistance en cybersécurité en raison de l'ancienneté de l'équipement (52).
- Durée de vie prolongée des dispositifs médicaux (souvent supérieure à 15 ans) comparée à celle des systèmes informatiques classiques (2–4 ans) (53).

Par exemple, un appareil d'Imagerie par Résonnance Magnétique (IRM) fonctionnant depuis plusieurs dizaines d'années peut encore délivrer un service clinique satisfaisant, mais ne bénéficie plus de correctifs de sécurité ni de support technique adapté. De tels équipements exposent l'ensemble du réseau hospitalier et les autres dispositifs connectés à des risques accrus (52).

En pratique, la majorité des établissements de santé utilisent leurs dispositifs bien au-delà de la fin de vie prévue des composants logiciels, ce qui renforce leur vulnérabilité et expose les patients à des menaces potentielles (48).



Sources: GAO interpretation of Department of Health and Human Services example (illustrations); gofficon/stock.adobe.com (icons); elenabsl/stock.adobe.com (illustrations). | GAO-24-106683

***Figure 8** : Exemple d'un dispositif médical compromis pouvant entraîner la perturbation d'autres dispositifs sur le réseau d'un hôpital*

L'obsolescence des « legacy devices » préfigure un second défi tout aussi critique : garantir la sécurité des échanges entre systèmes et des connexions à distance. En effet, l'interopérabilité – qui permet aux dispositifs de communiquer et de partager des données, combinée à la possibilité de supervision ou de pilotage à distance, élargit considérablement la surface d'attaque (48).

1.4.2.3 Interopérabilité et accès à distance : vecteurs critiques de vulnérabilité des dispositifs médicaux

L'interopérabilité entre dispositifs médicaux et systèmes d'information clinique, couplée à la possibilité d'accès à distance, accroît significativement la surface d'attaque. Cette connexion permanente s'appuie sur des réseaux locaux, des services cloud ou des ponts avec l'Internet grand public, exposant les appareils à des tentatives d'intrusion, de vol de données ou de manipulation malveillante (54).

Les principaux risques liés à ces fonctionnalités sont les suivants :

- Protocoles de communication non chiffrés ou obsolètes favorisant l'écoute clandestine et l'injection de commandes.
- Authentification insuffisante ou partagée, permettant à des acteurs non autorisés de prendre le contrôle des équipements.
- Points d'entrée multiples, difficiles à inventorier et à sécuriser dans leur globalité.
- Dépendance aux infrastructures externes (cloud), créant des ruptures de disponibilité en cas de panne ou d'attaque ciblée.

L'accès à distance, indispensable pour la maintenance, les mises à jour logicielles et la télésanté, devient un vecteur privilégié pour les cybercriminels lorsqu'il n'est pas correctement sécurisé. Exploiter ces accès non protégés permet de s'introduire dans le réseau hospitalier, de corrompre des données ou de prendre le contrôle des dispositifs, mettant directement en péril la sécurité des patients (54).

La sécurisation des échanges et des accès à distance met en évidence une réalité incontournable : la fiabilité d'un dispositif médical repose avant tout sur sa conception et son cycle de vie, façonnés par son fabricant.

1.4.3 Le rôle central des fabricants dans la cybersécurité des dispositifs médicaux

La digitalisation croissante du secteur médical a redéfini les interactions entre acteurs et renforcé le rôle pivot des fabricants de dispositifs médicaux dans la sécurisation du parcours de soin. En tant que concepteurs et propriétaires des logiciels embarqués, ils détiennent non seulement la responsabilité de la fiabilité de leurs produits, mais aussi celle de la protection des données et de la sûreté des patients (55).

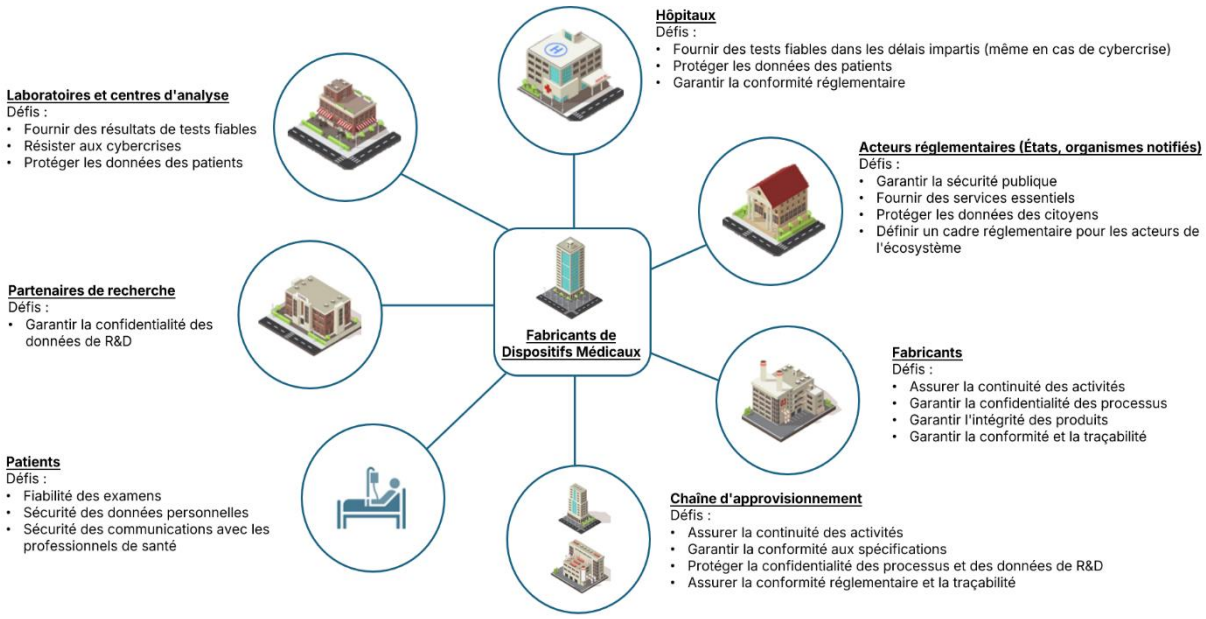


Figure 9 : Le fabricant : au cœur du défi de cybersécurité

La figure 9 illustre les flux d'informations entre le fabricant et les autres parties prenantes : établissements de santé, autorités réglementaires, fournisseurs de services tiers et utilisateurs finaux. Cette cartographie met en lumière la nature collaborative de la cybersécurité :

- Chaque acteur doit assumer ses responsabilités.
- Les échanges de données et de retours d'expérience doivent être sécurisés.
- La coordination est essentielle pour détecter et neutraliser rapidement les menaces.

En plus d'être responsable de la sécurité des dispositifs qu'ils produisent, les fabricants sont propriétaires des logiciels de leurs appareils. Dès lors, les équipes informatiques des établissements de santé ne sont pas en mesure d'accéder à ces logiciels et dépendent donc des fabricants pour assurer la sécurité des données (4).

En plaçant le fabricant au centre de ces processus, cela permet d'avoir une approche globale de la cybersécurité, fondée sur la prévention, la surveillance et la réactivité tout au long du cycle de vie du dispositif médical.

Fort de ce rôle central du fabricant dans la prévention, la détection et la réponse aux menaces, il convient désormais de confronter ces principes à des situations réelles.

1.4.4 Etudes de cas : Dispositifs cardiologiques implantables

Récemment, les implants cardiologiques (pacemakers et défibrillateurs) ont fait l'objet d'une attention médiatique majeure en matière de cybersécurité. Dès août 2016, le rapport de Muddy Waters Research mettait en garde contre le risque de piratage élevé de ces appareils (56).

L'étude portait sur l'environnement complet du fabricant St. Jude Medical Inc., articulé autour de quatre éléments clés :

Dispositif implantable :  ***Figure 10** : Stimulateur Cardiaque Assurity MRI™*	Les dispositifs cardiaques sont implantés chez les patients généralement pour traiter la tachycardie et la bradycardie. Ils sont compatibles avec les radiofréquences, de sorte qu'ils peuvent communiquer avec les dispositifs et les programmateurs Merlin@Home.
Programmateur :  ***Figure 11** : Programmateur MerlinTM*	Le programmateur est généralement utilisé par un médecin ou un professionnel de santé. Son rôle est d'interroger, programmer, afficher des données et tester le dispositif implantable.
Merlin@Home :  ***Figure 12** : Transmetteur Merlin@home*	Il a pour fonction de recevoir les données relatives à l'appareil et à l'état de santé du patient en provenance des dispositifs cardiaques, puis de les transmettre au réseau. Ces appareils contiennent des informations et des codes critiques non

	cryptés qui ouvrent la porte aux potentiels attaquants.
Réseau :  ***Figure 13** : Plateforme collaborative*	Le réseau permet le transfert de données entre les dispositifs implantés, les programmateurs, Merlin@Home et les médecins. Les informations transmises comprennent les données du patient, les diagnostics de performance à distance et les mises à jour relatives au dispositif.

Muddy Waters Research ont été capables de démontrer et reproduire, sans expérience en cybersécurité deux types de cyberattaques contre des dispositifs de produits par St. Jude Medical Inc (aujourd'hui Abbott) (56):

- Une attaque de type « crash » qui provoque un dysfonctionnement des dispositifs cardiaques - y compris en stimulant apparemment à une vitesse potentiellement dangereuse. La diffusion d'une combinaison de signaux via le dispositif vulnérable Merlin@Home permettaient en effet de faire dysfonctionner les dispositifs (56).
- Une attaque de type « battery drain » qui a pour objectif d'épuiser les batteries des dispositifs à une vitesse très accélérée. Pour se faire, les équipes en charge de l'étude ont généré des signaux là encore à partir du dispositif Merlin@Home. Ils soulignent également que les hackers pourraient vider progressivement les batteries des dispositifs pendant la nuit lorsque les patients sont endormis (56).

L'étude a montré que ces attaques, exploitant l'absence de mécanismes de chiffrement et d'authentification, s'appuyaient sur l'usurpation du dispositif Merlin@Home. Un attaquant pouvait ainsi émettre de fausses commandes et intercepter ou extraire des données patient, simplement en se plaçant à proximité du patient (rayon de 15 mètres) et sans nécessiter de compétences techniques avancées (56). Depuis la publication de ce rapport et une lettre d'avertissement de la Food and Drug Administration (FDA), plusieurs patchs ont été publiés afin de corriger les vulnérabilités détectées.

D'une façon plus générale, les potentielles vulnérabilités des stimulateurs et défibrillateurs sont résumées ci-dessous (57) :

- Périodes prolongées d’asystolie avec risque de syncope ou de mort subite, via réception de signaux non cardiaques inhibant la stimulation.
- Induction d’arythmies par séquences de stimulation malveillantes.
- Délivrance de chocs inappropriés, voire mortels, en raison d’une sur détection de signaux.
- Décharge prématurée de la batterie, privant le patient de thérapie en cas d’arythmie clinique vitale

Ces vulnérabilités illustrent combien la cybersécurité des implants cardiaques doit être intégrée dès la phase de conception et faire l’objet d’un suivi rigoureux des mises à jour et des incidents.

Comme l'ont montré les trois études de cas présentées dans cette première partie de thèse d’exercice, les établissements de santé et les fabricants de dispositifs médicaux ne sont pas à l'abri des cybermenaces sophistiquées. Ces exemples mettent en évidence le besoin urgent d'une approche structurée pour sécuriser les systèmes d’information. La deuxième partie de cette thèse d’exercice présente les exigences réglementaires fondamentales à la mise en place d'une cybersécurité robuste et examine les défis pratiques, réglementaires, techniques et organisationnels qui doivent être relevés pour protéger la sécurité des patients et l'intégrité des données.

PARTIE 2 : EXIGENCES EN MATIÈRE DE CYBERSÉCURITÉ ET DÉFIS

Les autorités de régulation ont pleinement pris la mesure de la gravité et de l'ampleur des risques liés à la cybersécurité. En réaction et depuis plusieurs années, tout un arsenal de référentiels réglementaires a été déployé.

D'une part, ces outils permettent aux établissements de santé et aux fabricants de dispositifs médicaux d'avoir accès aux bonnes pratiques et aux exigences les plus récentes en matière de cybersécurité. D'autre part, ils accompagnent les fabricants dans la constitution de leurs dossiers de conformité, indispensables notamment pour l'obtention du marquage CE.

Sur le plan international, un ensemble diversifié de règlements, normes, guides et recommandations a été publié pour encadrer la cybersécurité dans le secteur de la santé.

Les États-Unis se sont très tôt affirmés comme référence pour l'élaboration d'un cadre réglementaire en cybersécurité, rapidement imités par d'autres régions du monde comme L'Union Européenne, le Canada, l'Australie, le Japon ou encore la Chine.

Dans le cadre de cette thèse d'exercice, l'analyse portera principalement sur les textes applicables à l'Union européenne. Il ne s'agit pas d'exposer l'intégralité du référentiel, mais de mettre en lumière les textes les plus récents et/ou les plus influents.

2.1 CADRE LÉGISLATIF EUROPÉEN

Au sein de l'Union Européenne, les référentiels législatifs principaux sont les suivants :

- Le Règlement (UE) 2017/745 relatif aux dispositifs médicaux (MDR) et 2017/746 relatif aux dispositifs médicaux de diagnostic *in vitro* (IVDR) (7).
- Le Règlement Général sur la Protection des Données (RGPD) (58).
- Le Règlement « Cybersecurity Act » (59).
- La Directive sur sécurité des réseaux et des systèmes d'Information NIS-2 (Network and Information System) (60).

2.1.1 Règlement (UE) 2017/745 relatif aux dispositifs médicaux (MDR)

2.1.1.1 MDR et exigences principales

Les dispositifs médicaux sont réglementés dans l'Union européenne (UE) par une législation verticale : le Règlement sur les dispositifs médicaux (MDR) publié depuis mai 2017 au Journal Officiel (7).

Ce règlement régit la mise sur le marché et la mise en service des dispositifs médicaux dans l'Union Européenne. Il a pour objectif renforcer la sécurité, la qualité et la transparence des dispositifs médicaux mis sur le marché européen (7).

Bien que principalement destiné aux fabricants, en précisant leurs responsabilités en matière de conception, de documentation et de suivi post-commercialisation, le règlement exerce un impact direct sur les établissements de santé, en tant qu'utilisateurs finaux des dispositifs concernés. Et même s'il ne mentionne pas explicitement la notion de « cybersécurité », il intègre des exigences de sécurité qui imposent des obligations spécifiques aux fabricants de dispositifs médicaux (7) :

- ***Article 5-1*** *:*
  « Un dispositif ne peut être mis sur le marché ou mis en service que s'il est conforme au présent règlement » et si selon l'*article 5-2* « Un dispositif est conforme aux exigences générales en matière de sécurité et de performances » (7).

Les exigences générales de sécurité et de performance (Annexe I) intègrent plusieurs dispositions impliquant des mesures de protection informatique pour les fabricants :

- ***Annexe I – chapitre I – article 3*** :
  « Les fabricants établissent, appliquent, documentent et maintiennent un système de gestion des risques. » (7).
- ***Annexe I – chapitre II – article 14.1*** :
  « Si le dispositif est destiné à être utilisé en combinaison avec d'autres dispositifs ou équipements, l'ensemble, y compris le système de raccordement, est sûr et n'altère pas les performances prévues des dispositifs. » (7).
- ***Annexe I – chapitre II – article 14.2 d)*** :
  « Les dispositifs sont conçus et fabriqués de manière à éliminer ou à réduire autant que possible : tout risque associé à une éventuelle interaction négative entre les logiciels et l'environnement informatique dans lequel ceux-ci fonctionnent et avec lequel ils interagissent ; » (7).
- ***Annexe I – chapitre II – article 14.5*** :
  « Les dispositifs qui sont destinés à être mis en œuvre avec d'autres dispositifs ou produits sont conçus et fabriqués de manière que leur interopérabilité et leur compatibilité soient fiables et sûres. » (7).
- ***Annexe I – chapitre II – article 17.2*** :

« Pour les dispositifs qui comprennent des logiciels ou pour les logiciels qui sont des dispositifs à part entière, ces logiciels sont développés et fabriqués conformément à l'état de l'art, compte tenu des principes du cycle de développement, de gestion des risques, y compris la sécurité de l'information, de vérification et de validation. » (7).

