

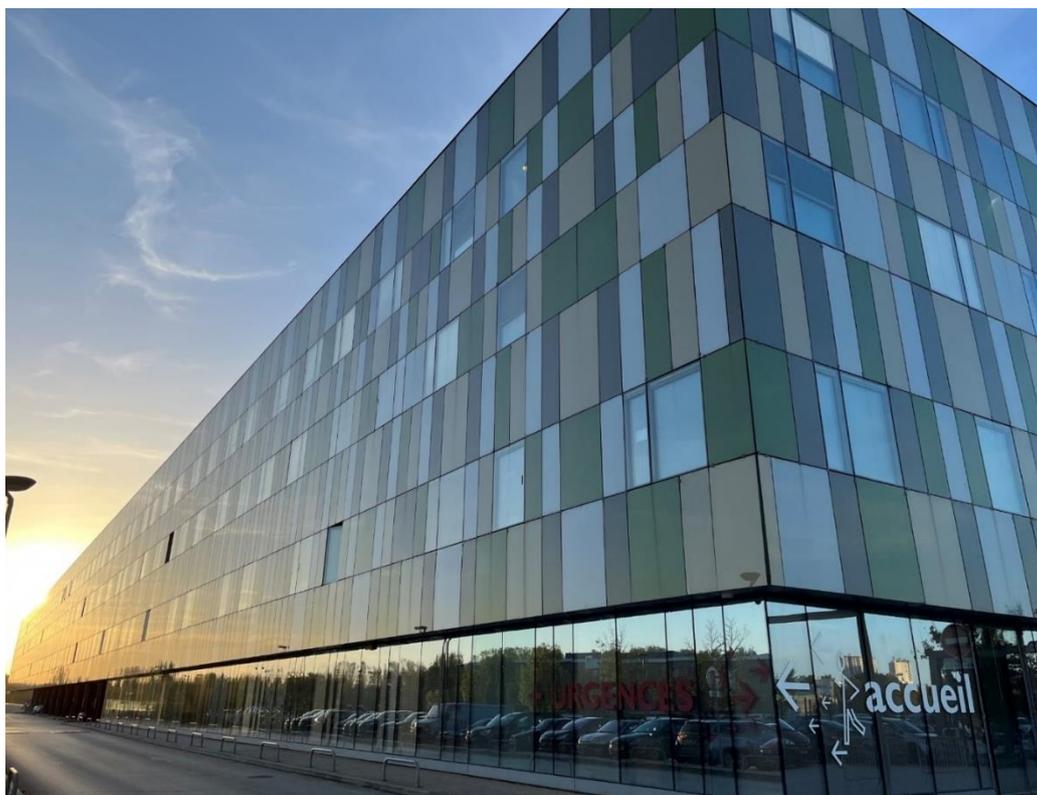
Raphaël PARODI
Master 2 Ingénierie de la Santé
Technologies Biomédicales et Territoires de Santé

Centre Hospitalier William MOREY
CHALON-SUR-SAÔNE
Direction des Technologies en Santé, de l'Innovation et de l'Ingénierie Clinique

Mémoire d'apprentissage de fin de master

Informatique biomédicale

Exploitation des données biomédicales et organisation des fonctions supports

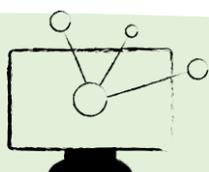


Centre Hospitalier William MOREY, Source : auteur

Disponible sur <https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids198/>

Maître d'apprentissage : Stéphane KIRCHE, Directeur

Tutrice UTC : Karine SLIWAK



Raphaël PARODI – M2 Ingénierie de la Santé – 2022/2023



Remerciements

Je remercie Stéphane KIRCHE, directeur des technologies en santé, de l'innovation et de l'ingénierie clinique et également mon maître d'apprentissage, pour m'avoir donné l'opportunité de réaliser mon année d'alternance au sein de son équipe, pour son accompagnement et sa confiance, à travers les projets qu'il m'a confiés.

J'adresse ma reconnaissance à Alexandre BENOIST, directeur adjoint et ingénieur clinique, pour son suivi, ses conseils et le partage quotidien de son expérience auprès des professionnels de santé.

Je remercie l'ensemble des équipes biomédicale, infrastructure réseau, interopérabilité, applicative et sécurité pour m'avoir permis, à travers leurs expertises, de mener à bien mon projet.

Également, je remercie Karine SLIWAK, ma tutrice UTC, pour sa disponibilité, son suivi et son regard sur l'avancée de mes travaux.

Enfin, je salue l'ouverture du master Ingénierie de la Santé à l'alternance, portée par Isabelle CLAUDE et Jean Matthieu PROT, responsables de la formation.

Résumé

Depuis septembre 2022, le groupement hospitalier de territoire (GHT) Saône et Loire Bresse Morvan a fusionné ses services informatique et biomédical au sein d'une direction des technologies en santé, de l'innovation et de l'ingénierie clinique. La politique générale commune vise à la modernisation, à la sécurisation et à l'accompagnement aux usages technologiques des métiers du soins. A ce titre, l'objectif de cette année d'alternance est de structurer l'activité d'informatique biomédicale à travers l'élaboration du document unique, dont le but est de compiler exhaustivement les informations relatives à l'exploitation des données biomédicales dans les services de soins, par un travail de cartographie des différentes architectures, d'analyse des risques et de rédaction de processus de maîtrise en exploitation. Le document unique s'intègre dans la démarche qualité de la direction, certifiée ISO 9001 sous le périmètre biomédical, et en préparation de la certification ISO 27001 pour le système d'information. En tant que futur professionnel, il s'agit de développer des compétences hybrides en ingénierie biomédicale et en informatique de santé afin de porter à terme, les projets d'intégration des dispositifs médicaux dans le système d'information, et d'exploitation des données biomédicales.

Abstract

Since September 2022, the Saône et Loire Bresse Morvan Territorial Hospital Group has merged its IT and biomedical departments into a Health Technology, Innovation and Clinical Engineering Department. The common general policy aims to modernise, secure and support the use of technology in the care professions. To achieve this, the goal of this apprenticeship year is to structure the biomedical IT activity by drawing up a guideline document, to compile all the informations relating to the use of biomedical data in care departments, by mapping the differentes IT architectures, analysing risk and drafting operational control processes. The guideline document is intended to form part of the management's quality approach, which is ISO 9001 certified in the biomedical area and in preparation for ISO 27001 certification for the information system. As a future professional, the objective is to develop hybrid skills in biomedical engineering and health IT, so as to be able to carry out projects involving the integration of medical devices into the information system and the use of biomedical data.

Mots-clés

Informatique biomédicale – dispositifs médicaux connectés – données biomédicales – système d'information – interopérabilité – sécurité-habilitation aux usages – fonctions supports

Liste des sigles

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information	LPPR : Liste des Produits et Prestations Remboursables
CESITECH : Centre d'Enseignement et de Simulation du Territoire Chalonnais	NEMA : National Electrical Manufacturers
CESU : Centre d'Enseignement des Soins d'Urgence	OSE : Organisme de Services Essentiels
CH : Centre Hospitalier	PACS : Picture archive and communication system
CNIL : Commission nationale de l'informatique et des libertés	PMSI : Programme de Médicalisation des Systèmes d'Information
CR : Compte-rendu	RGPD : Règlement Général sur la Protection des Données
D2IBT : Direction de l'Innovation et de l'Ingénierie Biomédicale de Territoire	RIS : Radiology Information System
DACS : Direction de l'Innovation et de l'Ingénierie Biomédicale de Territoire	RNIPP : Répertoire National d'Identification des Personnes Physiques
DICOM : Dose Archiving and Communication System	RPPS : Répertoire Partagé des Professionnels de Santé
DPI : Dossier Patient Informatisé	RSSI : Responsable de la Sécurité du Système d'Information
DSI : Direction du système d'information	SAMU : Service d'Aide Médicale Urgente
DTS2IC : Direction des Technologies en Santé, de l'Innovation et de l'Ingénierie Biomédicale	SIE : Système d'Information Essentiel
EAI : Enterprise Application Integration	SIH : Système d'Information Hospitalier
ECG : Electrocardiogramme / Electrocardiographe	SIL : Système d'Information du Laboratoire
GAM : Gestion Administrative du Malade	SMUR : Service Mobile d'Urgence et de Réanimation
GHT : Groupement Hospitalier de Territoire	UK : Unité Kangourou
GIE : Groupement d'intérêt Economique	USIC : Unité de Soins Intensifs de Cardiologie
HL7 : Health Level 7	VLAN : Virtual Local Area Network
IFSI : Institut de Formation des Soins Infirmiers	WLAN : Wireless Local Area Network
IHE : Integrating the Healthcare Enterprise	
INS : Identité Nationale de Santé	