- ***Annexe I – chapitre II – article 17.4*** :
  « Les fabricants énoncent les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu » (7).
- ***Annexe I – chapitre II article – 18*** :
  « Les dispositifs sont conçus et fabriqués de façon à les protéger autant que possible contre un accès non autorisé qui les empêcherait de fonctionner comme prévu. » (7).

Plusieurs obligations touchant directement à la cybersécurité, bien que déduites du règlement (UE) 2017/745, ne figurent pas sous l'étiquette « cybersécurité » (7):

- Évaluation de la conformité par un organisme notifié (*Article 52, Annexes II et III*) incluant la vérification de la prise en compte des Exigences Générales de Sécurité et de Performances.
- Système de management de la qualité incluant l'obligation de mettre en place un Système de Management de la Qualité (SMQ) conforme, couvrant l'ensemble du cycle de vie du dispositif.
- Protection de la vie privée et des données à caractère personnel (*Art. 62(4)(h)*) incluant le respect du RGPD pour les essais cliniques et le traitement des données issues des dispositifs médicaux.
- Surveillance post-commercialisation et vigilance (*Art. 83 à 89*) incluant la mise en place de systèmes PMS obligatoires et la remontée des incidents graves.

NB : Les mêmes exigences sont applicables pour les dispositifs médicaux de diagnostic in vitro encadrés par le règlement 2017/746.

Ces exigences, bien que fondamentales, restent très générales et ne précisent pas les mesures techniques et procédurales concrètes que doivent mettre en place les fabricants pour garantir la cybersécurité. Afin de combler ce manque de granularité, le Medical Device Coordination Group (MDCG) a publié en décembre 2019 le guide MDCG 2019-16 Rev.1 (61).

2.1.1.2 MDCG 2019-16 : Orientations sur la cybersécurité des dispositifs médicaux

Le guide MDCG 2019-16 Rev.1, publié en décembre 2019 (révisé en juillet 2020), a été élaboré par le Medical Device Coordination Group pour aider les fabricants à répondre aux exigences implicites de cybersécurité du Règlement (UE) 2017/745 (MDR) et du Règlement (UE) 2017/746 (IVDR) (61).

Ce guide vient donner des recommandations additionnelles sur :

- **La conformité** :
  Comment respecter les exigences en matière de cybersécurité énoncées à l'annexe I (61).
- **La gestion des risques** :
  Comment trouver l'équilibre adéquat entre les avantages et les risques dans tous les modes de fonctionnement possibles du dispositif médical. Et comment examiner la relation entre « sûreté et sécurité » et le risque (61).
- **Les mesures de sécurité** :
  Comment mettre en œuvre des mesures de sécurité informatique, y compris la protection contre les accès non autorisés, et veiller à ce que les correctifs de sécurité soient mis à jour en temps utile (61).
- **Les activités de cybersécurité à chaque étape du cycle de vie** :
  De la conception "security by design" jusqu'à la fin de vie du dispositif (61).
- **La surveillance après la mise sur le marché** :
  Bonnes pratiques pour la surveillance post-commercialisation et la remontée d'incidents (Periodic Safety Update Report, Field Safety Corrective Actions) (61).
- **L'importance de la formation du personnel** :
  L'identification des vulnérabilités et la mise en œuvre des contrôles de sécurité sont particulièrement soulignées (61).

Ce guide encourage à une approche proactive de la cybersécurité pour les dispositifs médicaux, en soulignant la nécessité de protéger la sécurité et la vie privée des patients grâce à des mesures de sécurité robustes et à une vigilance constante (62).

Bien que très détaillé, le guide MDCG 2019-16 n'a pas de valeur légale contraignante. Les fabricants restent libres de s'en écarter, pour autant qu'ils démontrent la conformité aux Exigences générales en matière de sécurité et de performances du MDR ou de l'IVDR (63).

Cette absence de force obligatoire peut conduire à une application hétérogène des bonnes pratiques de cybersécurité à travers l'Union européenne. Ce défi sera abordé plus en détail dans la section 2.3 de cette thèse d'exercice.

2.1.2 Le Règlement Général sur la Protection des Données (RGPD)

2.1.2.1 Champ d'application du RGPD

Le Règlement Général sur la Protection des Données (2016/679 ou « RGPD ») publié en mai 2016 « établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. » (58).

Son objectif principal est donc de renforcer la protection des données personnelles des individus au sein de l'Union Européenne tout en harmonisant les règles pour les organisations qui les traitent (58).

Il s'applique à toute entité, personnes physiques, entreprises ou organisations, qui traite des données concernant des individus résidant dans l'UE, et ce, même si le traitement est effectué en dehors du territoire européen.

Les fabricants de dispositifs médicaux et les établissements de santé entrent dans son périmètre dès lors qu'ils collectent, conservent, transmettent ou analysent des données de santé (58).

Les données à caractère personnel recouvrent toute information relative à une personne vivante identifiée ou identifiable : nom, prénom, date de naissance, adresse e-mail, ainsi que tout élément permettant, seul ou en combinaison, de remonter à l'identité d'un individu (58).

Une violation de données est définie comme toute « violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » (*article 4.12*) (58).

Conçu pour harmoniser les législations européennes et redonner aux citoyens le contrôle de leurs données, le RGPD s'applique indépendamment de la technologie ou du support utilisé (systèmes informatiques, vidéosurveillance, documents papier, etc.) : toutes les données personnelles sont soumises aux mêmes exigences de protection (58).

2.1.2.2 Principales exigences du RGPD

Le RGPD oblige toute organisation traitant des données à caractère personnel à mettre en place des mesures techniques et organisationnelles appropriées pour garantir la confidentialité, l'intégrité et la disponibilité des données, ainsi qu'à évaluer régulièrement les risques associés (64).

Les exigences principales sont (64):

- **Loyauté et transparence** :
  Obligation pour chaque traitement de données de reposer sur une base légale claire et informer les personnes concernées.
- **Minimisation des données** :
  Obligation de ne collecter que les données strictement nécessaires aux finalités déclarées.
- **Limitation des finalités** :
  Obligation d'utiliser les données uniquement pour les objectifs spécifiés lors de la collecte.
- **Droits des personnes** :
  Obligation de garantir l'accès, la rectification, l'effacement (« droit à l'oubli »), la portabilité et l'opposition au traitement.
- **Consentement explicite** :
  Obligation de recueillir un consentement libre, spécifique, éclairé et univoque lorsque requis.
- **Registre des activités de traitement** :
  Obligation de tenir à jour un document décrivant les traitements, les finalités et les durées de conservation.
- **Privacy by design et by default** :
  Obligation d'intégrer la protection des données dès la conception des systèmes et activer par défaut les paramètres les plus stricts.
- **Evaluation d'impact** :
  Obligation de procéder à une évaluation de l'impact sur la protection des données.
- **Protection du transfert de données** :
  Obligation de garantir la protection des données lors de leurs transferts.
- **Délégué à la protection des données (DPO)** :

Obligation de désigner un responsable chargé de veiller à la conformité RGPD qui a le rôle d'interface avec l'autorité de contrôle.

- **Sensibilisation et formation** :
  Obligation de former régulièrement l'ensemble du personnel aux bonnes pratiques de protection des données et aux procédures internes.

En cas de violation de données avérée, l'organisation doit notifier l'autorité de contrôle compétente dans les 72 heures. Lorsque le risque pour les droits et libertés des personnes est élevé, elle doit également informer les personnes concernées.

Le non-respect de ces obligations pouvant entraîner des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel (49).

2.1.3 Cybersecurity Act

2.1.3.1 Champ d'application du Cybersecurity Act

Le Cybersecurity Act (règlement UE 2019/881) (59) a été publié au Journal officiel en juin 2019 et marque une avancée décisive pour l'autonomie stratégique de l'Union européenne en matière de cybersécurité (65).

Le Cybersecurity Act établit un cadre légal européen unique pour renforcer la cybersécurité des Technologies de l'Information et de la Communication (TIC) dont font partie les dispositifs médicaux. Il confère également un mandat permanent à l'Agence de l'Union européenne pour la cybersécurité (ENISA) (59).

Il s'applique aux acteurs suivants (59):

- Fabricants de produits TIC intégrant des fonctions de sécurité, notamment les dispositifs médicaux équipés de logiciels embarqués ou d'interfaces réseau.
- Fournisseurs de services TIC (hébergement, communications électroniques, services de santé en ligne) utilisés par les établissements de santé.
- Prestataires de services de sécurité gérés assurant la supervision, la détection et la réponse aux incidents.
- Organismes nationaux de certification désignés pour superviser l'application des schémas européens sur le territoire des États membres.

2.1.3.2 Principales exigences du Cybersecurity Act

Le règlement définit deux obligations centrales pour les fabricants et prestataires (65):

- **Certification volontaire harmonisée** :

- Mise en place de schémas de certification qui couvrent les produits, services, processus et services de sécurité.
- Trois niveaux d'assurance (élémentaire, substantiel, élevé) avec preuves d'évaluation adaptées.
  Niveau élémentaire : auto-déclaration possible.
  Niveaux substantiel et élevé : évaluation par un organisme tiers.
- Reconnaissance mutuelle dans tous les États membres, simplifiant l'accès au marché européen pour les dispositifs médicaux certifiés.

- **Mandat renforcé de l'ENISA** :
  - Permanence du rôle d'appui aux autorités nationales et aux secteurs critiques (santé, dispositifs médicaux) pour la prévention et la réponse aux cybermenaces.
  - Élaboration et mise à jour, tous les cinq ans, des schémas de certification à la demande de la Commission européenne ou du Groupe européen de certification (ECCG).
  - Coordination du réseau paneuropéen des équipes d'intervention et diffusion des bonnes pratiques de cybersécurité pour le secteur médical.
- **Harmonisation des standards** :
  - Uniformiser les pratiques de cybersécurité dans l'UE.
  - Reconnaissance mutuelle des certificats entre États membres.

Le Cybersecurity Act ne prévoit pas d'amendes uniformes au niveau européen, il renvoie aux États membres le soin de fixer des sanctions « efficaces, proportionnées et dissuasives » (*article 65*) (59).

2.1.4 La Directive NIS-2

2.1.4.1 Une révision de la directive NIS-1

La directive NIS-2 (2022/2555) (60), publiée en décembre 2022, constitue aujourd'hui le texte de référence en matière de cybersécurité pour les établissements de santé et les fabricants de dispositifs médicaux. À la date de rédaction de cette thèse d'exercice, elle capte toute l'attention du secteur.

NIS-2 s'appuie sur la version précédente de la directive (NIS-1 / UE 2016/1148), publiée en 2016. Celle-ci avait pour ambition de définir des exigences minimales communes en matière de sécurité des réseaux et des systèmes d'information, ainsi que de mettre en place une coopération renforcée entre autorités nationales (66).

Toutefois, la mise en œuvre de NIS-1 a mis en lumière plusieurs limitations pratiques (66) :

- **Identification difficile des entités soumises aux exigences** :
  Chaque État membre a défini ses propres critères pour déterminer les entités concernées, ce qui a engendré de fortes disparités d'un pays à l'autre.
- **Exigences de sécurité et notification des incidents disparates** :
  Absence de spécifications communes sur le périmètre des événements déclarables et les délais de notification.
- **Supervision et échange d'informations insuffisant** :
  Le contrôle national était parfois limité et le partage transfrontalier de renseignements jugé insuffisant.

Pour remédier à ces lacunes, le législateur européen a élaboré la directive NIS-2, dont les principaux objectifs sont (67) :

- D'élargir le périmètre des entités concernées.
- De renforcer les exigences techniques et organisationnelles.
- D'harmoniser les modalités de notification et de contrôle, et de faciliter la coopération et le partage d'informations entre États membres.

Ces évolutions visent à accroître significativement la résilience globale de la cybersécurité au sein de l'Union européenne en uniformisant et en élevant le niveau minimal de sécurité pour les réseaux et systèmes d'information (60).

Après avoir présenté les objectifs et les apports de la directive NIS-2, il est désormais essentiel de préciser son champ d'application.

2.1.4.2 Champ d'application de la directive NIS-2

La directive NIS-2 étend et précise le périmètre des entités soumises à ses obligations. Elle ne vise pas seulement les fabricants de logiciels ou de dispositifs médicaux connectés, mais l'ensemble des acteurs de la chaîne de santé, ainsi que plusieurs secteurs jugés critiques au niveau européen (66).

La réglementation distingue deux grands ensembles d'entités (60) :

- Secteurs hautement critiques (Annexe I).
- Autres secteurs critiques (Annexe II).

Parmi les secteurs concernés figurent notamment l'énergie, les transports, la finance, ainsi que la santé.

Pour la santé, au sein des secteurs hautement critiques, sont concernés (60):

- Tous les prestataires de soins (hôpitaux, cliniques, cabinets médicaux…).
- Les laboratoires de référence de l'Union européenne.
- Les entités de recherche et développement pharmaceutique.
- Les fabricants de substances pharmaceutiques de base.
- Les fabricants de dispositifs médicaux jugés critiques en cas d'urgence de santé publique.

Les fabricants de dispositifs médicaux non considérés comme critiques en situation d'urgence relèvent, quant à eux, des « autres secteurs critiques » (60).

Depuis la publication de la directive en décembre 2022, les États membres disposaient d'un délai de transposition jusqu'au 17 octobre 2024 pour intégrer ces dispositions dans leur droit national (66).

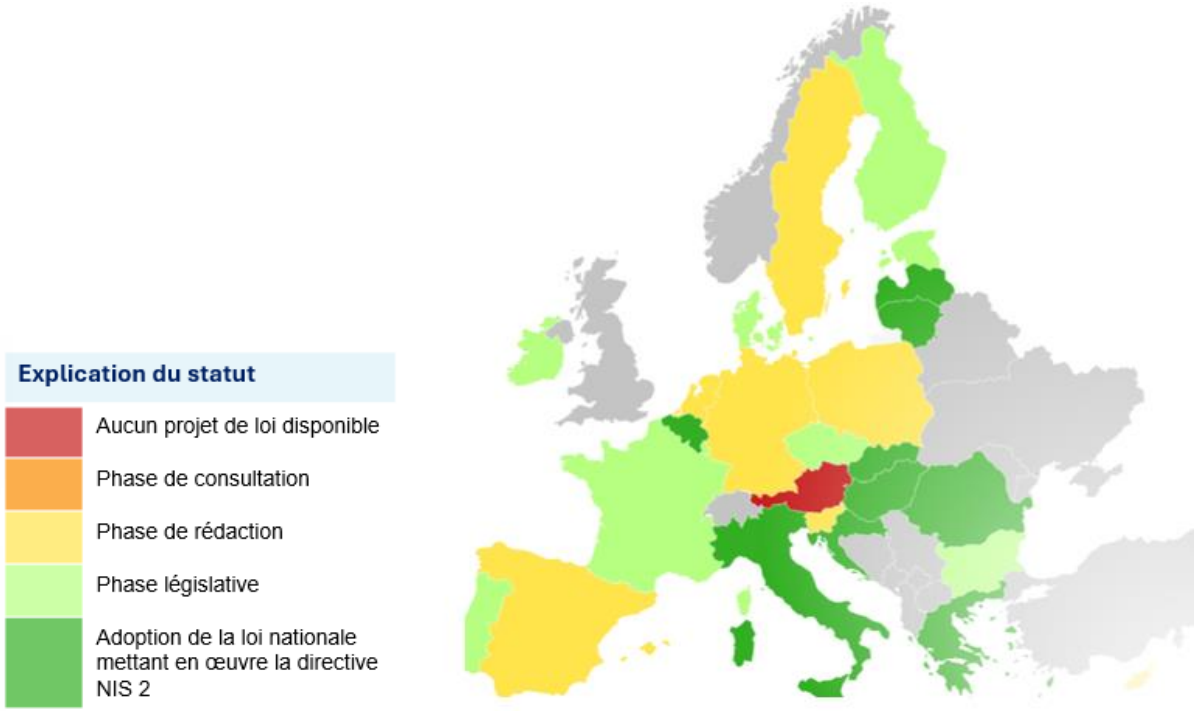


***Figure 14** : Directive NIS-2 : Statut de transposition dans l'UE*

Cette phase de transposition comprend l'adoption d'une loi nationale, la publication de textes d'application (décrets, arrêtés) et la notification formelle à la Commission européenne (68).

La figure 14 met en avant que de nombreux pays n'ont pas encore terminé la transposition de la directive. Ces États sont à différents stades – projet de loi en discussion, adoption récente ou attente de textes secondaires – ce qui crée un paysage fragmenté pour les acteurs de la santé et les fabricants de dispositifs médicaux.

Il est donc essentiel pour chaque entité concernée de suivre de près la transposition dans les pays où elle opère, afin de respecter les obligations de sécurité, d'enregistrement et de notification d'incidents prévues par NIS-2.

2.1.4.3 Vue d'ensemble des exigences de la directive NIS-2

La directive NIS-2 instaure un cadre harmonisé d'obligations à destination des entités essentielles et importantes afin de renforcer la résilience des réseaux et des systèmes d'information. Ses exigences couvrent cinq grands domaines : gestion des risques, sécurité de la chaîne d'approvisionnement, gouvernance, formation et notification des incidents (69).

Les entités doivent mettre en place des mesures techniques et organisationnelles adéquates et proportionnées pour identifier, analyser et maîtriser les risques pesant sur leurs réseaux et systèmes d'information.

Ces mesures comprennent notamment (70) :

- Politique de gestion des risques et de sécurité des systèmes d'information.
- Mise en place de dispositifs de prévention, détection et réponse aux incidents.
- Plans de continuité d'activité et de reprise après sinistre.
- Procédures de traitement et de divulgation des vulnérabilités.

La directive impose une évaluation systématique des risques liés aux fournisseurs et prestataires (60):

- Inventaire et classification des tiers critiques.
- Intégration de clauses de cybersécurité dans les contrats.
- Tests réguliers des services et produits tiers.
- Suivi des correctifs et des mises à jour de sécurité.

La conformité à NIS-2 relève directement de la responsabilité des organes de direction (60):

- Approbation formelle des mesures de sécurité et de gestion des risques.
- Supervision de la mise en œuvre et des résultats.

- Responsabilisation du top management en cas de manquement.

Pour garantir l'efficacité des mesures techniques, la directive exige :

- Programmes réguliers de formation pour l'ensemble du personnel, en particulier les équipes opérationnelles.
- Sessions adaptées aux dirigeants sur les enjeux et la gouvernance de la cybersécurité.
- Exercices de simulation d'incidents et de gestion de crise.

NIS-2 renforce et uniformise les délais et le contenu des signalements (60) :

- Alerte précoce sous 24 heures après détection d'un incident susceptible d'avoir un impact significatif.
- Notification détaillée sous 72 heures avec évaluation initiale (gravité, portée, indicateurs connus).
- Rapports intermédiaires à la demande des autorités ou des CSIRT nationaux.
- Rapport final sous un mois, incluant l'analyse de la cause racine, les mesures correctives et les impacts transfrontaliers.

Le rôle des autorités compétentes a également été complétement revu à la hausse avec la possibilité de réaliser des audits sur les sites des entités impactées.

La mise en place d'un cadre législatif européen précis constitue la première pierre d'une stratégie globale de cybersécurité pour les établissements de santé et les fabricants de dispositifs médicaux. Toutefois, pour que ces exigences juridiques se traduisent réellement en mesures de protection opérationnelles, il est essentiel de s'appuyer sur un environnement normatif rigoureux.

2.2 ENVIRONNEMENT NORMATIF

Des organisations telles que l'Organisation internationale de normalisation (International Organization for Standardization : ISO) et la Commission électrotechnique internationale (International Electrotechnical Commission : IEC) ont élaboré des normes internationales en lien avec la cybersécurité.

L'application de ces normes témoigne d'un engagement en faveur des meilleures pratiques en matière de sécurité de l'information, ce qui peut s'avérer essentiel pour satisfaire aux exigences réglementaires (certification des dispositifs médicaux) et instaurer un climat de confiance entre les différents acteurs de la santé.

Elles offrent donc une structure acceptée pour la gestion de la sécurité de l'information, garantissant une approche cohérente entre les différentes organisations et industries.

2.2.1 ISO 14971

L'ISO 14971 :2019 spécifie la terminologie, les principes et les processus de gestion des risques applicables à tous les types de dispositifs médicaux, y compris les logiciels utilisés en tant que dispositifs médicaux et les dispositifs médicaux de diagnostic *in vitro*. Cette norme couvre l'ensemble du cycle de vie d'un produit – de l'identification des dangers à la maîtrise des risques (71).

Les principaux aspects de la norme ISO 14971 :2019 sont les suivants (71):

- **Champ d'application** :
  La norme s'applique à toutes les étapes du cycle de vie d'un dispositif médical.
- **Processus de gestion des risques** :
  Il comporte plusieurs étapes, à commencer par la phase de planification, l'évaluation des risques (qui comprend l'analyse des risques et l'évaluation des risques), la maîtrise des risques, l'évaluation du risque résiduel global, l'examen de la gestion des risques, ainsi que les activités de production et de post-production.
- **Analyse des risques** :
  Identification des dangers associés à un dispositif médical, d'estimer le risque associé à chaque danger identifié et d'évaluer si chaque risque doit être contrôlé.
- **Évaluation des risques** :
  Détermination des risques acceptables sur la base de critères prédéfinis.
- **Maîtrise des risques** :
  Sélection et mise en œuvre des mesures pour maîtriser les risques. Il s'agit également de vérifier que les mesures de contrôle des risques sont efficaces.
- **Evaluation du risque résiduel** :
  Evaluation du risque résiduel global associé à l'ensemble des mesures de maîtrise des risques afin de s'assurer qu'il est acceptable.
- **Examen de la gestion des risques** :
  Examen du processus de gestion des risques et de ses résultats pour s'assurer qu'il est complet et efficace.
- **Informations sur la production et la post-production** :

Contrôle et rassemblement les informations pertinentes sur la production et la postproduction et, si nécessaire, de mettre à jour l'analyse des risques et/ou le processus de gestion des risques sur la base de ces informations.

La première étape de l'adaptation de la norme ISO 14971 à la cybersécurité consiste à étendre le processus d'évaluation des risques aux vulnérabilités numériques. Cela implique (72) :

- Une analyse approfondie de la conception du dispositif et des interactions avec le réseau afin d'identifier les vulnérabilités potentielles en matière de cybersécurité.
- Une collaboration avec des experts en cybersécurité, des professionnels de l'informatique de santé et des utilisateurs finaux afin de comprendre les menaces numériques potentielles.
- L'utilisation de techniques de modélisation des menaces pour prévoir les vecteurs d'attaque potentiels et s'y préparer.

2.2.2 IEC 62304

La norme IEC 62304 :2006 définit les exigences de cycle de vie pour le développement et la maintenance des logiciels de dispositifs médicaux, qu'il s'agisse de logiciels intégrés à un matériel (embedded), autonomes (Software as a Medical Device : SaMD) ou mobiles. Elle décrit un cadre commun de processus, d'activités et de tâches à mettre en œuvre par les fabricants pour garantir la sûreté et la qualité des logiciels médicaux tout au long de leur vie (73). Cette norme contribue indirectement à la cybersécurité en établissant un cadre pour le développement et la maintenance de logiciels sûrs et fiables.

Les principaux aspects de la norme IEC 62304 sont les suivants (74) :

- **Classification de sécurité du logiciel** :
  - Classe A : pas de risque pour le patient en cas de défaillance.
  - Classe B : risque de blessure non grave.
  - Classe C : risque de décès ou de blessure grave. Cette classification conditionne l'effort de vérification, de documentation et de tests à chaque étape du cycle de vie du dispositif.
- **Processus de développement logiciel** :

Planification, définition des exigences fonctionnelles et de sécurité, conception, implémentation, vérification et validation adaptées à la classe de sécurité du logiciel.

- **Processus de maintenance** :
  Gestion des correctifs, mises à jour de sécurité, contrôle des vulnérabilités découvertes post-commercialisation.
- **Gestion des risques logiciel** :
  Identification et analyse des dangers spécifiques au logiciel (y compris cybersécurité), estimation du risque, définition et validation des mesures de maîtrise (aligné avec norme ISO 14971).
- **Processus de gestion de configuration** :
  Traçabilité des versions, des modules et des composants tiers (Software of Unknown Provenance : SOUP), contrôles d'intégrité et de compatibilité.
- **Processus de résolution de problème logiciel** :
  Élaboration, suivi et analyse des rapports d'incidents (bug reports), investigations pour les problèmes de sûreté ou de sécurité cyber.

L'application de cette norme permet de garantir la sûreté du logiciel, d'identifier comme dangers potentiels les vulnérabilités logicielles et d'intégrer au plan de gestion des risques les menaces cyber tout au long du cycle de vie.

2.2.3 IEC 82304-1

L'IEC 82304-1 :2016, définit les exigences générales de sécurité et de sûreté applicables aux produits logiciels de santé autonomes. Elle s'adresse principalement aux fabricants et couvre l'ensemble du cycle de vie du logiciel : conception, développement, validation, installation, maintenance et élimination (75). L'adoption de l'IEC 82304-1 répond à un vide normatif pour les logiciels de santé non embarqués.

Son objectif est de fournir les outils pour garantir la confidentialité, l'intégrité et la disponibilité des données de santé ainsi que réduire la surface d'attaque en imposant des contrôles d'accès, des mécanismes d'authentification forte et un cryptage adapté.

Les exigences clés de la norme IEC 82304 sont les suivantes (76) :

- Définition de l'emploi prévu et des utilisateurs cibles, y compris le contexte clinique et technique.
- Spécifications de l'interface utilisateur, des exigences de sécurité fonctionnelle et de la protection des données personnelles.

- Gestion des risques logiciels, alignée sur les processus de l'IEC 62304.
- Planification et exécution de la validation indépendante, avec rapport documentaire sur les écarts et le risque résiduel.
- Rédaction d'instructions d'utilisation détaillées (installation, mise en réseau, mises à jour, mise hors service).
- Intégration des activités de maintenance logicielle dans un cadre de gestion des vulnérabilités : analyse d'impact, tests de régression et enregistrements des changements.

2.2.4 ISO/IEC 27001

La norme ISO/IEC 27001 : 2022 définit les exigences auxquelles un Système de Management de la Sécurité de l'Information (SMSI) doit répondre. Son objectif est d'assurer la confidentialité des données patients, la protection des dossiers médicaux contre toute divulgation non autorisée et garantir l'intégrité des informations cliniques (77).

Les exigences clés de la norme ISO/IEC 27001 sont les suivantes (78) :

- **Contexte de l'organisation** :
  Comprendre les besoins des parties prenantes et déterminer le périmètre du système d'information.
- **Direction** :
  Engagement de la direction, politique de sécurité de l'information et répartition claire des responsabilités (Responsable de la Sécurité des Systèmes d'Information : RSSI, DPO, etc.).
- **Planification** :
  Identification et évaluation des risques, élaboration de la déclaration d'applicabilité et des objectifs de sécurité.
- **Support** :
  Compétences, sensibilisation, communication interne et gestion documentaire.
- **Opération** :
  Mise en œuvre des mesures de sécurité, gestion des incidents et contrôle d'accès.
- **Évaluation de performance** :
  Audit interne, revue de direction et suivi des indicateurs de sécurité.
- **Amélioration** :

Traitement des non-conformités, actions correctives et amélioration continue du SMSI.

Pour les fabricants, l'application de ces normes constituent les pierres angulaires de toute démarche « security by design » : elles orientent les choix de conception, de développement et de validation des dispositifs pour maîtriser les risques de cybersécurité. Pour les établissements de santé, elle offre un référentiel d'évaluation et de sélection des dispositifs médicaux, permettant d'intégrer de manière sécurisée les produits au sein du système d'information et d'organiser la surveillance continue des risques.

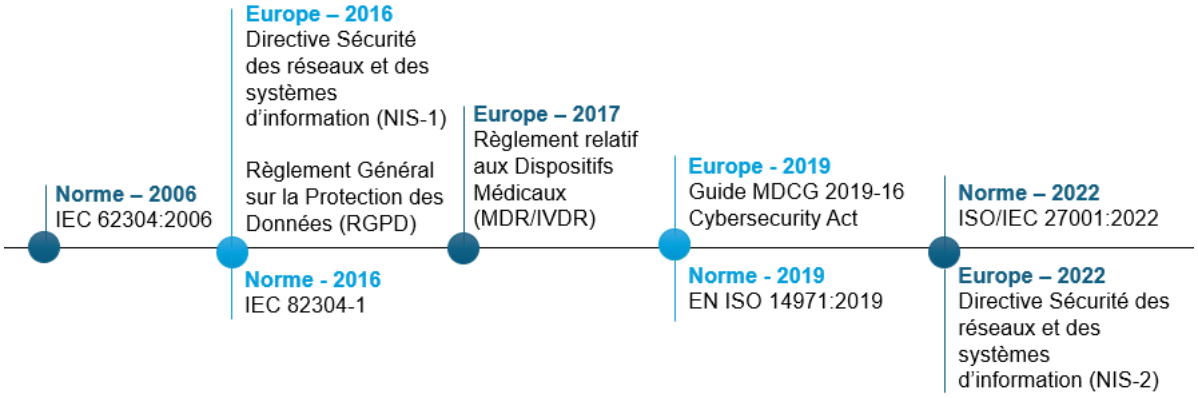


***Figure 15** : Chronologie des dates importantes sur la réglementation cybersécurité*

2.3 DÉFIS DE CONFORMITÉ POUR LES ÉTABLISSEMENTS DE SANTÉ ET LES FABRICANTS

Les établissements de santé mettent plus de temps que les autres secteurs à contenir les violations de données en raison de ressources limitées, tant financières que humaines, et d'une infrastructure souvent sous-dimensionnée. Cette situation accroît le risque d'exfiltration d'informations sensibles et compromet la continuité des soins (2).

2.3.1 Défis réglementaires

La cybersécurité des dispositifs médicaux est aujourd'hui encadrée par un ensemble hétérogène de textes et de normes : MDR 2017/745, IVDR 2017/746, Cybersecurity Act 2019/881, RGPD, directive NIS 2, MDCG 2019-16, etc.