Sommaire

Introduction	1
I - Contexte professionnel.....	2
1. Groupement Hospitalier de Territoire Saône et Loire Bresse Morvan.....	2
2. Centre Hospitalier de Chalon-sur- Saône William MOREY	3
3. Direction des Technologies en Santé, de l’Innovation et de l’Ingénierie Clinique .	4
II. Informatique biomédicale.....	6
1. Contexte, enjeux, problématique et objectifs	6
1.1 Numérique en santé.....	6
1.2 Sécurité	9
1.3 Interopérabilité.....	12
1.4 Urbanisation	19
1.5 Réglementation	21
1.6 Document Unique	22
2. Etude de l’architecture informatique biomédicale	22
2.1 Stratégie méthodologique.....	22
2.2 Dispositifs médicaux connectés	23
2.3 Structuration des données	24
2.4 Echanges de données et orientation des flux	25
2.5 Stockage des données	26
3. Préconisations et plan d’action	27
3.1 Criticité et corrections	27
3.2 Analyse des risques.....	29
3.3 Partenariats	30
III. Organisation des fonctions supports et évolution de l’ingénierie biomédicale	30
1. Organisation	30
2. Compétences.....	31
3. Réglementation	32
Conclusion.....	33
Bibliographie.....	34

Introduction

Les technologies en santé contribuent aujourd'hui pleinement à l'amélioration de la qualité et de la sécurité des soins, au développement des pratiques cliniques et à l'organisation institutionnelle à l'échelle des territoires. De plus, elles constituent les fondations de la mutation amorcée du système de santé français, en une réarticulation de l'ensemble des acteurs autour du patient, et non plus d'une pathologie, le tout de manière coordonnée.

Dans le contexte actuel de difficultés d'accès aux soins et de manque de personnels médicaux et paramédicaux, les établissements sanitaires publics s'efforcent de porter l'offre de soins et d'en garantir l'accès sur l'ensemble du territoire national. En l'état, les établissements doivent faire preuve de flexibilité et d'efficacité afin de répondre aux besoins de la population à échelle territoriale, le tout dans un contexte global d'instabilité.

En ce sens, l'exploitation et le développement de l'ensemble des technologies en santé doivent converger vers des objectifs communs centrés autour du patient, des soignants et du territoire. L'une des priorités porte sur l'accès à l'information, qu'elle soit médicale, clinique, administrative ou financière.

Ainsi, le traitement des données biomédicales s'inscrit aujourd'hui totalement dans cette dynamique. Néanmoins, l'intégration de nouvelles technologies innovantes et leur maîtrise en exploitation au sein des plateaux techniques impliquent une évolution des stratégies de support biomédical et informatique.

A ce titre, l'exploitation, l'interopérabilité et la sécurité des données biomédicales constituent un enjeu majeur dans l'organisation des soins. De plus, l'entrée en vigueur du règlement européen 2017/745 [1] a élargi le champ réglementaire en considérant les logiciels de santé comme dispositifs médicaux. Cette modulation induit une évolution significative des pratiques biomédicales sur le volet informatique.

L'objectif de cette année d'alternance est d'engager la mise en œuvre de cette transition en accompagnant la Direction des Technologies en Santé, de l'Innovation et de l'Ingénierie Clinique sous ses périmètres biomédical et informatique, ainsi que les personnels médicaux et paramédicaux. Le but est de développer une double compétence entre les systèmes d'information et les dispositifs médicaux afin d'être capable à terme, de porter des projets hybrides en vue du développement de l'informatique biomédicale et de l'accompagnement des usages en matière d'informatique clinique.

Le développement de ce mémoire sera consacré dans un premier temps à la présentation de l'environnement professionnel, puis dans un second temps à la contextualisation de l'informatique biomédicale et de la problématique. Enfin, les résultats obtenus seront exposés et analysés.

I - Contexte professionnel

1. Groupement Hospitalier de Territoire Saône et Loire Bresse Morvan

Le Groupement Hospitalier de Territoire (GHT) Saône et Loire Bresse Morvan couvre la moitié nord du département de la Saône et Loire (71), en Bourgogne-Franche-Comté (**figure 1**).

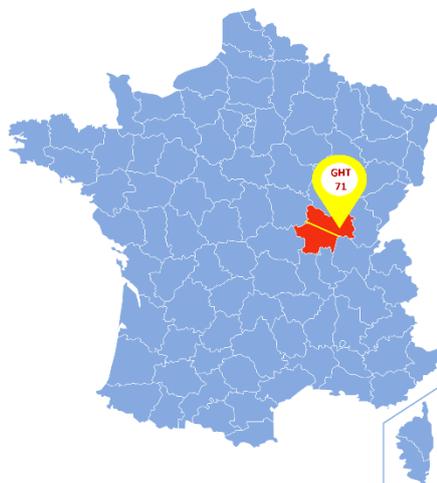


Figure 1 - Localisation du GHT 71 – source : auteur

Il représente un bassin de population de plus de 250 000 habitants [2]. Le GHT est composé d'une dizaine d'établissements (**figure 2**) dont :

- Un établissement support à Chalon-sur-Saône ;
- Deux centres hospitaliers ;
- Quatre hôpitaux de proximité ;
- Un centre hospitalier spécialisé en psychiatrie ;
- Deux établissements d'hébergements pour personnes âgées dépendantes (EHPAD)



Figure 2 - Implantation du GHT 71 [3]

Pour rappel, le GHT ne dispose pas de personnalité morale, c'est-à-dire que les établissements organisés en son sein restent indépendant juridiquement et financièrement [4].

Néanmoins, l'organisation de l'offre de soins est formalisée entre les établissements du GHT autour d'un plan médical partagé (PMP), qui est l'adaptation du Plan régional de Santé (PRS) [5] à l'échelle du territoire de Nord Saône et Loire. Plusieurs spécialités se réorganisent en filières de territoire dans le but de mutualiser les compétences médicales et les ressources matérielles.

2. Centre Hospitalier de Chalon-sur-Saône William MOREY

Le Centre Hospitalier de Chalon-sur-Saône William MOREY est l'établissement support du GHT : il définit et met en œuvre les politiques de gestion pour l'ensemble du territoire notamment pour les achats, le système d'information et les ressources humaines.

Il dispose d'une capacité d'accueil de 800 lits et places¹ dont 290 en médecine, 100 en chirurgie et 30 en obstétrique. En parallèle, on compte 75 places en alternative à l'hospitalisation qui comprend l'hémodialyse, l'hospitalisation de jour en hémato-oncologie, la chirurgie ambulatoire et la médecine ambulatoire. Enfin 42 places sont disponibles en Soins de Suite et Réadaptation (SSR).

Les soins sont organisés autour de neuf pôles et un dixième regroupe la direction et l'administration. Environ 370 praticiens (internes inclus) et 2400 personnels hospitaliers (dont 1500 soignants) travaillent dans l'établissement. Le budget d'exploitation annuel est de l'ordre de 230M€ pour 6M€ d'investissement [6].

L'hôpital héberge le siège du SAMU² 71-Centre 15 qui organise les interventions du SMUR³ et de l'HéliSMUR sur tout le département de la Saône-et-Loire. Au-delà de ses missions sanitaires, le centre hospitalier (CH) assure également des missions de formations à travers trois entités : l'Institut de Formation en Soins Infirmiers (IFSI), le Centre d'Enseignement des Soins d'Urgence (CESU) et le Centre d'Enseignement et de Simulation du Territoire Chalonnais (CESITECH), qui permet aux soignants de consolider ou de faire évoluer leurs pratiques médicales à travers des mises en situations en conditions réelles sur mannequins.

L'établissement possède un plateau technique complet notamment composé :

- d'un bloc opératoire (9 salles, 1 robot de chirurgie orthopédique),
- d'une stérilisation interne,
- d'une maternité (5 salles de travail, 1 bloc de césarienne),
- d'un plateau d'imagerie (4 salles de radiologie conventionnelle, 1 mammographe, 2 scanners, 1 IRM en coopération (GIE) avec les radiologues libéraux)
- d'un parc de 60 échographes,
- d'un laboratoire de biologie médicale (25 automates, 1 spectromètre de masse, 1 cytomètre en flux),
- d'un plateau de dialyse (30 générateurs) ,
- d'un parc de moniteurs de surveillance (160 lourd et 300 légers).

¹ La distinction entre un lit et une place réside dans le fait qu'un lit est occupé durant plus de 24h par un patient, ce qui introduit la notion de séjour. Une place est occupée moins de 24h et peut donc accueillir plusieurs patients durant une journée, comme dans les prises en charges en ambulatoire.

² SAMU : Service d'Aide Médicale Urgente

³ SMUR : Service Mobile d'Urgence et de Réanimation

De par la dynamique de son activité, l'hôpital a engagé en 2022 le développement de son infrastructure médicale à travers l'extension du plateau de dialyse (10 générateurs supplémentaires) la création d'un plateau interventionnel de cardiologie composé d'une salle hybride et d'une salle de coronarographie et l'installation d'une seconde IRM.