Chaque référentiel comporte ses propres exigences, parfois redondantes ou contradictoires, ce qui complique l'élaboration et la mise à jour d'une politique de cybersécurité unifiée et opérationnelle. Les fabricants doivent en permanence (79):

- Assurer une veille réglementaire couvrant les évolutions de chaque texte et de leurs lignes directrices.
- Comparer et synthétiser des exigences variables (gestion des vulnérabilités, notification d'incidents, tests de résistance, etc.).
- Adapter leurs procédures internes pour concilier conformité et optimisation des coûts.

Cette situation réglementaire complexe s'explique par deux phénomènes majeurs que sont la transposition en droit national et le chevauchement des réglementations.

2.3.1.1 La transposition en droit national

La directive NIS 2 par exemple, est un texte nécessitant une transposition en droit interne de chaque État membre. Si cette phase est indispensable pour prendre en compte les spécificités nationales, elle introduit plusieurs difficultés pour les fabricants implantés dans plusieurs pays de l'Union (79):

- Une veille continue sur l'avancée des décrets de transposition et sur le calendrier d'application dans chaque juridiction.
- L'ajustement du plan de conformité pour répondre à des seuils de notification, à des délais de reporting et à des modalités d'audit qui peuvent différer d'un État à l'autre.
- La nomination éventuelle d'un représentant local pour les entités étrangères, exigence prévue par la directive NIS 2 pour les organisations hors UE.

Cette variabilité peut encourager le « shopping réglementaire », où les fabricants privilégient les pays offrant un cadre d'application plus souple afin de réduire leurs coûts de conformité (79).

Même lorsque le Cybersecurity Act définit un schéma de certification volontaire harmonisé, certains États membres peuvent imposer des obligations supplémentaires pour les dispositifs médicaux connectés (59). Par exemple :

- Obligation d'un certificat de cybersécurité pour toute mise sur le marché, alors que d'autres pays se limitent à une approche facultative.
- Exigence de tests complémentaires ou de rapports périodiques pour les dispositifs déjà certifiés au niveau européen.

En l'absence d'une harmonisation plus poussée, le marché unique souffre d'une fragmentation pouvant engendrer des coûts disproportionnés et retarder l'accès rapide aux innovations pour les professionnels de santé et les patients (63).

2.3.1.2 Chevauchement des réglementations et duplication des exigences

Le paysage réglementaire européen associe aujourd'hui des cadres verticaux (MDR/IVDR) et horizontaux (Cybersecurity Act, directive NIS 2), sans toujours préciser leurs interactions. Cette superposition génère des zones d'ombre pour l'application aux dispositifs médicaux et complique la conformité pour les fabricants (63).

L'Union Européenne manque d'éclaircissements sur l'applicabilité des différents règlements et directives pour les dispositifs médicaux. Cela se traduit par différentes observations (63) :

- L'absence d'orientation unique fournit par l'Union européenne qui n'a pas publié de guide unifiant MDR, Cybersecurity Act et NIS 2 pour les dispositifs médicaux par exemple.
- Les redondances et divergences avec des exigences de documentation, de tests, de notification et de certification qui peuvent se recouper, entraînant des démarches parallèles et coûteuses.

La juxtaposition de plusieurs cadres législatifs conduit à des obligations de notification redondantes et génératrices de charge pour les fabricants et les établissements de santé.

La notification d'incidents est un exemple de duplication des exigences. Dans le cadre des dispositifs médicaux, trois cadres juridiques différents s'appliquent à la notification d'incidents

1. **Règlement (UE) 2017/745 (MDR)** (7):
   - Exige la notification des incidents sérieux impliquant un dispositif médical.
   - Autorité destinataire : l'agence nationale compétente (en France, l'ANSM).
2. **Règlement général sur la protection des données (RGPD)** (58):
   - Implique la notification des violations de données à caractère personnel sous 72 heures si risque pour les droits et libertés des individus.
   - Autorité destinataire : l'autorité de contrôle (en France, la CNIL).
3. **Directive NIS 2** (60):
   - Oblige les entités de gestion d'infrastructures critiques (dont les hôpitaux et certains fournisseurs de dispositifs médicaux connectés) à signaler tout incident remettant en cause la continuité ou la confidentialité des services essentiels.

- Autorité destinataire : l'autorité nationale de cybersécurité ou le CSIRT (Computer Security Incident Response Teams) compétent (en France, l'ANSSI).

Cette situation peut amener à plusieurs conséquences (63) :

- **Définitions et seuils divergents** :
  Chaque texte fixe ses propres critères de « sévérité » ou « volume » déclenchant l'obligation de notifier, sans alignement sémantique.
- **Procédures et délais hétérogènes** :
  Les formulaires, canaux et délais (2 jours, 10 jours, 72 heures, etc.) diffèrent, contraignant les fabricants à maintenir plusieurs workflows parallèles.
- **Multiplication des interlocuteurs** :
  L'obligation de notifier trois autorités distinctes multiplie les points de contact et accroît le risque d'erreur ou d'oubli.
- **Charge administrative et coûts** :
  La préparation de dossiers spécifiques, la coordination interne entre équipes vigilance, cyber et protection des données, et le suivi des retours de trois administrations pèsent lourdement, notamment pour les PME (Petites et Moyennes Entreprises).

Il n'est mentionné ici qu'un exemple dans le cadre européen mais les données de santé et les chaînes d'approvisionnement étant globales, les fabricants doivent souvent composer aussi avec les lignes directrices de la US FDA, les règlements chinois (NMPA), canadiens (Health Canada) ou japonais (PMDA) aux exigences parfois contradictoires.

L'absence de consensus mondial sur les schémas de certification, le SBOM ou le cycle de vie des correctifs pèse sur l'agilité des fabricants et peut retarder la mise à jour des dispositifs face à des menaces transfrontalière (47).

Finalement, toutes les exigences en matière d'évaluation des risques de cybersécurité, de conception sécurisée, de surveillance post-commercialisation et de mises à jour régulières peuvent représenter une charge importante pour les fabricants, en particulier pour les petites entreprises ou celles dont les ressources sont limitées.

2.3.2 Limitation des ressources

Les établissements de santé allouent encore une part réduite de leur budget informatique à la cybersécurité, malgré l'augmentation constante des cyberattaques

qui compromettent directement la continuité et la qualité des soins aux patients (32). Cette sous allocation renforce la vulnérabilité des systèmes d'information hospitaliers et retarde la mise en place de mesures de protection indispensables (29).

Le financement dédié à la cybersécurité représente généralement seulement 1 à 2 % du budget annuel des technologies de l'information dans les structures de santé, contre 4 à 10 % dans d'autres secteurs économiques (80).

Ce déséquilibre se traduit par (81) :

- Un manque de moyens pour assurer les mises à jour régulières et les correctifs de sécurité.
- Des outils de détection d'intrusions et de gestion des vulnérabilités obsolètes ou insuffisants.
- Une incapacité à financer des audits externes et des tests de pénétration poussés.

Les retours d'expérience des acteurs de santé soulignent un déficit de compétences internes en cybersécurité, conséquence du coût élevé de ces profils, de la complexité réglementaire et de l'évolution rapide des tactiques d'attaque. En 2017, une étude estimait à 1,8 million le nombre de spécialistes en sécurité de l'information manquants dans le secteur de la santé à l'horizon 2022 (82). Cette pénurie oblige les hôpitaux à recourir à des prestataires externes dont les tarifs dépassent souvent leurs capacités financières (80).

Le personnel médical consacre l'essentiel de son temps aux activités cliniques, ne laissant que peu de marge pour la formation ou la sensibilisation aux bonnes pratiques de cybersécurité. Par conséquent, des solutions au quotidien, telles qu'Office 365, ne sont pas systématiquement déployées, alors même qu'elles offrent des mécanismes de protection intégrés plus robustes que les logiciels traditionnels.

2.3.3 Manque d'expertise et de sensibilisation en matière de cybersécurité

Le facteur humain constitue l'un des maillons les plus vulnérables de la chaîne de cybersécurité en santé. De nombreuses attaques exploitent des erreurs quotidiennes telles que l'hameçonnage, l'utilisation de mots de passe faibles ou le partage inapproprié d'informations sensibles.

Ces incidents soulignent la nécessité de programmes de formation et de sensibilisation adaptés à la diversité des profils—des infirmiers aux techniciens biomédicaux—pour renforcer la posture globale de sécurité.

Toutefois, la mise en œuvre de ces programmes se heurte à plusieurs difficultés (49) :

- Diversité des rôles et niveaux d'expertise techniques au sein du personnel soignant.
- Charge de travail élevée, limitant le temps disponible pour la formation continue.
- Priorité clinique souvent perçue comme antinomique avec les exigences de cybersécurité.

Le secteur de la santé est le seul pour lequel la principale source de violation de données provient de l'interne. En 2017, au Royaume-Uni, 46 % des fuites étaient imputables au comportement des employés (clics sur liens infectés, négligence ou abus d'accès) (2).

La culture centrée sur le patient favorise des pratiques compromises, comme le partage généralisé de mots de passe, jugé plus "efficace" pour les soins en urgence mais préjudiciable à la sécurité des systèmes (80).

Le personnel médical demeure peu sensibilisé aux menaces informatiques et aux meilleures pratiques d'utilisation des réseaux hospitaliers, ce qui peut freiner l'adoption des outils de sécurité. De plus, déléguer entièrement la cybersécurité aux services informatiques ne suffit pas : il est crucial d'instaurer des solutions « security by design » qui combinent robustesse technique et simplicité d'usage pour les soignants (35).

Il parait alors évident que la cybersécurité des dispositifs médicaux est une responsabilité partagée entre les fabricants de dispositifs et les prestataires de soins de santé. Les deux parties doivent comprendre leur rôle et leurs responsabilités et collaborer étroitement afin de surveiller, évaluer, atténuer, les risques et menaces potentiels en matière de cybersécurité tout au long du cycle de vie du dispositif.

PARTIE 3 : BONNES PRATIQUES POUR LES ACTEURS DU SECTEUR DE LA SANTÉ

La cybersécurité constitue une démarche continue et évolutive. Aucun dispositif, aucune infrastructure ni aucun processus ne peut garantir une immunité totale face aux menaces. Toutefois, l'adoption d'un ensemble cohérent de mesures techniques, organisationnelles et humaines permet de réduire significativement le risque d'incident, d'en limiter l'impact sur la sécurité des patients et d'assurer la continuité des soins.

La présente partie ne propose pas une liste prescriptive et exhaustive de contrôles à mettre en œuvre. Elle présente plutôt une sélection de bonnes pratiques structurées selon trois niveaux d'acteurs : les fabricants de dispositifs médicaux, les organisations, ainsi que le personnel.

3.1 BONNES PRATIQUES POUR SÉCURISER UN DISPOSITIF MÉDICAL

La cybersécurité d'un dispositif médical relève en grande partie de la responsabilité du fabricant. Toute démarche rigoureuse s'appuie sur une approche « Secure by Design » qui commence dès la phase de conception et se prolonge jusqu'aux activités de surveillance post-commercialisation. Cette approche assure une résilience face à l'évolution rapide des vulnérabilités et des menaces.

Les fabricants de dispositifs médicaux doivent clairement documenter et résumer leurs activités liées à la cybersécurité. En fonction de la classe de risque du dispositif, l'organisme notifié peut exiger la documentation pour évaluer le dispositif médical avant sa mise sur le marché ou l'exiger au cours de la phase post-commercialisation du cycle de vie du produit (53).

Les fabricants doivent documenter et centraliser l'ensemble de ces activités sous la forme d'un dossier de cybersécurité produit. Selon la classe de risque du dispositif et les exigences du Règlement (UE) 2017/745 (MDR), l'organisme notifié peut solliciter cette documentation dans le cadre de l'évaluation pré-commercialisation ou à tout moment pendant la phase post-market (surveillance après la mise sur le marché) (7).

3.1.1 La gestion de risques comme clé de voute

La cybersécurité des dispositifs médicaux s'inscrit dans une démarche de gestion des risques abordée notamment dans la norme ISO 14971 :2019 ou encore aux principes énoncés par l'IMDRF (International Medical Device Regulators Forum). Cette approche impose une prise en compte systématique des dangers, des menaces et

des vulnérabilités à chaque étape du cycle de vie du produit, de la conception à la surveillance post-commercialisation (71).

Dans le vocabulaire normatif, on distingue notamment (71):

- **Risque** : Combinaison de la gravité d'un dommage au patient, ou à l'utilisateur ou à l'environnement, et de la fréquence de ce dommage.
- **Danger** : source potentielle de préjudice pour le patient ou l'utilisateur (vulnérabilités informatiques).
- **Situation dangereuse** : combinaison de circonstances dans lesquelles le patient ou l'utilisateur est exposé au danger (attaque informatique).

Dans le domaine de la cybersécurité, l'ANSM souligne l'importance d'évaluer les risques selon quatre critères prioritaires (83):

Critère	Définition
Disponibilité	Faculté d'un système à rendre un service (par exemple, l'accès à une information ou une ressource) dans des conditions prédéterminées d'exploitation et de maintenance, en respectant des contraintes de performance et de temps de réponse.
Intégrité	Propriété d'un système ou d'une information de ne pas être modifiés, altérés ou supprimés de façon illégitime.
Confidentialité	Propriété d'une information de n'être connue que des personnes, entités ou processus dûment autorisés à la connaître : restriction des accès en lecture.
Auditabilité	Faculté d'un système à conserver les traces des opérations effectuées sur les biens à protéger et à garantir l'exploitabilité de ces traces à des fins de contrôle ou d'investigation

La gestion des risques doit être continue et documentée. Tout risque de cybersécurité susceptible d'altérer la sécurité ou les performances essentielles du dispositif, d'entraver les opérations cliniques ou de fausser un diagnostic doit être évalué et traité.

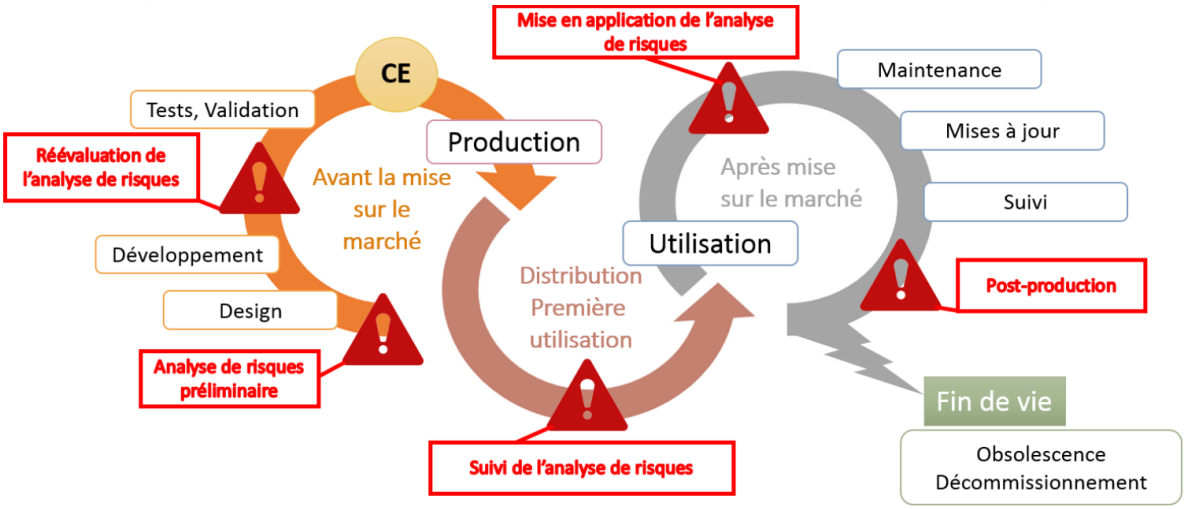


***Figure 16** : Analyse des risques en cybersécurité*

Le processus comprend cinq étapes (71) :

1. Identifier les dangers et les vulnérabilités associées.
2. Estimer le risque initial (fréquence × gravité).
3. Mettre en œuvre des mesures de maîtrise pour réduire les risques à un niveau acceptable.
4. Vérifier et valider l'efficacité des mesures par des indicateurs et des tests de vulnérabilité.
5. Surveiller les risques résiduels en post-market et mettre à jour l'analyse à partir des retours terrain.

L'analyse de risque doit porter plus particulièrement sur l'estimation (71) :

- De l'exploitabilité de la vulnérabilité : facilité d'accès, existence d'outils de compromission, compétences nécessaires.
- De la gravité du préjudice potentiel : impact sur la sécurité du patient, sur la performance essentielle du dispositif ou sur la fiabilité des données cliniques.

Pour structurer l'analyse, l'ANSM recommande d'adapter la méthode EBIOS Risk Manager (ANSSI) au contexte des dispositifs médicaux ; cette démarche comporte cinq phases clés (83):

1. **Contexte** : définition des finalités cliniques, des interfaces et de l'environnement d'utilisation du DM.
2. **Étude des événements redoutés** : identification des conséquences critiques sur les patients ou sur l'infrastructure.

3. **Étude des scénarii de menace** : cartographie des sources potentielles d'attaques (interne/externe), techniques (en faisant par exemple du reverse-engineering) et motivations (malveillance, sabotage).
4. **Évaluation des risques** : estimation de la probabilité d'exploitation et de la gravité du préjudice pour chaque scénario.
5. **Détermination des exigences de sécurité** : formulation de mesures de prévention, de détection, de réponse et de réparation afin de ramener chaque risque à un niveau acceptable.

Pour compléter la gestion des risques, la norme ISO 13485 :2016 recommande de documenter dans le Système de Management de la Qualité du fabricant (84):

- Un plan de gestion des risques formalisé et documenté.
- Des revues périodiques et des comités multidisciplinaires.
- La traçabilité de toutes les décisions (y compris celles liées à la cybersécurité).
- La mise à jour continue de l'analyse en post-market.

Une documentation précise est exigée par les organismes notifiés et les autorités réglementaires dans le dossier technique du produit (MDR 2017/745). Elle garantit la traçabilité des décisions et la transparence des choix dans l'objectif de maîtrise des risques.

3.1.2 Les bonnes pratiques avant commercialisation

Le fabricant d'un dispositif médical doit, avant toute mise sur le marché, démontrer que son produit intègre des mesures de cybersécurité proportionnées aux risques cliniques et réglementaires.

Trois axes structurent cette phase (53) :

- Implémenter une stratégie de protection dès la conception (security by design).
- Conduire un programme d'essais et de vérifications de sécurité (security testing).
- Mettre à disposition des utilisateurs une documentation claire et exhaustive (transparence & support).

3.1.2.1 Implémentation d'une stratégie de protection dès la conception (security by design)

Les exigences techniques, réglementaires et éthiques convergent : la cybersécurité doit être inscrite dans l'ADN du produit. Plus elle est prise en compte tôt, plus le coût de remédiation ultérieure diminue et plus la sécurité clinique est robuste.

Pour cela, le point de départ est le suivant (83):

1. **Etablir la liste des biens critiques à protéger** :
    - Dans le cas d'un DM en tant que cible de l'attaque, ce sont ceux, qui, s'ils sont attaqués, peuvent avoir un impact négatif sur la prise en charge du patient.
    - Dans le cas d'un DM comme point d'entrée, ce sont ceux qui vont conduire à altérer le fonctionnement de l'infrastructure.
2. **Définir un objectif de sécurité** pour chacun des biens en termes d'intégrité, confidentialité, disponibilité et traçabilité et les fonctions de sécurité à implémenter pour atteindre cet objectif de sécurité.

Une fois les biens critiques identifiés, le fabricant doit définir les vulnérabilités potentielles, les dangers et les risques associés. Cette étape permet d'avoir une vision globale de l'ensemble des protections à mettre à place (cf. section 3.1.1).

Ci-dessous est présentée une liste non-exhaustive de recommandations auxquelles devraient penser les fabricants lors de la phase de conception et développement (53,83):

Catégorie	Recommandations
Dispositions générales	- Intégrer les risques liés aux outils logiciels (télémaintenance, gestion des licences) dans l'analyse de risque. - Proscrire la sécurité par l'obscurité et mettre en place un contrôle transparent et documenté. - Réduire la surface d'attaque en ne conservant que les composants et données strictement nécessaires. - Documenter les exigences de sécurité dans la conception logicielle. - Adopter une politique formalisée d'achats, de gestion de composants et de sous-traitance.

	- Prévoir dès la conception des moyens de remédiation (droits d'accès minimaux, badge d'authentification, restriction du compte administrateur)
Contrôle des accès	- Définir et documenter clairement les rôles et privilèges des utilisateurs en fonction de leurs fonctions.
Gestion des authentifications	- Imposer une authentification préalable pour tout accès aux données, aux composants logiciels et aux communications (utilisateur, logiciel, message).
Environnement d'utilisation	- Se conformer à l'état de l'art en utilisant des versions à jour de tous les composants. - Interdire le maintien d'un système hôte obsolète au motif d'une incompatibilité et définir explicitement les compatibilités logiciel/matériel.
Traçabilité et journalisation	- Intégrer une fonction de journalisation locale des accès et des événements à impact critique. - Documenter les modalités de journalisation : capacités de stockage, stratégies de sauvegarde et d'exploitation des journaux.
Surveillance en exploitation	- Vérifier dès la conception l'état de l'art en cybersécurité pour identifier les vulnérabilités connues. - Implémenter une auto-vérification d'intégrité et une alerte locale sur tout événement critique (par exemple, contrôle du code au démarrage).
Fonctionnement en mode dégradé	- Prévoir un mode dégradé sécurisé pour assurer la reprise des données et, le cas échéant, la continuité de service (notamment pour les dispositifs portés ou implantés) en cas de détection d'attaque ou de ses effets.
Choix des règles de programmation	- Appliquer des règles de codage vérifiées automatiquement par inspection continue pour détecter les vulnérabilités. - Assurer l'intégrité du code source et la traçabilité des modifications.

Méthodes de vérification	- Spécifier les fonctions logicielles attendues dans la documentation. - Soumettre le dispositif à un processus d'évaluation de la sécurité.

3.1.2.2 Programme d'essais et de vérifications de sécurité (security testing)

L'exécution d'un programme d'essais de sécurité (security testing) est essentielle pour identifier les vulnérabilités, démontrer la robustesse du dispositif médical, et garantir la conformité aux exigences réglementaires et normatives.

Ce programme doit être planifié dès les premières phases de conception et poursuivi jusqu'au déploiement et au suivi post-commercialisation.

Les objectifs sont les suivants :

- Détecter les failles techniques exploitables (bugs, erreurs de configuration, vulnérabilités logicielles ou matérielles).
- Évaluer la résistance du DM face aux scénarios d'attaque réalistes.
- Vérifier le bon fonctionnement des mesures de protection implémentées.
- Documenter les résultats pour les audits qualité et réglementaires.

Il existe différents types d'essais que les fabricants peuvent mettre en place :

Type d'essai	Description
Analyse statique (SAST) (85)	L'analyse statique de la sécurité des applications consiste à examiner le code source d'une application sans avoir recours à son exécution, dans le but d'identifier les erreurs de programmation ainsi que les vulnérabilités connues. En se concentrant sur la structure interne du logiciel, cette méthode permet de repérer les failles de sécurité dès les premières phases du cycle de développement. Elle offre ainsi aux développeurs l'opportunité de corriger ces défauts de manière précoce, limitant les risques liés à leur exploitation future et réduisant les coûts associés à leur résolution.
Analyse dynamique (DAST) (85)	Les tests d'analyse dynamique visent à examiner le comportement d'un système ou d'une application en

	phase d'exécution lorsqu'il est exposé à des entrées malveillantes. Contrairement à l'analyse statique du code (SAST), cette approche ne requiert aucun accès au code source. Elle s'applique directement sur des applications opérationnelles, en simulant des scénarios d'attaque réalistes afin d'évaluer concrètement leur niveau de sécurité. Le DAST offre ainsi une vision globale de la résilience de l'application face aux menaces externes.
Tests d'intrusion (Pentest) (86)	L'analyse d'intrusion, également désignée par le terme anglais penetration testing, constitue une démarche méthodique visant à reproduire une attaque informatique dans le but d'évaluer la résilience d'un système ou d'un réseau face aux menaces potentielles. Ce processus repose sur l'intervention de professionnels en cybersécurité, souvent appelés hackers éthiques, qui s'emploient à déjouer les dispositifs de protection existants afin d'identifier les vulnérabilités exploitables. L'objectif fondamental est de détecter les points faibles avant qu'ils ne soient exploités par des acteurs malveillants, contribuant ainsi au renforcement global de la posture sécuritaire de l'organisation ciblée.
Fuzzing (87)	Le fuzzing, ou test de robustesse automatisé, constitue une méthode d'évaluation en cybersécurité visant à identifier les vulnérabilités potentielles d'un logiciel en l'exposant à une multitude d'entrées aléatoires, imprévues ou volontairement malformées. En analysant la manière dont le programme réagit à ces sollicitations atypiques, cette technique permet de mettre en évidence des erreurs de codage ainsi que des failles de sécurité susceptibles d'être exploitées. Bien que le fuzzing soit parfois utilisé par des attaquants dans une optique malveillante, il demeure un outil essentiel pour les professionnels de la sécurité, qui s'en servent afin de détecter proactivement les failles et de les corriger avant qu'elles ne soient compromises.

Le plan de test doit être basé sur l'analyse des risques et doit être motivé par une menace identifiée lors de la modélisation décrite au chapitre 3.1.1. L'objectif étant de se rapprocher le plus possible des conditions réelles d'utilisation.

L'exploitation des résultats de ces tests doit permettre la remédiation des vulnérabilités critiques avant commercialisation et la révision des paramètres de configuration par défaut si des risques sont identifiés.

3.1.2.3 Documentation claire et exhaustive (transparence & support)

La transparence dans la documentation technique constitue une exigence majeure en matière de cybersécurité pour les dispositifs médicaux. Elle vise à garantir la traçabilité des composants, à faciliter l'intégration au sein des infrastructures hospitalières et à permettre une gestion proactive des risques en post-commercialisation.

Le fabricant doit fournir, entre autres, une liste exhaustive des éléments constituant le dispositif, comprenant :

- **Composants matériels** : processeurs, capteurs, modules de communication (ex. : Wi-Fi, Bluetooth, 4G), puces de sécurité, etc.
- **Composants logiciels** : Système d'exploitation (nom, version, correctifs installés), Applications embarquées, Protocoles de communication utilisés.
- **Software Bill of Materials (SBOM)** : Inventaire standardisé des dépendances logicielles.
- **Manufacturer Disclosure Statement for Medical Device Security** (MDS2): Déclaration volontaire utilisée par les fabricants de dispositifs médicaux pour fournir des informations détaillées sur la sécurité de leurs produits.

Ces informations doivent être accessibles de manière sécurisée à l'utilisateur final (établissement de santé ou professionnel). Cette approche documentaire exhaustive et structurée permet non seulement de répondre aux exigences réglementaires, mais aussi d'instaurer un climat de confiance entre le fabricant et les acteurs de la santé, tout en renforçant la résilience du dispositif tout au long de son cycle de vie.

3.1.3 Les bonnes pratiques après commercialisation

La gestion sécuritaire des dispositifs médicaux ne saurait s'arrêter à leur mise sur le marché : elle doit impérativement se prolonger jusqu'à la date de fin de vie (End of Life, EOL) définie par le fabricant au regard des considérations de cybersécurité. Cette échéance marque le moment à partir duquel la capacité du fabricant à assurer une

prise en charge exhaustive des menaces numériques se réduit de manière significative (53).

De plus, les technologies évoluant sans cesse, il n'est pas possible d'identifier dès le départ l'ensemble des vulnérabilités d'un dispositif médical tout au long de son cycle de vie. Un suivi post-commercialisation de l'apparition de nouvelles failles est une démarche proactive indispensable afin de pouvoir agir en conséquence et réduire le risque patient.

Le tableau ci-après synthétise les principales actions (liste non-exhaustive) à mener par le fabricant, de la mise sur le marché jusqu'à la date de fin de support (EoS), afin d'assurer une cybersécurité continue de ses dispositifs médicaux (53,83):

Catégorie	Recommandations
Veille des vulnérabilités	- Mise en place d'une surveillance active sur les bases de données de vulnérabilités. - Réévaluation périodique de l'analyse de risque intégrant chaque nouvelle vulnérabilité. - Traçabilité de l'identification et du suivi de traitement des vulnérabilités.
Gestion des incidents et actions	- Signalement aux autorités compétentes de tout incident grave ou mesure corrective de sécurité (Article 87 du MDR). - Analyse exhaustive des incidents et retours d'expérience des utilisateurs. - Mise en place d'un programme de divulgation des vulnérabilités pour faciliter la coopération.
Mises à jour et maintenance	- Développement et distribution de correctifs sécurisés avant la date EoS. - Fonction de mise à jour logicielle sécurisée garantissant authenticité et intégrité du patch. - Envoi d'alertes aux utilisateurs en cas de retrait produit ou de maintenance nécessitant rappel ou mise à jour corrective.
Retour d'expérience et amélioration	- Collecte structurée des incidents et des indicateurs clés (temps de correction, nombre de vulnérabilités traitées). - Publication d'un bilan annuel de cybersécurité.

	- Intégration des leçons apprises dans la conception des prochaines générations de dispositifs.

En amont de l'échéance EoL (End of Life – Fin de Vie), le fabricant se doit d'informer clairement les utilisateurs des modalités d'assistance résiduelle envisageables au-delà de cette date. Cette communication inclut notamment la date de fin de support (End of Support, EoS), à partir de laquelle toute responsabilité en matière de cybersécurité cesse d'être assumée par le fabricant (53).

À présent, il convient d'élargir le focus technique et de considérer la sécurité des dispositifs médicaux comme un élément indissociable d'une stratégie organisationnelle globale. Si les mesures de protection sont indispensables, leur efficacité dépend largement du cadre institutionnel dans lequel elles s'inscrivent. La section suivante présente les bonnes pratiques à adopter au niveau des établissements de santé et des fabricants, afin d'instaurer une gouvernance, des processus et une culture de cybersécurité cohérents et durables.

3.2 BONNES PRATIQUES À DESTINATION DES ORGANISATIONS

Dans le domaine de la cybersécurité appliquée aux organisations, la responsabilité ne repose pas uniquement sur les services informatiques. Bien que leur rôle technique soit incontournable, l'implication active de l'ensemble de l'organisation et plus particulièrement, de la direction générale est désormais une condition nécessaire à la mise en œuvre de stratégies de sécurité efficaces. En effet, c'est elle qui impulse les politiques de gouvernance, alloue les ressources, fixe les priorités et promeut une culture organisationnelle axée sur la sécurité.

Cette responsabilité renforcée s'inscrit notamment dans le cadre des réglementations européennes récentes telles que la directive NIS-2, qui élargit les obligations des dirigeants en matière de gestion des risques et de continuité d'activité face aux menaces numériques (60). Quelle que soit la taille, le chiffre d'affaires ou le domaine d'activité de l'établissement, certaines bonnes pratiques peuvent et doivent être mises en œuvre afin de structurer une approche proactive et durable de la cybersécurité.

Les priorités pour les organisations peuvent se structurer autour des axes suivants (88) :

- Identification et compréhension des vulnérabilités organisationnelles.
- Sensibilisation continue des collaborateurs aux risques cyber.