La gouvernance est commune à l'ensemble du GHT et constituée de trois grands pôles intégrant les différentes directions territoriales (**figure 3**).

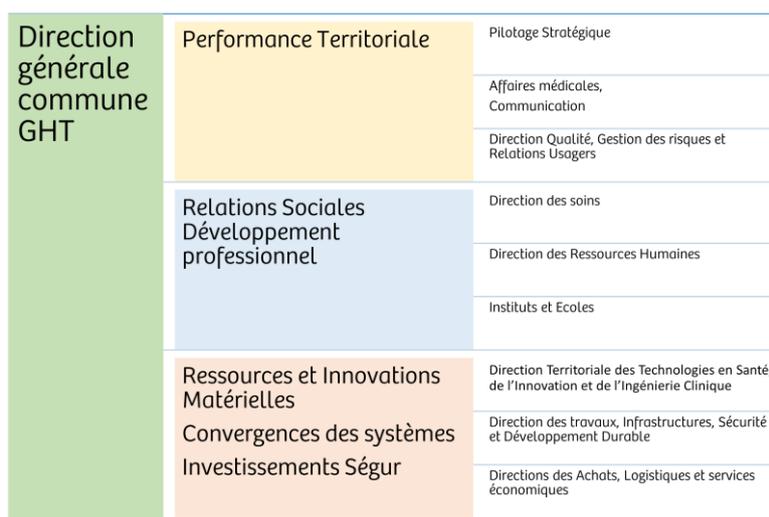


Figure 3 - Schéma de l'organisation de la gouvernance commune du GHT- source : auteur

Chaque responsable de pôle a pour mission la coordination des directions concernées sur la politique générale du groupement.

3. Direction des Technologies en Santé, de l'Innovation et de l'Ingénierie Clinique

La Direction des Technologies en Santé, de l'Innovation et de l'Ingénierie Clinique (DTS2IC), mise en place fin 2022, est la nouvelle entité issue de la fusion de la Direction des Systèmes d'Information (DSI) et de la Direction de l'Innovation et de l'Ingénierie Biomédicale de Territoire (D2IBT). Intégrant plus d'une soixantaine de techniciens, ingénieurs, personnels administratifs, personnels médicaux et paramédicaux, la DTS2IC a vocation à décroquer et à faire converger les technologies en santé (informatique et biomédical) vers une même politique de développement et de gestion au sein des établissements du territoire.

Cette nouvelle organisation vise à la mutualisation des outils et méthodes de gestion de projet, d'achat, de qualité et de services rendus aux personnels médicaux et paramédicaux. De plus, l'évolution des technologies et en particulier des dispositifs médicaux, implique une gestion hybride sur le volet technique avec des spécificités liées à la fois aux usages cliniques mais également à l'interopérabilité, à la sécurité ou au stockage des données biomédicales. Cette évolution du cadre des fonctions supports est rendue possible par l'adhésion de la direction générale au fait que les technologies en santé permettent et favorisent la mise en œuvre d'un plan médical partagé dans un territoire tel que celui de la Saône et Loire.

L'organigramme est construit de manière transversale et repose sur une logique d'ingénierie (figure 4).

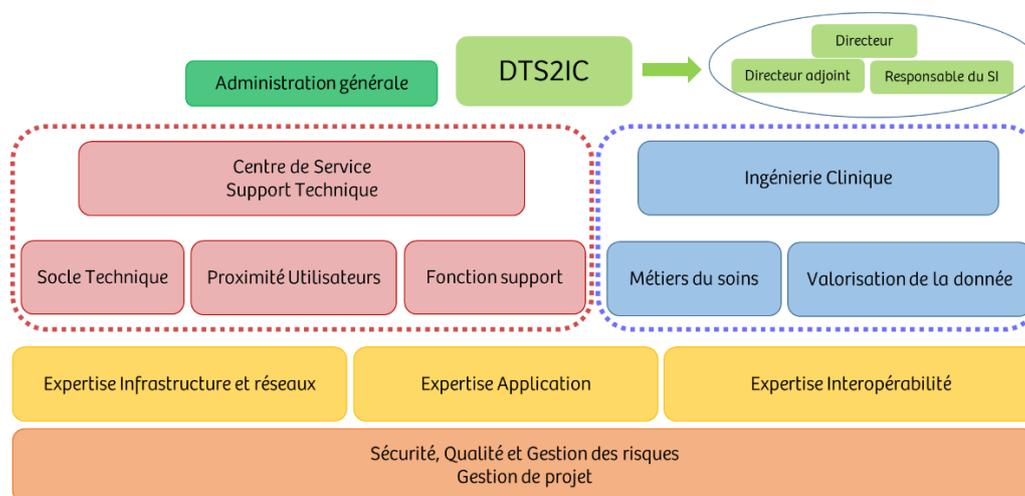


Figure 4 - Schéma de l'organisation de la DTS2IC - source : auteur

La direction définit une politique générale commune et une stratégie territoriale qui vise à répondre aux attentes et aux besoins des utilisateurs, à sécuriser et à améliorer la prise en charges des patients, le tout dans une maîtrise réglementaire et économique. La coordination et la mise en œuvre de la stratégie sont assurées par le directeur adjoint et le responsable du système d'information.

Le *Centre de service* regroupe les techniciens biomédicaux et informatiques. Il a pour mission d'apporter un support technique quotidien à l'ensemble des utilisateurs de l'hôpital, qu'ils soient médicaux ou non, afin de garantir la disponibilité et le bon fonctionnement des équipements. Cette entité est l'interface unique à laquelle s'adresse les utilisateurs lorsqu'ils rencontrent des difficultés techniques.

L'*Ingénierie Clinique* s'articule autour de l'usage des technologies et leur intégration dans les pratiques cliniques. Elle vise à accompagner les professionnels de santé, à moderniser leurs outils et à améliorer leurs conditions de travail. L'équipe est composée d'ingénieurs clinique et informatique biomédicale, de techniciens et de référents cliniques, qui sont des médecins, infirmiers et aides-soignants dont une partie de leur temps est dédié à la DTS2IC, afin de créer des liens robustes de communication avec les professionnels de santé. De plus, le pôle d'ingénierie clinique est en charge de la valorisation des données biomédicales sur l'ensemble de la chaîne d'information, de la production par les dispositifs médicaux au stockage dans l'entrepôt de données et à l'exploitation par les systèmes d'intelligences artificielles d'aide au diagnostic ou de gestion (logistique, flux patients, etc...)

Les équipes du *Centre de service* et de l'*Ingénierie clinique* peuvent s'appuyer sur un socle d'experts techniques en interopérabilité, application et infrastructure qui veillent à la bonne intégration des nouvelles technologies et à leur exploitation dans les meilleures conditions opérationnelles. De plus, ils assurent la disponibilité et l'intégrité générale du système d'information.

Enfin, la sécurité est intégrée dans la totalité des projets de développement ou de modernisation. Elle est portée par le Responsable de la Sécurité du Système d'Information

(RSSI) qui veille à la conformité du système d'information en terme de sécurité à travers des niveaux de criticités établis par des analyses de risques systématiques.

La gestion de projet, le management de la qualité et la gestion des risques sont transversaux et communs à l'ensemble des professionnels de la DTS2IC, qu'ils soient biomédicaux ou informatiques.

Au global, la D2TS2IC exploite sur le site de Chalon plus de 8 500 équipements biomédicaux, 1 700 ordinateurs, 600 serveurs, 180 logiciels et coordonne plus de 7 800 interventions de support biomédical et 11 000 interventions de support informatique par an [6].

II. Informatique biomédicale

1. Contexte, enjeux, problématique et objectifs

1.1 Numérique en santé

L'introduction des outils informatiques au sein des hôpitaux français n'est pas récente puisqu'elle date des années 60 [7]. Initialement dédiée aux traitements des tâches administratives, l'informatisation s'est progressivement développée vers les soins et les professionnels de santé à travers plusieurs stratégies politiques successives, dont les plans *Hôpital 2007* [8], *Hôpital numérique (2012)* [9], *Ma santé 2022* [10] et *le Ségur numérique* [11].

La feuille de route 2023-2027 du numérique santé [12] a pour ambition d'accélérer la modernisation et le déploiement d'outils favorisant l'échange d'informations de santé sous quatre grands axes :

- La *prévention*, en intégrant le patient au cœur de son parcours de santé ;
- La *prise en charge*, avec la modernisation des outils des professionnels de santé permettant de leur libérer du temps dédié aux patients ;
- L'accès à la santé, en mettant en œuvre des outils d'aide à l'orientation des patients ;
- L'*innovation*, en créant un cadre économique et réglementaire propice au développement technologique et à l'accompagnement aux nouveaux usages.

L'élément central de cette politique d'accélération du numérique en santé est *Mon Espace Santé*[13] qui est le point de convergence des informations pour chaque patient. En effet, l'objectif est de rendre accessible et exhaustif les documents et données de santé au patient et au professionnel de santé qui le prend en charge. *Mon Espace Santé* doit devenir un outil incontournable de la coordination des soins puisqu'il doit être alimenté par l'ensemble des acteurs : les établissements de santé, les structures médico-sociales, les cabinets d'imagerie, les laboratoires de biologie médicale, la médecine de ville et les officines (**figure 5**).

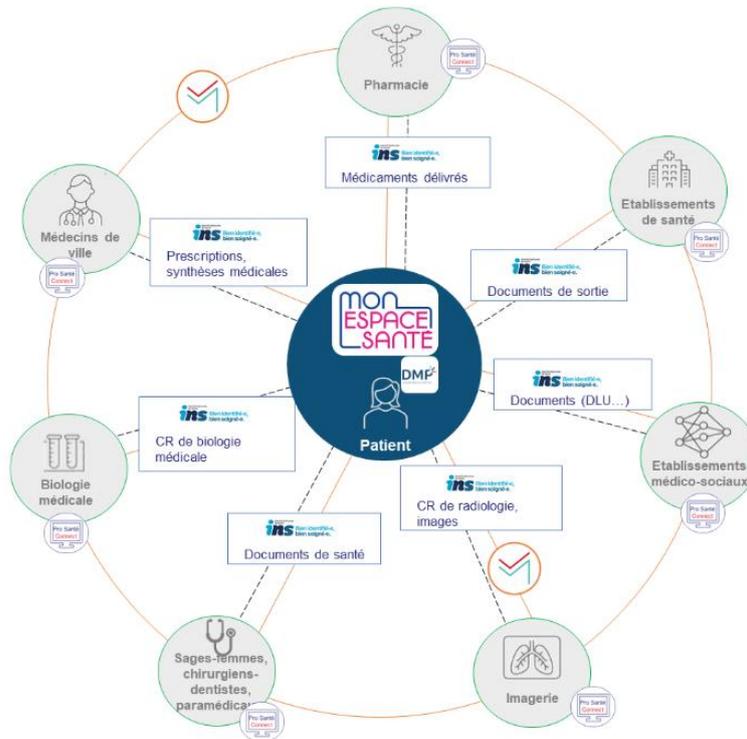


Figure 5 - Interactions , référentiels et flux entre les acteurs du système de soins avec Mon Espace Santé [14]

Les échanges sont structurés par différents référentiels dont :

- *l'Identité Nationale de Santé (INS)*, qui est reliée au Répertoire National d'Identification des Personnes Physiques (RNIPP) [15] géré par l'INSEE, et qui permet à chaque citoyen de posséder un identifiant unique dans l'ensemble de son parcours de soins, et qui permet également de faciliter l'identitovigilance au sein des établissements de santé [14].
- *Pro Santé Connect*, qui permet de constituer un annuaire de santé et de sécuriser l'accès et l'identification des professionnels à *Mon Espace Santé* [14] par l'intermédiaire d'une double authentification sur la base de l'état civil et du Répertoire Partagé des Professionnels de Santé (RPPS) [16].
- *La Messagerie Sécurisée de Santé (MSS)*, dont le but est de garantir un canal de communication sécurisé entre le patient et les professionnels de santé, notamment pour l'échange de documents confidentiels [14].

De plus, chaque spécialité médicale dispose de référentiels dédiés selon les usages :

- L'ordonnance numérique pour la pharmacie [17], où le patient peut directement envoyer par voie dématérialisée son ordonnance à la pharmacie de son choix qui pourra anticiper sa commande.
- Le partage national d'imagerie médicale [18], dont l'objectif est de donner aux médecins l'accès aux images dans *Mon Espace Santé*. Techniquement, il s'agit de créer un maillage national des PACS (publics et privés) par l'intermédiaire de passerelles (DRIMBOX).

En terme financier, l'accélération du déploiement et de modernisation du numérique en santé est portée par des modalités d'incitation : l'état finance des solutions pour le compte des établissements et autres acteurs de santé, à condition que ces solutions soient conformes aux référentiels produits par l'Agence du Numérique en Santé [14]. Il en va de même pour les dispositifs médicaux numériques. En effet, un dispositif médical est considéré comme étant numérique si il traite des données à caractère personnel selon le règlement général sur la protection des données (RGPD)[19] [20]. Dans ces conditions, il peut être remboursé si il apparait dans la liste des produits et prestations remboursables (LPPR) [21], ou dans le cadre d'une prise en charge anticipée ou transitoire [20].

C'est dans ce contexte que les établissements de santé ont un rôle important à jouer et particulièrement dans l'alimentation et l'exploitation de *Mon Espace Santé*. En effet, la variété des activités médicales représente un potentiel important de production de documents médicaux parmi les comptes-rendus d'imagerie, de biologie, de chirurgie, obstétrique, de séjour ou de consultation. Pour la très grande majorité des spécialités médicales, les dispositifs médicaux sont capables de produire des données biomédicales permettant d'enrichir les comptes-rendus associés, idéalement de manière automatisée.

Ainsi, l'informatique biomédicale couvre la production, la structuration et l'exploitation des données issues des dispositifs médicaux. Les enjeux liés à la valorisation des données biomédicales sont stratégiques et dépassent la seule alimentation de *Mon Espace Santé*. En effet, le traitement des données biomédicales s'inscrit comme l'un des vecteurs de transformation et de modernisation des pratiques cliniques, de sécurisation de la prise en charge, de la territorialisation de l'offre de soins de manière coordonnée et de flexibilité des établissements face aux aléas (**figure 6**).

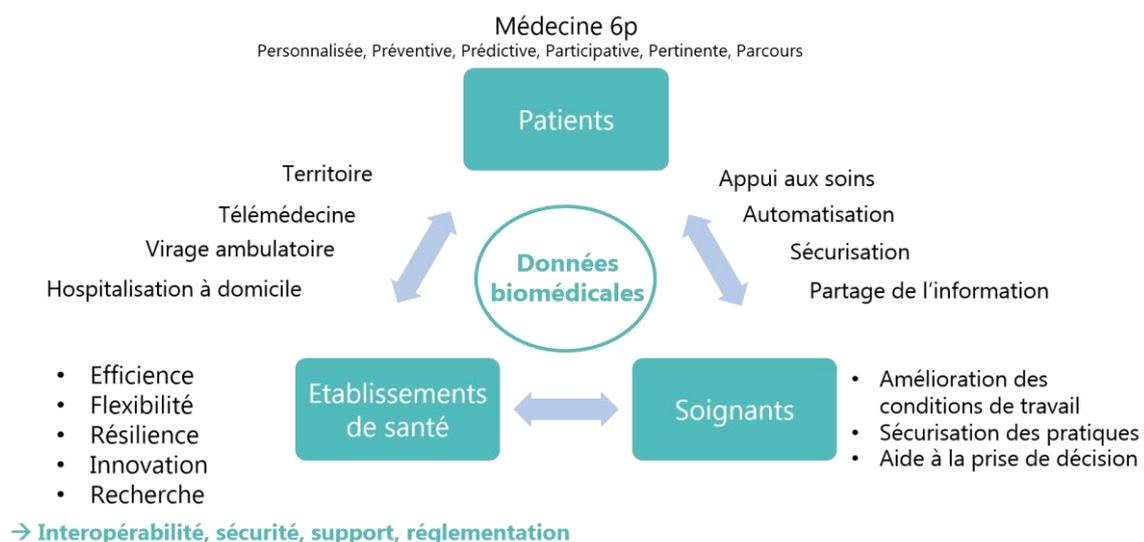


Figure 6 - Enjeux liés à la valorisation des données biomédicales pour les patients, les professionnels et les établissements de santé – source : auteur

Néanmoins l'informatique biomédicale doit reposer sur un socle technique, organisationnel et réglementaire adapté et structuré par la sécurité, l'interopérabilité, le support et la réglementation.

1.2 Sécurité

La sécurité demeure la priorité de tous les professionnels des technologies en santé. Elle est la condition sine qua non au développement du numérique en santé et à la montée en puissance de l'informatique biomédicale dans les établissements de santé.

Depuis 2017, les établissements de santé sont soumis à une obligation de déclaration des incidents sur leurs systèmes d'information selon l'article L.1111-8-2 du code de la santé publique [22] dont les modalités de signalement ont été mises à jour en 2022 [23]. Ainsi, l'analyse de ces signalements permet de dessiner le panorama actuel de l'exposition et de la vulnérabilité des établissements de santé face à la cybercriminalité et aux risques inhérents à leurs systèmes d'information. En 2022, 432 structures⁴ ont déclaré au moins un incident et 75% des établissements supports de GHT ont été concernés [24].