- Préparation à la gestion d'une crise cyber et à la réponse aux incidents.

3.2.1 Comprendre les vulnérabilités de son organisation

La connaissance fine des vulnérabilités est la première étape vers une posture de cybersécurité mature. Les organisations doivent procéder à des analyses de risques régulières, centrées sur les processus internes, les outils déployés, ainsi que l'infrastructure globale (88). Cette démarche s'apparente à l'analyse de risques réalisée pour les dispositifs médicaux mais s'attache ici à la sécurité de l'organisation elle-même (77).

- **Evaluations de vulnérabilité** :

De la même façon qu'évoqué au chapitre 3.1.2.2, Il est impératif pour les organisations de réaliser des évaluations techniques récurrentes, incluant des tests de pénétration, des analyses de configuration, des audits de sécurité et des simulations d'attaques ciblées (8). Ces exercices permettent d'anticiper les stratégies d'exploitation utilisées par des attaquants, d'identifier des points faibles dans les architectures numériques, et d'ajuster les dispositifs de protection en conséquence (48).

- **Analyse des vecteurs d'attaques potentielles** :

Les évaluations doivent intégrer l'ensemble des éléments connectés au système d'information : serveurs, postes de travail, logiciels métiers, dispositifs médicaux numériques, objets connectés, solutions en cloud et outils tiers (88). La diversité et la complexité des interconnexions multiplient les risques d'entrée. Ainsi, chaque technologie déployée doit faire l'objet d'un examen rigoureux (48).

- **Exigence auprès des fournisseurs et sous-traitants** :

La sécurité de la chaîne d'approvisionnement numérique devient critique. Les directions doivent exiger des garanties en matière de cybersécurité de la part des fournisseurs de dispositifs médicaux et de logiciels (88). Une politique de vérification des tiers et de contractualisation sécurisée devrait être instaurée (48).

- **Documentation et amélioration continue** :

Les résultats des évaluations doivent être documentés, analysés et intégrés dans les processus de gestion des risques (88). Ils servent de base à une stratégie d'amélioration continue, incluant la formation des équipes, la révision des politiques de sécurité, et la mise en œuvre de mesures correctives (49).

En maîtrisant ces principes, les organisations disposent d'une base solide pour prioriser les actions et anticiper l'évolution du paysage des menaces. La section suivante détaillera les méthodes de sensibilisation continue des collaborateurs aux risques en cybersécurité.

3.2.2 Préparer ses employés : l'importance des programmes de sensibilisation

Dans le secteur de la santé, un simple clic sur un lien malveillant peut compromettre l'ensemble des dossiers patients et paralyser les activités cliniques. C'est pourquoi l'élaboration et le déploiement d'un programme de sensibilisation solide doivent devenir une priorité (32).

Objectifs des programmes de sensibilisation (45) :

- Renforcer la vigilance face aux techniques d'hameçonnage.
- Garantir l'usage de mots de passe robustes et la gestion sécurisée des identifiants.
- Diffuser les procédures de traitement et de partage des données de santé.
- Préparer le personnel à réagir efficacement lors d'une cyberattaque ou d'une urgence sanitaire concomitante.

Contenus et méthodes pédagogiques (88):

- Sessions de formation régulières avec par exemple des exercices de reconnaissance des tentatives d'hameçonnage et d'ingénierie sociale.
- Formation interactive à la création et à la gestion de mots de passe.
- Ateliers pratiques sur le respect des procédures de sauvegarde et de restauration des données.
- Exercices de simulation de crise. Simulations de fausses tentatives d'hameçonnage pour évaluer la réactivité et ajuster les contenus pédagogiques.
- Modules e-learning accessibles en continu et adaptés aux spécificités métiers.

Extension de la culture de cybersécurité (55):

MedTech Europe recommande d'étendre la sensibilisation aux patients et au grand public afin d'ancrer une prise de conscience sociétale de long terme. À titre d'exemple, l'intégration de modules élémentaires de cybersécurité dans les programmes scolaires pourrait contribuer à des citoyens mieux informés et plus résilients face aux risques numériques.

Il faut donc aller au-delà de la simple sensibilisation mais chercher à instaurer une « culture de la cybersécurité ». Les protocoles et les normes établis doivent être mis en œuvre de manière adéquate par tous les employés et il est nécessaire de vérifier en permanence la mise en œuvre des bonnes pratiques de cyber-hygiène tout en simulant les circonstances réelles des cyberattaques.

En alignant formation continue, évaluation et pilotage, les organisations peuvent transformer leurs collaborateurs en premiers remparts contre les menaces numériques.

3.2.3 Préparer et renforcer son organisation

3.2.3.1 Ressources critiques et sauvegardes régulières

Dans toute infrastructure hospitalière, il ne s'agit pas de se demander « si » une cyberattaque survient, mais plutôt « quand ». Une organisation solidement préparée identifie d'abord l'ensemble des ressources et les classe selon leur criticité, afin d'adapter la stratégie de sauvegarde à l'impact potentiel sur les soins et la confidentialité des données (35).

Les sauvegardes sécurisées et régulières sont nécessaires notamment pour les ressources critiques contenant des informations confidentielles (8). Les ressources critiques pourraient être les dossiers patients numérisés ou les dispositifs médicaux connectés. Alors que des ressources moins importantes seraient les applications de facturation ou des procédures obsolètes.

Sur la base de cette évaluation, une stratégie de sauvegarde est définie : combiner sauvegardes complètes, incrémentales et différentielles pour garantir une couverture adaptée à chaque typologie de données et optimiser le rapport rapidité de restauration / volume stocké (89).

Ces sauvegardes permettent de maintenir la résilience du système et être en mesure de récupérer rapidement les données en cas d'attaque (4).

3.2.3.2 Mise en place d'une « défense en profondeur »

La défense en profondeur consiste à superposer, de manière coordonnée, plusieurs couches de protection afin que la faille d'un dispositif n'entraîne pas la compromission du système dans son ensemble (90).

Chaque barrière — qu'elle soit technique, organisationnelle ou humaine — vient ralentir l'attaquant, réduire la surface d'exposition et offrir un temps de réaction pour détecter et contenir l'incident (88).

***Figure 17** : Modèle de défense en profondeur (85)*

Certains principes clés de la mise en place d'une défense en profondeur sont listés ci-dessous (88,90):

- **Principe du moindre privilège** : chaque utilisateur, chaque process et chaque équipement ne dispose que des droits strictement nécessaires.
- **Séparation des tâches** : éviter qu'une même entité ne puisse initier, valider et exécuter une transaction critique.
- **Redondance et diversité** : recourir à des solutions complémentaires (éditeurs, technologies, modes d'authentification) pour éviter le point de défaillance unique.
- **Surveillance continue et réponse rapide** : collecte et corrélation des journaux de sécurité. Mise en place de procédures d'escalade clairement définies.

Concrètement les couches et mesures qui peuvent être recommandées sont les suivantes (88,90):

- **Contrôles d'identité et d'accès** :
  - Authentification multifactorielle (MFA) ou biométrie pour tous les accès à privilèges.
  - Gestion centralisée des identités et politique de mots de passe robustes.
- **Protection du périmètre et segmentation réseau** :
  - Firewall nouvelle génération et systèmes de prévention d'intrusion.
  - Segmentation stricte des réseaux cliniques, administratifs et de recherche.
- **Sécurité des postes de travail et des serveurs** :
  - Solutions antivirus couplées à une mise à jour automatisée des signatures et des correctifs.
  - Verrouillage des ports USB et gestion des médias amovibles.
- **Sécurité des applications et des dispositifs médicaux** :
  - Tests de vulnérabilité et analyses de code à chaque mise à jour logicielle.
- **Chiffrement et protection des données** :

- Journalisation intégrale des accès aux données de santé et traçabilité conforme au RGPD (58).

La défense en profondeur peut sembler ralentir la productivité en raison de l'augmentation des contrôles de sécurité et peut sembler redondante à première vue.

Cependant, l'application rigoureuse de cette stratégie, depuis la planification stratégique jusqu'à l'exploitation quotidienne, garantit que, même si un attaquant parvient à franchir un périmètre, il rencontrera immédiatement d'autres obstacles. Cette approche est particulièrement adaptée aux environnements de santé, où la protection des données patients, la disponibilité des équipements et la sécurité des dispositifs médicaux sont des enjeux critiques.

La mise en place d'une défense en profondeur instaure un bouclier robuste en combinant contrôles techniques, mesures organisationnelles et vigilance humaine. Toutefois, même la stratégie la plus aboutie ne peut éliminer totalement le risque d'incident ou de compromission.

Il est donc indispensable de préparer l'organisation à continuer ses missions critiques et à se relever rapidement lorsqu'une attaque ou une défaillance survient.

3.2.3.3 Continuité et résilience des activités

La continuité et la résilience des activités visent à garantir que, quel que soit le scénario d'incident, cyberattaque, sinistre informatique ou défaillance majeure, les fonctions cliniques et administratives essentielles restent opérationnelles, ou retrouvent leur capacité de service dans des délais définis. Dans le contexte de la santé, cela signifie préserver l'accès aux dossiers patients, aux dispositifs médicaux critiques et aux systèmes de communication entre professionnels, sans compromettre la sécurité des données ni la qualité des soins.

Exemple de séquence de réponse à une cyberattaque :

1. **Réaction immédiate** :
   - **Détection et confirmation** :
     - Vérifier les alertes et les logs pour confirmer l'anomalie.
     - Catégoriser rapidement la nature de l'attaque (ransomware, malware, compromission interne).
   - **Priorisation** :
     - Estimer l'impact sur les systèmes critiques et la sécurité des données patients.

- Classer l'incident selon un niveau d'urgence défini.

➢ **Activation du plan de réponse** :

- Déclencher la cellule de gestion de crise.
- Mobiliser immédiatement les rôles définis (RSSI, DSI, référents métiers).

➢ **Isolation et préservation** :

- Déconnecter ou segmenter les sous-réseaux impactés (y compris Wi-Fi).
- Bloquer les comptes compromis et appliquer des règles de firewall temporaires.

➢ **Conserver les preuves** :

- Ne pas redémarrer, formater ou modifier les systèmes infectés.
- Réaliser des images forensiques des disques et captures mémoire.
- Documenter chaque action (horodatage, opérateur, outils et commandes utilisées).

2. **Communication et signalement :**

➢ **Communication interne** :

- Alerter les équipes cliniques et administratives des services impactés.
- Diffuser les procédures de repli (dossiers papier, interruptions planifiées).

➢ **Signalement aux autorités** :

- En France : contacter l'ANSSI et la CNIL

➢ **Communication externe** :

- Informer les patients et partenaires (laboratoires, établissements référents) de manière transparente.
- Préparer un communiqué de presse ou FAQ selon la gravité et la visibilité médiatique.

➢ **Coordination avec les expertises externes** :

- Faire appel à un CERT national ou à un prestataire spécialisé pour l'éradication de la menace
- Partager de façon anonymisée les indicateurs de compromission avec d'autres établissements pour anticiper des vagues similaires.

3. **Eradication et restauration** :

- Mettre à jour ou remplacer les systèmes infectés après nettoyage.
- Restaurer les données depuis les sauvegardes sécurisées.
- Valider l'intégrité des données et le bon fonctionnement des applications critiques avant remise en production.

La robustesse des dispositifs techniques et des plans de reprise ne suffit pas à elle seule : la sécurité repose tout autant sur l'appropriation par chaque collaborateur des procédures et réflexes indispensables. C'est pourquoi, après avoir examiné les mécanismes de continuité et de résilience, il convient de se pencher sur les bonnes pratiques à destination du personnel.

3.3 BONNES PRATIQUES À DESTINATION DU PERSONNEL

La sécurité des établissements de santé et des dispositifs médicaux repose avant tout sur l'engagement quotidien du personnel, qu'il soit soignant, technique ou administratif. Cette section propose un ensemble de recommandations pragmatiques visant à renforcer la vigilance, l'hygiène informationnelle et le respect des procédures au sein des équipes.

3.3.1 Reconnaissance et signalement des courriels malveillants

La vigilance face à un courriel reste le premier rempart contre les cyberattaques car il constitue l'outil principal utilisé. Pour détecter les messages suspects et les signaler efficacement, chaque collaborateur doit adopter les comportements suivants :

- **Vérification de l'expéditeur** (48) :

  Il est conseillé de vérifier attentivement l'adresse de l'expéditeur. Il est courant d'usurper le nom d'une organisation en modifiant un seul caractère (par exemple « google.c0m » au lieu de « google.com »). Il s'agit également d'être attentif aux variantes subtiles du domaine interne, comme « @univ-lile.fr » au lieu de « @univ-lille.fr »

- **Suivi des liens** (88) :

  Il est conseillé de considérer tous les liens d'un message comme suspects, passer le curseur sur chaque lien pour afficher discrètement l'URL cible et vérifier qu'elle correspond bien au libellé affiché. Les liens dont le texte ne correspond pas à l'adresse réelle ou qui pointent vers un domaine inconnu doivent être signalés.

- **Analyse des pièces jointes** (88):

Il est conseillé de ne jamais télécharger une pièce jointe sans avoir vérifié son origine. Une méfiance particulière doit être appliquée aux messages exigeant une action immédiate (« Lire ceci immédiatement ») ou provenant d'expéditeurs inconnu.

- **Identification du contenu suspect** (48):

Les cybercriminels jouent sur l'urgence, la peur ou l'appât du gain (« Votre compte sera désactivé… », « Vous avez gagné 100 €… »). Tout message faisant pression pour une action rapide ou promettant un avantage trop alléchant doit éveiller la méfiance de l'utilisateur.

- **Refus des sollicitations d'action immédiate** (48):

Les requêtes pressantes de transmission d'informations sensibles par exemple doivent toujours être validées via un canal interne fiable (appel téléphonique, messagerie instantanée officielle, etc.). En cas de doute, il est recommandé de contacter immédiatement le support informatique ou le responsable sécurité.

Ci-dessous sont exposés deux exemples de courriels à caractère suspects :

Exemple 1 :

De : contact@univ-**lile**.fr
Objet : Invitation à valider votre nouvelle session
Cher(e) collègue,
Vous avez été inscrit(e) à un webinaire interne.
Veuillez ouvrir la pièce jointe "Webinaire.pdf" et confirmer votre présence **avant demain**.
Bien à vous,
Service Formation

Caractères suspects :

1. domaine "univ-lile.fr" (manque un l)
2. pièce jointe inconnue, expéditeur non usuel
3. pression temporelle ("avant demain")

Exemple 2 :

De : support@hopita**1**-centre.fr
À : it-department@hopital-centre.fr
Objet : [**URGENT**] Mise à jour critique du logiciel DMP
Bonjour,

Une vulnérabilité critique (CVE-2025-1234) a été détectée dans notre solution de Dossier Médical Partagé (DMP). Pour garantir la confidentialité des données patients, veuillez télécharger et installer le patch joint **dans l'heure qui suit**.
Pièce jointe : **Patch_DMP.exe**
En cas de difficulté, contactez le support au +33 1 23 45 67 89.
Cordialement,
Service Sécurité Informatique – Hôpital Centre

Caractères suspects :
1. expéditeur « hopita1-centre.fr » avec un « 1 » à la place du « l »
2. pression temporelle excessive (« dans l'heure qui suit »)
3. pièce jointe .exe inattendue pour une mise à jour médicale
4. absence de lien officiel ou de portail interne
5. coordonnées génériques, sans signature formelle ni logo vérifiable

En cas de réception d'un courriel suspect, la procédure interne de remontée des incidents doit être utilisée pour que l'équipe de sécurité puisse analyser et bloquer la menace.