Plusieurs niveaux d'échelles sont à considérer afin de se saisir des risques et des impacts associés :

- la sécurité des données ;
- la sécurité de l'infrastructure ;
- la sécurité du patient.

Concernant les données, 63% des structures ont déclarées au moins un incident impactant, dont 43% concernaient des données de santé à caractère personnel (fuite de données, indisponibilité)[24].

Au niveau de l'infrastructure du système d'information, 39% des établissements ont dû déclencher un mode dégradé lié à l'indisponibilité de certains équipements ou logiciels. Pour 19% des structures, cela a mené à une interruption de la chaîne de prise en charge des patients entraînant de fait, une perte de chance pour les patients concernés [24].

Pour les cas les plus graves, l'incident a pu mettre la vie du patient en danger (76 cas) dont 5 où la mise en danger a été avérée[24].

Face à ces situations, il est important d'identifier les causes ayant menées à ces incidents : 50 % sont d'origine malveillante. Ils ont principalement pour origine le vol d'identifiant et mot de passe via des techniques d'hameçonnage⁵, des attaques par rançongiciel⁶ et l'utilisation de failles d'équipements obsolètes [24].

Les 50% d'incidents restant ne sont pas d'origine malveillante et sont liés à des défaillances techniques. En effet, la première cause est le dysfonctionnement de l'infrastructure lié à des interventions internes sur le système, ou externes menées par les hébergeurs et autres prestataires. La deuxième cause provient de la perte du lien télécom auprès des opérateurs téléphoniques qui peut être critique pour le service des urgences et la régulation du SAMU. Enfin, les bugs d'applications métiers sont à l'origine d'incidents pouvant perturber la prise en charge des patients [24].

⁴ Structures qui intègrent les établissements de santé publics et privés ainsi que les établissements médico-sociaux.

⁵ Hameçonnage : (ou phishing) : technique utilisée pour soutirer l'identifiant et le mot de passe d'un utilisateur en se faisant passer pour une entité officielle par l'intermédiaire d'un faux mail [25].

⁶ Rançongiciel : logiciel malveillant utilisé pour chiffrer les données pour lesquelles, une rançon est demandée.[26]

Ainsi, il est nécessaire de différencier la sécurité et la sûreté du système d'information et des dispositifs médicaux. La sécurité vise à protéger les équipements d'actions volontaires malveillantes (menaces) alors que la sûreté désigne la protection des équipements d'actions involontaires (vulnérabilités) [27]. La sûreté peut être caractérisée par la confiance que les utilisateurs ont dans le système d'information [28].

En somme, de par les risques encourus par les patients, les établissements de santé doivent renforcer la sécurité et la sûreté de leurs systèmes d'information. Cependant, plusieurs facteurs limitants viennent freiner cette démarche :

- la difficulté d'investissements pérennes sur l'infrastructure ;
- le manque de ressources humaines qualifiées ;
- l'absence de cadre réglementaire et normatif spécifique aux établissements de santé.

En effet, l'exploitation des systèmes d'informations des établissements de santé n'est pas encadrée réglementairement au même titre que celle des dispositifs médicaux, régie par le code de la santé publique (articles R5211-1 à R5232-22)[29].

Depuis 2021, les établissements supports des Groupements Hospitaliers de Territoires (GHT) ont été désignés par le gouvernement comme « Organismes de Services Essentiels (OSE) » [30], qui les place sous l'autorité de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). A ce titre, les établissements sont soumis à une série d'obligations :

- désigner un représentant auprès de l'ANSSI ;
- appliquer les 23 règles de sécurité informatique de la directive européenne NIS (Network and Information Security)[31] transposées dans le droit français par la loi n° 2018-133 du 26 février 2018 [32] puis mises à jour dans la directive NIS 2 votée en 2022 [33] ;
- se soumettre à des contrôles réalisés par l'ANSSI ou ses prestataires ;
- identifier et déclarer ses Systèmes d'Information Essentiels (SIE).

Les règles de sécurité à appliquer, fixées par l'arrêté du 14 septembre 2018 [34], portent sur la gouvernance, la protection, la défense et la résilience du système d'information (**figure 7**)

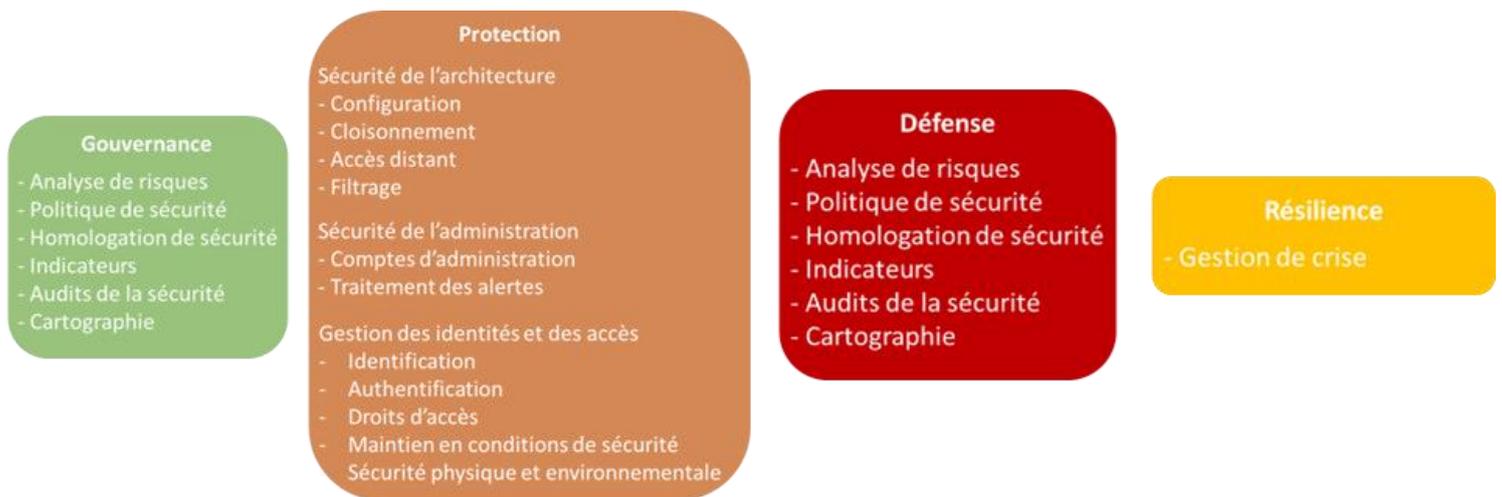


Figure 7 - Règles de sécurité appliquées aux OSE- source : auteur

Concernant les Systèmes d'Informations Essentiels (SIE) en établissement de santé, ils désignent les plateaux techniques ou services pour lesquels une atteinte à l'intégrité, la disponibilité ou la confidentialité du système d'information a un impact sur la prise en charge des patients [35]. Leur déclaration doit notamment inclure une cartographie, contenant l'infrastructure, les flux, le plan d'adressage et les applicatifs. La liste des SIE n'est pas exhaustive et peut varier selon les établissements mais concerne en principe :

- Le SAMU ;
- L'imagerie médicale ;
- Le laboratoire ;
- La pharmacie ;
- Les urgences ;
- Les soins critiques ;
- Le bloc de chirurgie associé à la stérilisation ;
- Le dossier patient informatisé (transverse sur tous les services).

La désignation des OSE va obliger les établissements à plus de transparence sur le niveau de sécurité de leurs systèmes d'information et leurs pratiques en terme de gouvernance, de gestion de crise et d'infrastructure technique. Cette incitation réglementaire va permettre de structurer les activités d'exploitation des systèmes d'information appliqués à la santé.

1.3 Interopérabilité

L'interopérabilité des données de santé désigne la capacité des systèmes (dispositifs médicaux, logiciels et plus généralement le système d'information) à communiquer et à échanger des données structurées, interprétables et intégrées dans les processus cliniques. La notion d'interopérabilité peut être définie en quatre niveaux [36] : technique, syntaxique, sémantique et organisationnelle.

Interopérabilité technique

Le niveau technique correspond à la capacité des équipements à communiquer physiquement entre eux et à échanger des données. De nombreuses normes existent aujourd'hui et permettent d'assurer ce niveau d'interopérabilité, les plus connus étant la norme USB⁷, les protocoles Ethernet⁸ ou WIFI⁹.

Interopérabilité syntaxique

Le niveau syntaxique désigne l'aptitude des systèmes à échanger des données structurées. Plus d'une quarantaine de normes et standards existent à l'échelle internationale, dont les standards HL7¹⁰ (V2, CDA, RIM, FHIR)[39] et DICOM¹¹ [40].