La détection et le signalement ne suffisent pas à eux seuls à garantir une cybersécurité solide. Il faut aussi instaurer des habitudes numériques saines et des usages responsables au quotidien.

3.3.2 Hygiène numérique et bonnes pratiques d'usage

Une politique rigoureuse de gestion des mots de passe constitue un pilier fondamental de la sécurité. Il est essentiel de privilégier des mots de passe uniques, longs et alphanumériques, générés idéalement par un gestionnaire de mots de passe.

- **Longueur et complexité** (91):
  - Au **minimum** 12 caractères mêlant lettres, chiffres et symboles. Face à l'ampleur des menaces actuelles, il est cependant recommandé d'allonger ce nombre de caractères le plus possible selon le secteur d'activité.
  - Préférence pour des phrases de passe qui peuvent facilement être mémorisées.
- **Utilisation d'un gestionnaire de mots de passe** (91):
  - Centralisation chiffrée des identifiants.
  - Synchronisation sécurisée entre postes de travail et appareils mobiles.
- **Authentification multifactorielle (MFA)** (91):
  - Activation systématique de la MFA pour tout accès à un compte sensible.
  - Privilégier les applications d'authentification ou les clés physiques plutôt que les SMS.

- **Renouvellement et révocation** (91):
    - Changement périodique en cas de compromission détectée.
    - Suppression rapide des accès en cas de départ ou de changement de poste.

La protection des dispositifs et des connexions réseau participe activement à la prévention des intrusions. Chaque dispositif doit être configuré selon les principes de moindre privilège et relié uniquement à des infrastructures de confiance. Le principe du moindre privilège consiste à limiter les droits d'un utilisateur, d'une application ou d'un service au strict nécessaire pour l'exécution de ses fonctions. Autrement dit, chaque acteur ne dispose que des permissions minimales requises, ce qui réduit considérablement la surface d'attaque et empêche la propagation latérale d'un potentiel cyberattaquant ou logiciel malveillant en cas de compromission de compte

- **Sécurisation des dispositifs** (83):
    - Mises à jour automatiques des systèmes d'exploitation et des applications.
    - Verrouillage automatique par code ou biométrie après période d'inactivité.
    - Installation d'antivirus et de solutions de détection des malwares.
- **Configuration réseau** (83):
    - Recours à un VPN d'entreprise pour toute connexion en dehors du réseau interne.
    - Désactivation du Wi-Fi et du Bluetooth lorsque non utilisés.
    - Limitation du partage de fichiers et impression en réseau à des segments protégés.

La sécurisation des mots de passe, des terminaux et des réseaux constitue le socle d'une bonne hygiène numérique. Cependant, dans un environnement de santé, ces bonnes pratiques doivent être complétées par des mesures spécifiques liées aux dispositifs médicaux connectés, dont la compromission peut mettre en péril la sécurité des patients et la confidentialité des données cliniques.

3.3.3 Sécurité des dispositifs médicaux connectés et protection des données patients

La sécurisation des dispositifs médicaux connectés repose tout autant sur des mesures techniques que sur l'adoption de bonnes pratiques par le personnel. Il est indispensable que chaque collaborateur comprenne les enjeux de confidentialité et

d’intégrité des données patient, afin de limiter les risques de compromission des données.

- **Inventaire et classification** (83):
  Le personnel doit maintenir un registre à jour des dispositifs médicaux connectés déployés (version logicielle, modèle, accès réseau) et les classer selon leur criticité clinique. Cette traçabilité facilite l’évaluation des vulnérabilités et la priorisation des mises à jour.
- **Gestion des accès et authentification** (83):
  Mettre en œuvre des politiques d’accès fondées sur le rôle et l’authentification forte (MFA) pour toute interaction avec les dispositifs. Les identifiants provisoires doivent être supprimés ou remplacés systématiquement dès la mise en service.
  Changer périodiquement les mots de passe et codes PIN des dispositifs selon la politique interne.
  Interdire le partage d’identifiants et recourir à un gestionnaire centralisé si besoin.
- **Mises à jour et correctifs sécurisés** (83):
  Le personnel doit appliquer les correctifs et mises à jour dès leur publication par le fabricant. Un processus formel de validation des mises à jour en environnement de test devra précéder systématiquement le déploiement.
- **Segmentation réseau et pare-feu applicatif** (83):
  Isoler les dispositifs médicaux connectés dans des segments réseau dédiés, protégés par des pares-feux applicatifs et un système de détection d’intrusion.

En complément des recommandations déjà présentées, le personnel doit adopter une approche rigoureuse au quotidien face à l’usage des dispositifs médicaux connectés.

L’objectif est de réduire la surface d’attaque puis de limiter les impacts en cas d’incident. Ces mesures s’intègrent dans le processus clinique sans alourdir les tâches, tout en garantissant un haut niveau de sécurité (83):

- **Vérification systématique des environnements** :
  Avant toute utilisation, s’assurer que le dispositif est branché à l’infrastructure sécurisée (Wi-Fi hospitalier, VLAN dédié). Éviter les points d’accès publics ou les hotspots personnels susceptibles d’être compromis.
- **Limitation des privilèges** :

N’accorder que les droits strictement nécessaires à chaque rôle utilisateur (principe de moindre privilège). Les techniciens de maintenance ne doivent pas utiliser de comptes administrateurs pour des tâches cliniques, et vice versa.

La protection des données de santé repose autant sur des mesures techniques que sur la vigilance humaine. Chaque étape du traitement des données – acquisition, stockage, transmission, affichage – doit intégrer des contrôles adaptés. Le personnel reste le maillon crucial pour prévenir les fuites et garantir la confidentialité.

Afin de garantir une stricte conformité aux principes de protection des données, il convient de limiter la collecte aux seules informations indispensables à la prise en charge. Chaque enregistrement de données doit être anonymisé ou, lorsqu’un pseudonyme suffit, substitué dès que possible avant tout transfert ou archivage, afin de préserver la confidentialité des patients tout au long du cycle de vie des données.

Il est formellement proscrit d’envoyer des comptes rendus contenant des données nominatives par des moyens non approuvés, qu’il s’agisse de courriers électroniques classiques ou de services de stockage grand public non conformes aux exigences réglementaires.

Les opérations de sauvegarde des données patients doivent être planifiées et exécutées régulièrement selon une politique robustement chiffrée, assortie d’un mécanisme de contrôle d’intégrité.

Face à l’essor des dispositifs médicaux connectés et à la complexité croissante des menaces numériques, la sécurité dans le secteur de la santé est une exigence fondamentale. Cette troisième partie a mis en lumière un ensemble de bonnes pratiques essentielles, articulées autour de trois axes complémentaires : la sécurisation des dispositifs médicaux, la préparation des organisations, et la responsabilisation du personnel. De la conception à la post-commercialisation, en passant par la formation des employés et la mise en place de stratégies de résilience, chaque acteur du système de santé a un rôle déterminant à jouer. L’adoption de ces pratiques ne garantit pas l’invulnérabilité, mais elle constitue un socle indispensable pour anticiper les risques et limiter les impacts.

CONCLUSION

Cette thèse d'exercice avait pour vocation de mettre en lumière trois axes principaux. Le premier état de réaliser un état des lieux de la cybersécurité pour les établissements de santé et les fabricants de dispositifs médicaux. Le second était de présenter les exigences réglementaires et normatives qui encadrent les établissements et les fabricants de dispositifs médicaux. Et enfin, le dernier était de présenter une liste non-exhaustive de bonnes pratiques à adopter pour assurer la protection des patients et la résilience des systèmes. L'intention principale consistait à offrir aux non-initiés un ensemble d'outils conceptuels et pratiques leur permettant d'aborder les fondamentaux de la cybersécurité.

Les données bibliographiques recueillies montrent que le secteur de la santé reste une cible privilégiée pour les cybercriminels, en raison de la valeur et de la sensibilité des informations traitées. Les vecteurs d'attaque sont multiples et les conséquences sont lourdes, tant sur le plan opérationnel que financier et réputationnel. La numérisation et l'interconnexion croissante des dispositifs médicaux ont quant à eux élargi la surface d'attaque. Les systèmes d'information hospitaliers, souvent hétérogènes et vieillissants, et les « legacy devices » non sécurisés exposent également les patients et les établissements de santé à des risques majeurs.

L'Union européenne a renforcé son cadre législatif, notamment via le MDR, le RGPD, le Cybersecurity Act et la directive NIS-2, imposant des exigences accrues en matière d'évaluation des risques, de traçabilité et de notification des incidents par exemple. Les normes ISO quant à elles, ont apporté un référentiel technique afin de guider les acteurs de la santé pour l'application de ces exigences. Toutefois, la transposition nationale tardive, la complexité de la juxtaposition des textes et le manque de ressources ou d'expertise en cybersécurité freinent la mise en conformité.

Pour les fabricants de dispositifs médicaux, la cybersécurité doit être intégrée dès la conception par une démarche « security by design » combinant analyses de risques, tests de vulnérabilité et mises à jour planifiées. Dans les établissements de santé, la direction et les services informatiques doivent déployer une vision globale du risque, fondée sur la cartographie des actifs critiques, la segmentation des réseaux et la formation ciblée des équipes, tout en organisant régulièrement des exercices de continuité et en envisageant une cyber assurance. Quant au personnel soignant, adopter une hygiène numérique rigoureuse, une gestion sécurisée des identifiants,

des mises à jour systématiques et chiffrement des échanges s'avèrent indispensable pour préserver la confidentialité des données.

La mise en œuvre d'une approche pluridisciplinaire, associant personnel médical, informaticiens, fabricants de dispositifs médicaux et experts en cybersécurité sera essentiel pour harmoniser les bonnes pratiques et coordonner les réponses urgentes en cas d'attaque. Garantir la confiance des patients exige des investissements continus, la formation et la veille technologique, ainsi qu'une transparence renforcée sur les performances de sécurité. Ces mesures doivent toutefois être appréhendées comme des réflexes incontournables si l'on souhaite préserver l'un des droits essentiels du patient : le secret médical.

Pour aller plus loin, il serait pertinent d'examiner comment l'Intelligence Artificielle et le Machine Learning redéfinissent le paysage de la cybersécurité dans les établissements de santé et chez les fabricants de dispositifs médicaux. L'intégration croissante d'algorithmes de diagnostic et de systèmes d'aide à la décision embarquée soulève leur lot de nouveaux défis.

BIBLIOGRAPHIE

1. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Secteur de la Santé - Etat de la menace informatique [Internet]. 2024 nov [cité 23 mars 2025] p. 45. Disponible sur: https://cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-010.pdf

2. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. Lancet Digit Health. mai 2019;1(1):e10-2.

3. Franceinfo [Internet]. 2024 [cité 23 mars 2025]. Cyberattaque à l'hôpital d'Armentières : 300 000 patients concernés par le vol de données. Disponible sur: https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-a-l-hopital-d-armentieres-300-000-patients-concernes-par-le-vol-de-donnees_6393823.html

4. Coventry, Lynne and Branley, Dawn. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Elsevier [Internet]. [cité 13 avr 2025]; Disponible sur: https://core.ac.uk/reader/157854043?utm_source=linkout

5. Medtronic. Urgent Medical Device Correction | Medtronic [Internet]. 2022 [cité 23 mars 2025]. Disponible sur: https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice19-letter

6. ANNSI. Le CyberDico | ANSSI [Internet]. [cité 6 avr 2025]. Disponible sur: https://cyber.gouv.fr/le-cyberdico#C

7. Règlement - 2017/745 - FR - EUR-Lex [Internet]. [cité 15 août 2025]. Disponible sur: https://eur-lex.europa.eu/eli/reg/2017/745/oj/fra

8. European Union Agency for Cybersecurity. ENISA threat landscape report: health sector (January 2021 to March 2023). [Internet]. LU: Publications Office; 2023 [cité 23 mars 2025]. Disponible sur: https://data.europa.eu/doi/10.2824/163953

9. Agence Numérique en Santé - observatoire-incidents-cybersecurite-sante-2024 [Internet]. [cité 28 août 2025]. Disponible sur: https://esante.gouv.fr/sites/default/files/media_entity/documents/observatoire-incidents-cybersecurite-sante-2024.pdf

10. CrowdStrike.com [Internet]. [cité 30 mai 2025]. Qu'est-ce qu'un vecteur d'attaque? Définition et vulnérabilités | CrowdStrike. Disponible sur: https://www.crowdstrike.com/fr-fr/cybersecurity-101/threat-intelligence/attack-vector/

11. Fortinet [Internet]. [cité 30 mai 2025]. Qu'est-ce qu'une surface d'attaque ? Définition et comment la réduire. Disponible sur: https://www.fortinet.com/fr/resources/cyberglossary/attack-surface.html

12. Cloudfare. Qu'est-ce qu'un vecteur d'attaque ? [Internet]. [cité 30 mai 2025]. Disponible sur: https://www.cloudflare.com/fr-fr/learning/security/glossary/attack-vector/

13. European Union Agency for Cybersecurity. ENISA threat landscape 2022: July 2021 to July 2022. [Internet]. LU: Publications Office; 2022 [cité 30 mai 2025]. Disponible sur: https://data.europa.eu/doi/10.2824/764318

14. CrowdStrike.com [Internet]. [cité 29 mars 2025]. Compromission de données | CrowdStrike. Disponible sur: https://www.crowdstrike.com/fr-fr/cybersecurity-101/cyberattacks/data-breach/

15. Le Figaro [Internet]. 2025 [cité 14 juill 2025]. Accusé d'espionnage sur les vaccins contre le Covid-19 des États-Unis, un hacker chinois arrêté en Italie. Disponible sur: https://www.lefigaro.fr/international/accuse-d-espionnage-sur-les-vaccins-contre-le-covid-19-des-etats-unis-un-hacker-chinois-arrete-en-italie-20250707

16. Les Assises. Hacktiviste | Glossaire Cyber [Internet]. [cité 30 mars 2025]. Disponible sur: https://www.lesassisesdelacybersecurite.com/fr-FR/glossaire-cyber/hacktiviste

17. ANSSI. Dénis de service distribués (DDoS) [Internet]. [cité 30 mars 2025]. Disponible sur: https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos

18. BBC. Wiggins and Froome medical records released by « Russian hackers ». BBC News [Internet]. 15 sept 2016 [cité 7 juin 2025]; Disponible sur: https://www.bbc.com/news/world-37369705

19. Sam Reardon. Pindrop. [cité 30 mars 2025]. Understanding the Threat of Deepfakes in Healthcare. Disponible sur: https://www.pindrop.com/article/threat-deepfakes-in-healthcare/

20. Ponemon Institute. The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking [Internet]. [cité 25 mai 2025]. Disponible sur: https://www.censinet.com/impact-of-ransomware-on-patient-safety-and-value-of-cybersecurity-benchmarking

21. Ponemon Institute. Cyber Insecurity in Healthcare: The cost and Impact on Patient Safety and Care. 2024; Disponible sur: https://assets.turtl.co/customer-assets/tenant%3Dteam/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report-2024%20(1).pdf

22. Claunch D, McMillan M. Determining the right level for your IT security investment. Healthc Financ Manag J Healthc Financ Manag Assoc. mai 2013;67(5):100-3.

23. Anapaya. How cyberattacks hurt business reputation [Internet]. [cité 25 mai 2025]. Disponible sur: https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation

24. WalkMe. Qu'est-ce que la numérisation ? Définition du concept [Internet]. WalkMe™ - Digital Adoption Platform. [cité 6 juill 2025]. Disponible sur: https://www.walkme.com/fr/glossaire/numerisation/

25. Mustafa D, Al-Kfairy M. Editorial: Ethical considerations in electronic data in healthcare. Front Public Health. 15 juill 2024;12:1454323.

26. The Lancet Respiratory Medicine. Digital health: balancing innovation and cybersecurity. Lancet Respir Med. juill 2021;9(7):673.

27. SI-Portail [Internet]. [cité 1 juin 2025]. Découvrir le DMP. Disponible sur: https://www.dmp.fr/ps/je-decouvre

28. Agence du Numérique en Santé [Internet]. [cité 18 mai 2025]. Covidom - Catégorie Application Covid. Disponible sur: https://esante.gouv.fr/virage-numerique/talents-esante/covidom

29. Vukotich G. Healthcare and Cybersecurity: Taking a Zero Trust Approach. Health Serv Insights. 19 juill 2023;16:11786329231187826.

30. CNIL. Comment déterminer la notion d'interconnexion ? [Internet]. [cité 30 mai 2025]. Disponible sur: https://www.cnil.fr/fr/comment-determiner-la-notion-dinterconnexion

31. Cour des Comptes. La Sécurité Informatique des Etablissements de santé [Internet]. [cité 30 mars 2025]. Disponible sur: https://www.ccomptes.fr/sites/default/files/2024-12/20250103-S2024-1456-La-securite-informatique-des-etablissements-de-sante.pdf

32. Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Secur Appl. déc 2023;1:100016.

33. Fedlex. Convention de Genève du 12 août 1949 [Internet]. [cité 30 mai 2025]. Disponible sur: https://www.fedlex.admin.ch/eli/cc/1951/300_302_297/fr

34. Cybersecurity Center AHA. The importance of cybersecurity in protecting patient safety [Internet]. [cité 11 mai 2025]. Disponible sur: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

35. Sendelj R, Ognjanovic I. Cybersecurity Challenges in Healthcare. In: Achievements, Milestones and Challenges in Biomedical and Health Informatics [Internet]. IOS Press; 2022 [cité 7 juin 2025]. p. 190-202. Disponible sur: https://ebooks.iospress.nl/doi/10.3233/SHTI220951

36. Niam Yaraghi. Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches [Internet]. Brookings. 2016 [cité 11 mai 2025]. Disponible sur: https://www.brookings.edu/articles/hackers-phishers-and-disappearing-thumb-drives-lessons-learned-from-major-health-care-data-breaches/

37. AP-HP. L'Entrepôt de Données de Santé de l'AP-HP [Internet]. 2025 [cité 15 juin 2025]. Disponible sur: https://www.aphp.fr/connaitre-lap-hp/recherche-innovation/lentrepot-de-donnees-de-sante-de-lap-hp

38. Centre Hospitalier Sud Essone - SCHÉMA DIRECTEUR DU SYSTÈME D'INFORMATION SDSI [Internet]. [cité 17 août 2025]. Disponible sur: https://www.ch-sudessonne.fr/sites/ch-sudessonne/files/u2280/schema_directeur_du_systeme_dinformation.pdf

39. IT Pro [Internet]. 2016 [cité 30 mai 2025]. Nine in 10 NHS trusts still use Windows XP. Disponible sur: https://www.itpro.com/public-sector/27740/nine-in-10-nhs-trusts-still-use-windows-xp

40. Alder S. 63% of Known Exploited Vulnerabilities Can be Found in Hospital Networks [Internet]. The HIPAA Journal. 2024 [cité 15 juin 2025]. Disponible sur:

https://www.hipaajournal.com/63pc-known-exploited-vulnerabilities-hospital-networks/

41. A.J. BURNS, M. ERIC JOHNSON, AND PETER HONEYMAN. A brief chronology of medical device security. ResearchGate [Internet]. 2016 [cité 30 mai 2025];59. Disponible sur: https://www.researchgate.net/publication/309058858_A_brief_chronology_of_medical_device_security

42. DSIH. Cyberattaque au Centre Hospitalier Sud Francilie... [Internet]. 2023 [cité 23 mars 2025]. Disponible sur: https://dsih.fr/articles/5263/cyberattaque-au-centre-hospitalier-sud-francilien-chsf-le-bilan-un-an-apres

43. Looi JC, Allison S, Bastiampillai T, Maguire PA, Kisely S, Reutens S, et al. Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. Australas Psychiatry. févr 2025;33(1):106-10.

44. European Data Protection Board. Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations [Internet]. [cité 25 mai 2025]. Disponible sur: https://www.edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

45. ns-yannick. MedTech Europe. 2015 [cité 13 avr 2025]. Medical devices and pharmaceuticals: Two different worlds in one health setting. Disponible sur: https://www.medtecheurope.org/news-and-events/news/medical-devices-and-pharmaceuticals-two-different-worlds-in-one-health-setting/

46. Charlie Treadwell. Elisity. [cité 15 juin 2025]. Navigating the Risks and Best Practices for Medical Device Security in Healthcare. Disponible sur: https://www.elisity.com/blog/navigating-the-risks-and-best-practices-for-medical-device-security-in-healthcare

47. Dimitrov DV. Medical Internet of Things and Big Data in Healthcare. Healthc Inform Res. juill 2016;22(3):156-63.

48. Heatlhcare & Public Health Sector Coordinating COuncil. Cybersecurity Practices for Medium and Large Healthcare Organizations [Internet]. [cité 8 juin 2025]. Disponible sur: https://405d.hhs.gov/Documents/tech-vol2-508.pdf

49. Elendu C, Omeludike EK, Oloyede PO, Obidigbo BT, Omeludike JC. Legal implications for clinicians in cybersecurity incidents: A review. Medicine (Baltimore). 27 sept 2024;103(39):e39887.

50. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices Auckl NZ. 20 juill 2015;8:305-16.

51. Zetter K. It’s Insanely Easy to Hack Hospital Equipment. Wired [Internet]. [cité 2 mai 2025]; Disponible sur: https://www.wired.com/2014/04/hospital-equipment-vulnerable/

52. GAO. Agencies Need to Update Agreement to Ensure Effective Coordination [Internet]. [cité 15 juin 2025]. Disponible sur: https://www.gao.gov/assets/d24106683.pdf

53. IMDRF. Principles and Practices for Medical Device Cybersecurity. 2020; Disponible sur: https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

54. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. J Med Internet Res. 20 avr 2021;23(4):e21747.

55. MedTech Europe. MedTech Europe's vision for cybersecurity in the medical technology ecosystem [Internet]. [cité 6 mai 2025]. Disponible sur: https://www.medtecheurope.org/wp-content/uploads/2023/05/medtech-europe-cybersecurity-position-paper-1.pdf

56. Muddy Waters Capital LLC. MW is Short St. Jude Medical [Internet]. [cité 4 mai 2025]. Disponible sur: https://muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf

57. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, et al. Cybersecurity for Cardiac Implantable Electronic Devices. J Am Coll Cardiol. 20 mars 2018;71(11):1284-8.

58. Regulation - 2016/679 - FR - gdpr - EUR-Lex [Internet]. [cité 15 août 2025]. Disponible sur: https://eur-lex.europa.eu/eli/reg/2016/679/oj/fra

59. Règlement - 2019/881 - FR - EUR-Lex [Internet]. [cité 15 août 2025]. Disponible sur: https://eur-lex.europa.eu/eli/reg/2019/881/oj/fra

60. Directive - 2022/2555 - EN - EUR-Lex [Internet]. [cité 20 juill 2025]. Disponible sur: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

61. Medical Device Coordination Group. MDCG 2019-16 rev. 1 [Internet]. [cité 15 août 2025]. Disponible sur: https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

62. Taylor S, Gilje Jaatun M, Bernsmed K, Androutsos C, Frey D, Favrin S, et al. A Way Forward for the MDCG 2019-16 Medical Device Security Guidance. In: Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments [Internet]. Crete Greece: ACM; 2024 [cité 9 juin 2025]. p. 593-9. Disponible sur: https://dl.acm.org/doi/10.1145/3652037.3663894

63. Biasin E, Kamenjasevic E. Cybersecurity of Medical Devices: Regulatory Challenges in the EU [Internet]. Rochester, NY: Social Science Research Network; 2020 [cité 8 juin 2025]. Disponible sur: https://papers.ssrn.com/abstract=3855491

64. Wadhwa P. GDPR Requirements: How to Stay Compliant with Data Privacy Laws [Internet]. Sprinto. 2024 [cité 21 juin 2025]. Disponible sur: https://sprinto.com/blog/gdpr-requirements/

65. Cybersecurity Act | ANSSI [Internet]. [cité 13 juill 2025]. Disponible sur: https://cyber.gouv.fr/cybersecurity-act

66. Biasin E, Kamenjašević E. Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. Int Cybersecurity Law Rev. 2022;3(1):163-80.

67. Proofpoint [Internet]. 2024 [cité 21 juin 2025]. What Is the NIS2 Directive? Compliance Requirements | Proofpoint US. Disponible sur: https://www.proofpoint.com/us/threat-reference/nis2-directive

68. ANSSI [Internet]. [cité 20 juill 2025]. Avancement de la transposition de la directive NIS 2. Disponible sur: https://aide.monespacenis2.cyber.gouv.fr/fr/article/avancement-de-la-transposition-de-la-directive-nis-2-1b3j1da/

69. ANSSI. La directive NIS 2 [Internet]. [cité 20 juill 2025]. Disponible sur: https://cyber.gouv.fr/la-directive-nis-2

70. KPMG [Internet]. [cité 20 juill 2025]. Directive NIS2 pour la Cybersécurité - Décryptage. Disponible sur: https://kpmg.com/fr/fr/articles/cybersecurite/directive-nis-2.html

71. ISO [Internet]. [cité 27 juill 2025]. ISO 14971:2019. Disponible sur: https://www.iso.org/fr/standard/72704.html

72. ISO 14971 and Medical Device Cybersecurity - Blue Goat Cyber [Internet]. [cité 13 juill 2025]. Disponible sur: https://bluegoatcyber.com/blog/iso-14971-risk-management-in-medical-device-security/

73. ISO [Internet]. [cité 27 juill 2025]. IEC 62304:2006. Disponible sur: https://www.iso.org/fr/standard/38421.html

74. IEC 62304 - Quelles exigences pour les Logiciels de Dispositif Médical ? • Tuleap [Internet]. Tuleap. [cité 27 juill 2025]. Disponible sur: https://www.tuleap.org/fr/qualite-logicielle/iec-62304-exigences-norme-logiciels-de-dispositif-medical

75. ISO [Internet]. [cité 27 juill 2025]. IEC 82304-1:2016. Disponible sur: https://www.iso.org/fr/standard/59543.html

76. Promé G. Résumé de la norme IEC 82304-1 : Logiciels de santé [Internet]. Qualitiso. 2018 [cité 27 juill 2025]. Disponible sur: https://www.qualitiso.com/iec-82304-1-norme-logiciels-de-sante/

77. ISO [Internet]. [cité 27 juill 2025]. ISO/IEC 27001:2022. Disponible sur: https://www.iso.org/fr/standard/27001

78. Exigences de la norme ISO 27001 [Internet]. [cité 27 juill 2025]. Disponible sur: https://www.pqb.fr/page-quelles-sont-les-exigences-de-la-norme-iso-27001-version-2022-.php

79. Sénat. Sénat. 2023 [cité 17 août 2025]. La surtransposition du droit européen en droit français : un frein pour la compétitivité des entreprises. Disponible sur: https://www.senat.fr/rap/r17-614/r17-614.html

80. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? BMJ. 6 juill 2017;j3179.

81. US News & World Report [Internet]. [cité 11 mai 2025]. A Health Hack Wake-Up Call. Disponible sur: //www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call

82. Smith C. Cybersecurity Implications in an Interconnected Healthcare System. Front Health Serv Manage. 2018;35(1):37-40.

83. 20220923-recommandations-ansm-cybersecurite-des-dmil.pdf [Internet]. [cité 22 juin 2025]. Disponible sur: https://ansm.sante.fr/uploads/2022/09/23/20220923-recommandations-ansm-cybersecurite-des-dmil.pdf

84. ISO. ISO. [cité 17 août 2025]. ISO 13485:2016. Disponible sur: https://www.iso.org/fr/standard/59752.html

85. Synack. Understanding the Difference Between DAST vs. SAST for Application Security Testing [Internet]. [cité 3 août 2025]. Disponible sur: https://www.synack.com/knowledge-base/understanding-the-difference-between-dast-vs-sast-for-application-security-testing/

86. Oneconsult AG. Penetration Testing [Internet]. [cité 3 août 2025]. Disponible sur: https://www.oneconsult.com/en/services/penetration-testing/

87. Imperva. What is Fuzzing (Fuzz Testing)? [Internet]. Learning Center. [cité 3 août 2025]. Disponible sur: https://www.imperva.com/learn/application-security/fuzzing-fuzz-testing/

88. Healthcare & Public Health Sector Coordinating Council. Health Industry Cybersecurity Practices [Internet]. [cité 19 juin 2025]. Disponible sur: https://405d.hhs.gov/Documents/HICP-Main-508.pdf

89. Acronis [Internet]. [cité 10 août 2025]. Ultimate Healthcare Data Backup Guide - Importance, Benefits, Best Practices. Disponible sur: https://www.acronis.com/en-us/blog/posts/health-care-data-backup/

90. Search Security [Internet]. [cité 19 juin 2025]. What is defense in depth? Disponible sur: https://www.techtarget.com/searchsecurity/definition/defense-in-depth

91. Assistance aux victimes de cybermalveillance [Internet]. [cité 28 août 2025]. Pourquoi et comment bien gérer ses mots de passe ? Disponible sur: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

Université de Lille
UFR3S-Pharmacie
DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE
Année Universitaire 2024/2025

Nom : Cleuet

Prénom : Arthur

Titre de la thèse : Cybersécurité : Etat des lieux, exigences et bonnes pratiques pour les établissements de santé et les fabricants de dispositifs médicaux.

Mots-clés : Cybersécurité, Dispositifs Médicaux, Etat des lieux, Exigences, Bonnes Pratiques.

Résumé : Le secteur de la santé, hautement numérisé et interconnecté, est aujourd'hui confronté à des cyberattaques menaçant les données, les systèmes d'information et les dispositifs médicaux connectés. Ces attaques ont des répercussions opérationnels, financiers et réputationnels nuisant aux acteurs de santé et fragilisant surtout la qualité des soins dispensés aux patients. La conformité aux référentiels législatifs (tel que le MDR, RGPD, Cybersecurity Act, NIS-2…), et l'adoption de bonnes pratiques se révèlent indispensables pour garantir résilience et continuité des soins.

Abstract: The healthcare sector, extensively digitized and interconnected, currently confronts cyberattacks that threaten data, information systems, and connected medical devices. These incursions carry operational, financial, and reputational repercussions, adversely affecting health-care stakeholders and, above all, undermining the quality of care delivered to patients. Compliance with regulatory frameworks (MDR, GDPR, Cybersecurity Act, NIS-2) and the implementation of best practices are indispensable to ensuring resilience and continuity of care.

<u>Membres du jury</u> :

Président : Monsieur le Professeur Nicolas BLANCHEMAIN, Professeur des Universités en Pharmacotechnie industrielle à l'UFR3S – Pharmacie, Université de Lille.

Directeur de thèse : Monsieur Jérémy POROPANE, Directeur associé en Affaires Réglementaires**,** Biorad – Cressier Suisse

Assesseur(s) :

Madame le docteur Morgane MASSE, Maître de Conférence – Praticien Hospitalier**,** en Biopharmacie, Pharmacie galénique et hospitalière à l'UFR3S – Pharmacie, Université de Lille.

Madame le docteur Daniela ROMON, Coordonnateur Régional en Matériovigilance Réactovigilance**,** Hauts-de-France