Interopérabilité sémantique

L'interopérabilité sémantique traduit la faculté des équipements et logiciels à échanger des données dont le sens clinique n'est pas altéré, pour en permettre l'interprétation. Plusieurs bases de terminologies internationales permettent de coder les données (observations cliniques, pathologies, etc ...) tel que LOINC [41] ou SNOMED [42].

Interopérabilité organisationnelle

L'interopérabilité organisationnelle porte sur la contextualisation de l'intégration des données structurées et interprétables sémantiquement dans les processus cliniques. C'est l'association internationale IHE (Integrating the Healthcare Enterprise) [43], composée de praticiens et d'industriels, qui développe des profils d'intégrations. Chaque spécialité médicale dispose de plusieurs profils en fonction des cas d'usages de données. Pour exemple, la **figure 8** décrit le profil d'imagerie SWF qui intègre les données dans les flux de planification de l'examen, d'acquisition, de visualisation et de stockage des images, entre les dispositifs médicaux, le système d'information de radiologie et le système de stockage.

⁷ www.usb.org/

⁸ Protocole régie par la norme ISO/IEC/IEEE 8802-3 [37].

⁹ Différents protocoles encadrés par la norme ISO/IEC/IEEE 8802-11:2018 [38].

¹⁰ HL7 : Health Level 7

¹¹ DICOM : Digital Imaging and Communications in Medicine.

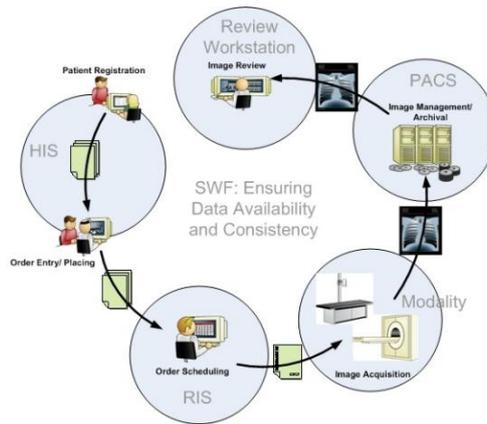


Figure 8 - Profil Scheduled Workflow (SWF) en imagerie - source : https://wiki.ihe.net/index.php/Scheduled_Workflow

Une synthèse des niveaux d'interopérabilité est illustrée dans la figure 9.

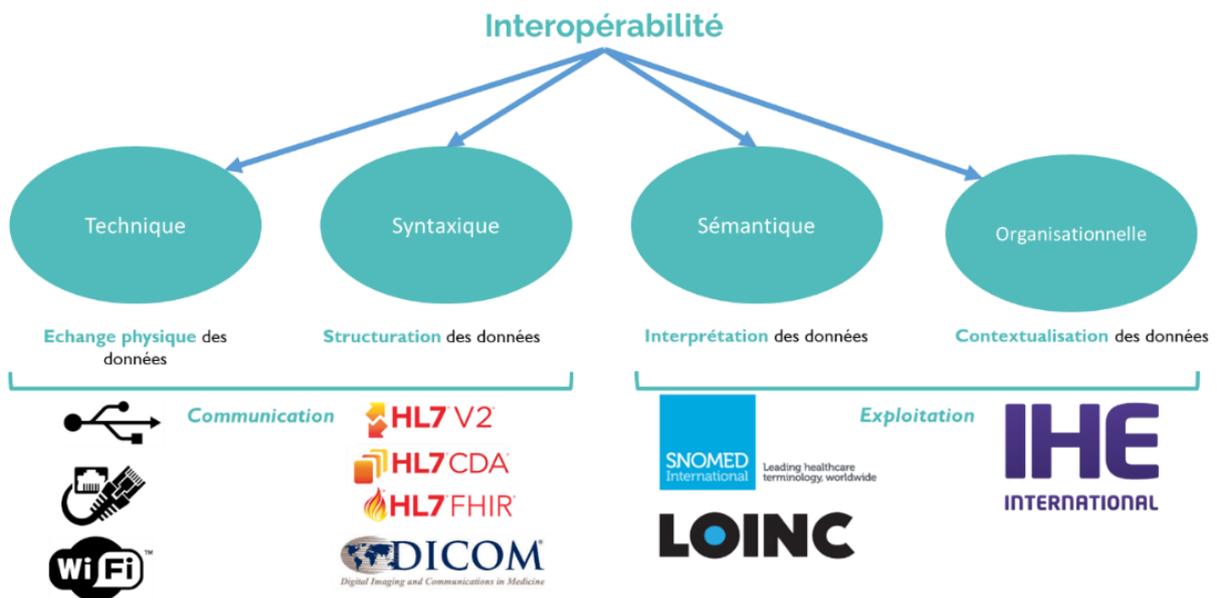


Figure 9 - Niveaux d'interopérabilité et standards associés - source : auteur

L'interopérabilité des données de santé n'est pas une problématique récente. En effet, la première norme DICOM date de 1985, la première norme HL7 date de 1987 et l'association IHE de 1998 : toutes n'ont eu cesse de se développer au cours des années, comme actuellement en imagerie, où l'utilisation des systèmes d'information standardisés n'est plus remise en question. Ainsi, nous pouvons considérer que le cadre technique est propice au développement de l'interopérabilité des données biomédicales. Cependant, des freins autres ont empêché les établissements de santé d'exploiter les données produites par leurs dispositifs médicaux, comme en témoigne une étude menée en 2010 sur plus de 800 hôpitaux américains par la *Healthcare Information and Management Systems Society* [44] :

- 90 % des établissements disposent au sein de leurs parcs au d'au moins 6 types de dispositifs médicaux connectables (qui possèdent une ou plusieurs interfaces physiques et logiciels) ;

- Environ 30 % d'entre eux connectent moins de 3 types de dispositifs médicaux pour en exploiter les données (**figure 10**).

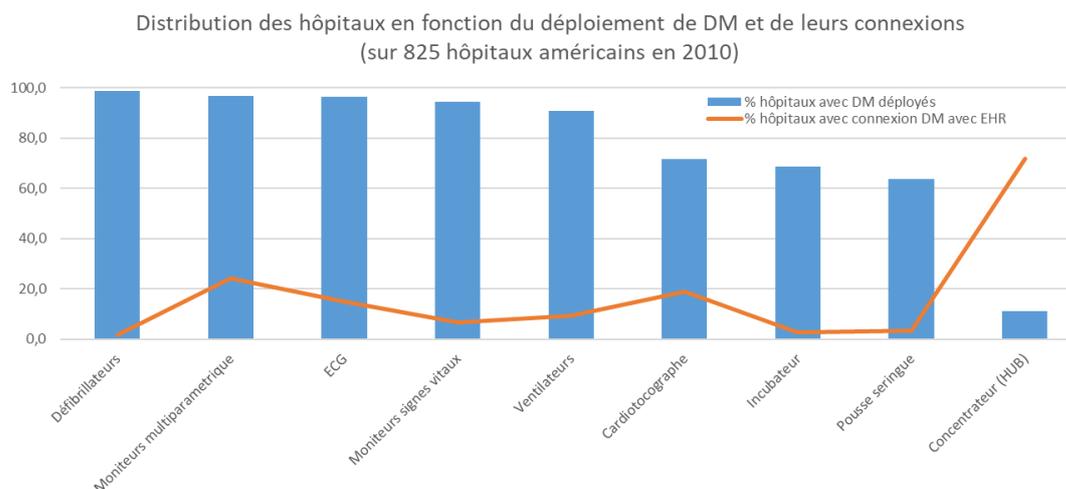


Figure 10 - Distribution des hôpitaux en fonction des types de dispositifs médicaux et de leurs connexions - source : auteur d'après les données de l'HIMSS [44]

Les enjeux commerciaux autour des dispositifs médicaux sont l'un des principaux freins au développement de l'interopérabilité, ce qui a un fort impact clinique mais également financier.

Impact clinique

En 2000, l'Institute of Medicine (US) Committee on Quality of Health Care in America a publié un rapport estimant à environ 100 000 le nombre de décès annuels aux Etats-Unis, ayant pour causes des erreurs médicales, dont 40% sont des erreurs techniques, 20% des erreurs médicamenteuses et 17 % des erreurs de diagnostic [45]. Pour chacune de ces typologies, le manque d'interopérabilité des dispositifs médicaux est identifié comme un facteur significatif de responsabilité [46].

En France, l'étude des événements indésirables graves signalés par les établissements de santé auprès de la Haute Autorité de Santé en 2021 [47] permet d'apprécier les enjeux liés au manque d'interopérabilité, notamment sur les erreurs médicamenteuses (**figure 11**).

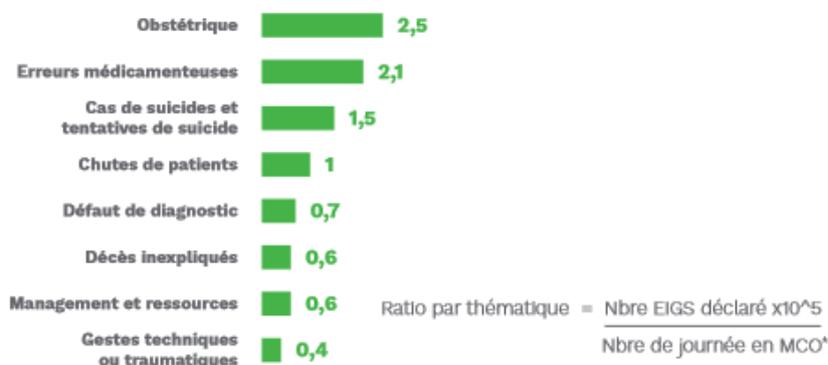


Figure 11 - Nombre d'événements indésirables graves signalés, déclarés par jour [47]

En effet, le nombre d'erreurs médicamenteuses est supérieur aux cas et tentatives de suicides. En d'autres termes, le nombre d'événements indésirables graves évitables et

supérieur au nombre d'événements indésirables graves inévitables. Le détail de la nature des erreurs médicamenteuses (**figure 12**) met en évidence une majorité d'erreur de dosage.

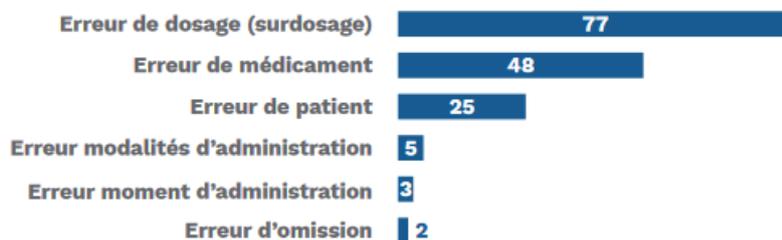


Figure 12 - Nature des erreurs médicamenteuses [47]

Plus de 60% de ces erreurs de dosage surviennent lors de la phase d'administration des médicaments aux patients [47] (**figure 13**) : phase où les dispositifs médicaux sont à l'interface du soignant et du patient (pousse-seringues).

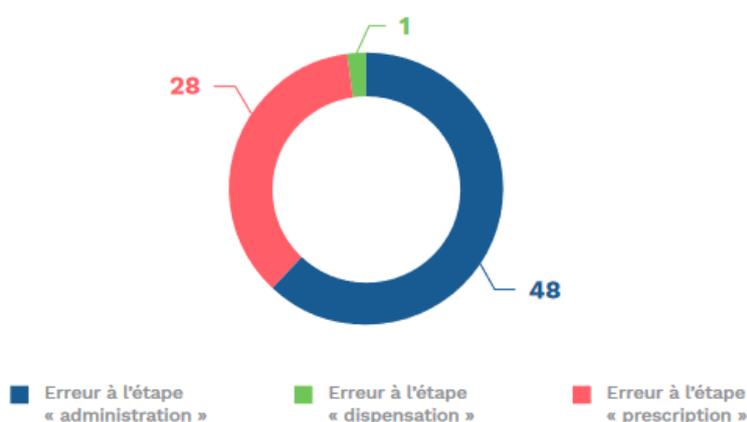


Figure 13 - Distribution des erreurs de dosage selon l'étape de prise en charge médicamenteuse [47]

Ainsi, l'interopérabilité des données biomédicales permet d'automatiser les flux d'informations sur toute la chaîne médicamenteuse, de la prescription à l'administration, minimisant de fait le risque d'erreurs de saisie. La **figure 14** illustre l'apport de l'interopérabilité :

- A gauche, le médecin prescrit une injection médicamenteuse de 8mg à un débit de 1mg/h. Cependant, lors de l'administration, la pompe est programmée manuellement pour 1mg à 8mg/h suite à une erreur de saisie et entraîne une dégradation de l'état clinique du patient.
- A droite, l'interopérabilité des données biomédicales permet de transmettre automatiquement les données de la prescription à la pompe à perfusion, dont le fonctionnement peut être ajusté en fonction de l'évolution des constantes vitales monitorées.

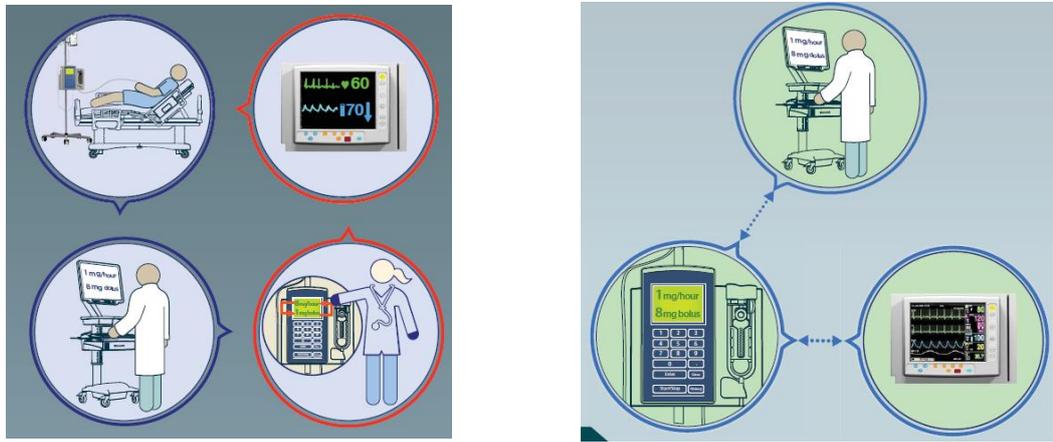


Figure 14 - Comparaison de la chaîne d'information médicamenteuse sans interopérabilité (à gauche) et avec (à droite) [46]

L'interopérabilité contribue également à améliorer les conditions de prise en charge et de diagnostic des patients. En effet, l'envoi automatique des données produites par les dispositifs médicaux directement dans le dossier patient informatisé permet aux professionnels de santé d'avoir accès instantanément à l'ensemble des données nécessaires pour poser un diagnostic (imagerie, biologie, monitoring des fonctions vitales, etc...).

La **figure 15** ci-dessous représente l'impact de l'interopérabilité sur la réalisation d'un électrocardiogramme.

- A gauche, le patient pris en charge se voit réaliser un électrocardiogramme (ECG) afin d'évaluer son activité cardiaque, dont le tracé est uniquement imprimé sur papier. Cependant, le document n'est pas transmis (perdu, jeté, etc...) au cardiologue qui ne peut pas poser de diagnostic précis. Ainsi, dans le cas d'une prise en charge en urgence, ce type de défaillance peut engendrer des pertes de chance pour le patient.
- A droite, l'interopérabilité des données permet d'envoyer directement le tracé de l'ECG dans le dossier patient informatisé, le médecin pouvant y avoir accès directement.

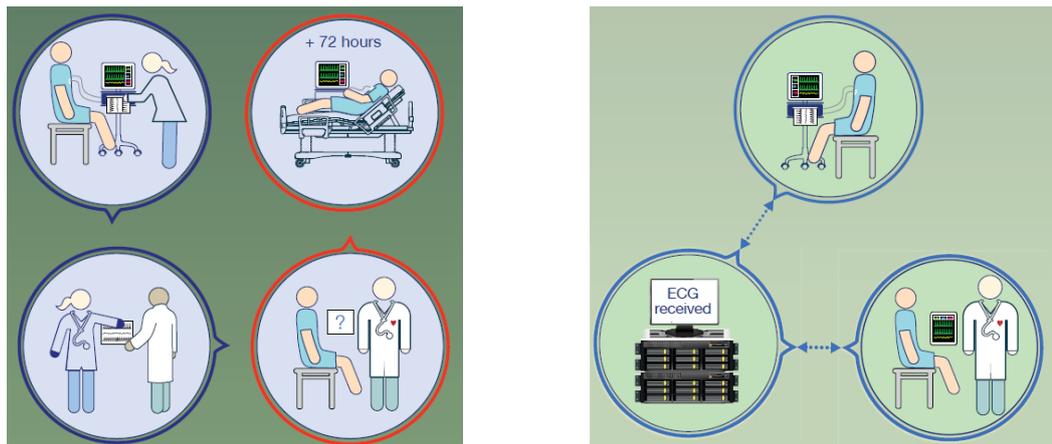


Figure 15 - Comparaison de la chaîne d'information de diagnostic sans interopérabilité (à gauche) et avec (à droite) [46]

Enfin, l'interopérabilité des données biomédicales contribue largement à la sécurité du patient durant son hospitalisation. L'exemple présenté ci-dessous en **figure 16**, illustre les conséquences potentielles de la non-interopérabilité en soins critiques :

- A gauche, le patient est hospitalisé en réanimation suite à des lésions cérébrales. Les paramètres du ventilateur sont ajustés selon les analyses de gaz du sang réalisés au laboratoire de biologie de l'hôpital. Ce réajustement est effectué plusieurs fois par jour. Sans interopérabilité, le médecin paramètre le ventilateur manuellement à partir des résultats sanguins envoyés dans le dossier patient informatisé, ou à partir des résultats communiqués oralement, ce qui peut induire dans les deux cas des erreurs.
- A droite, l'interopérabilité permet de faire communiquer directement le ventilateur avec le système d'information du laboratoire offrant ainsi la possibilité d'asservir les paramètres de ventilation en fonction des résultats sanguins.

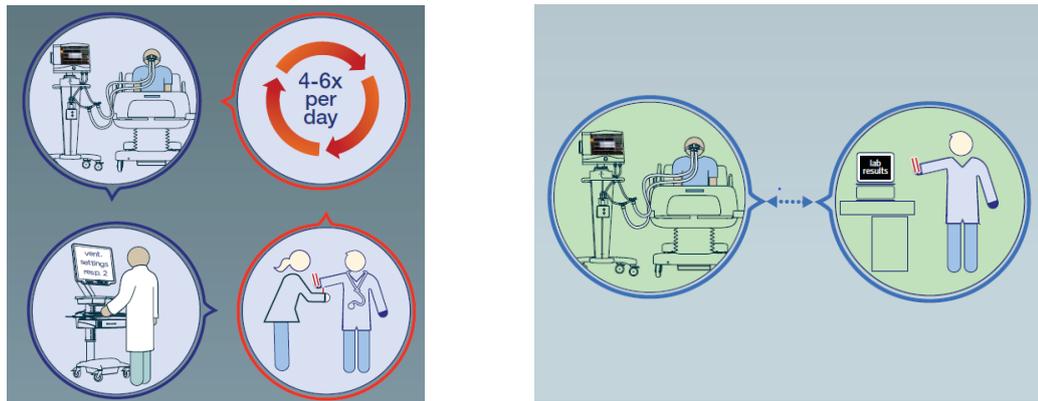


Figure 16 - Comparaison de la chaîne d'information en soins critiques sans interopérabilité (à gauche) et avec (à droite) [46]

Ces quelques exemples permettent d'illustrer la nécessité de développer l'interopérabilité des données biomédicales dans un souci de sécurité et de qualité de prise en charge du patient. De plus, l'exploitation de ces données à travers l'automatisation d'une multitude de flux permet de débarrasser les professionnels de tâches chronophages qui se substituent au temps qu'ils souhaitent dédier à leurs patients.

Impact financier

Au-delà de l'impact purement clinique, le manque d'interopérabilité a également un impact financier significatif pour le système de santé. En effet, en 2010, les dépenses de santé américaines représentaient environ 18% du PIB [48], soit 2400 G\$. Cependant, la part de dépenses dites « gaspillées » a été évaluée à environ 23 % (1700 G\$)[48], dont au moins 5% (35 G\$) sont directement imputables à la non-interopérabilité des dispositifs médicaux [46] (**figure 17**).

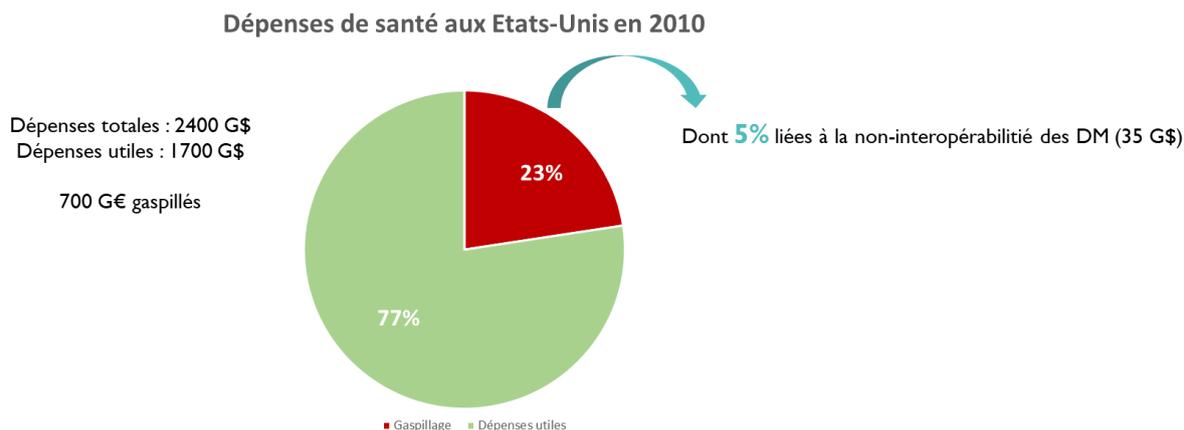


Figure 17 - Part des coûts induits par le manque d'interopérabilité sur les dépenses de santé américaines en 2010 [46] [48]

L'étude détaillée des postes de dépenses liés à la non-interopérabilité des dispositifs médicaux (**figure 18**) permet de mettre en évidence concrètement les enjeux de l'exploitation des données biomédicales dans les établissements de santé.

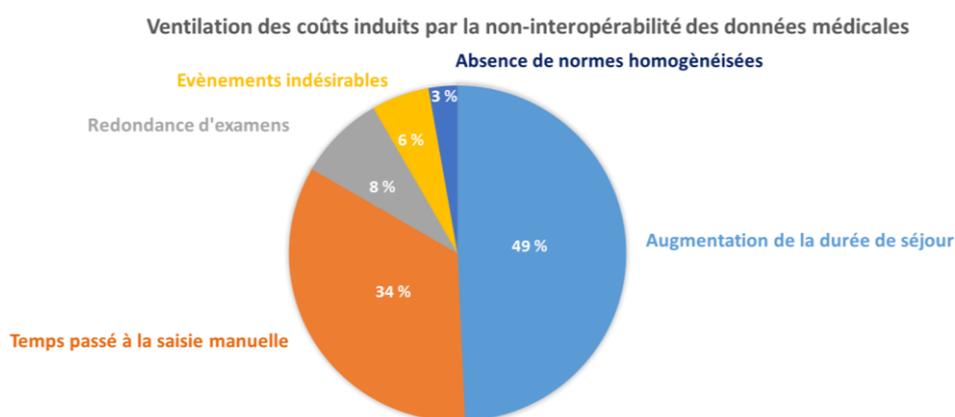


Figure 18 - Ventilation des coûts induits par le manque d'interopérabilité des données biomédicales [46]

Il apparaît que la moitié des dépenses sont générées par l'augmentation de la durée de séjour des patients, non pas pour des raisons médicales mais pour un défaut d'information, ce qui s'oppose totalement au développement des pratiques cliniques en ambulatoire. De plus, un tiers des dépenses sont liées au temps passé par les professionnels de santé à de la saisie manuelle d'informations, qui pourrait largement être automatisée, afin que ce temps puisse être dédié au patient [46].

Ainsi, le manque d'interopérabilité des données biomédicales génère des dépenses importantes pour le système de santé qui en 2023, ne sont plus justifiées.

En résumé, l'interopérabilité permet de produire des données structurées, interprétables et intégrées dans les pratiques cliniques. Cependant, elle n'est qu'une condition partielle à la bonne exploitation des données biomédicales dans un contexte hospitalier. En effet, ces données sont d'autant plus pertinentes et utilisables lorsqu'elles sont croisées entre elles et

accessibles par les professionnels de santé via une interface unique. Or actuellement, les architectures des systèmes d'information ne le permettent pas car sont encore construits sur des « silos de données ». En outre, la valorisation des données biomédicales doit être associée à un travail d'urbanisation augmentée du système d'information.

1.4 Urbanisation

L'urbanisation du système d'information désigne l'évolution de son architecture en rapport des besoins des usages métiers et des technologies. Il ne s'agit pas de supprimer la totalité du système (dossier patient, gestion administrative, logiciels métiers, etc....) mais bien de maintenir ses principales composantes dans une nouvelle structuration. En termes techniques, il s'agit de rendre le système d'information fiable selon des critères d'intégrité, de disponibilité, de confidentialité et d'audibilité [27] [49]. De plus le but est de mettre en œuvre une surveillance permanente et automatique des flux de données et de l'infrastructure physique et virtuelle. Enfin, l'urbanisation doit renforcer la flexibilité et la robustesse du système afin de le rendre résilient en cas de défauts de fonctionnement ou en cas d'évolution technologique [50].

Dans le contexte hospitalier et de l'informatique biomédicale, l'urbanisation du système d'information doit être orientée vers l'exploitation des données biomédicales, en les rendant structurées et accessibles. L'objectif est de collecter et de structurer les données contenues dans l'ensemble des systèmes de stockage différents afin de les valoriser. Cependant, au sein d'une architecture segmentée, les différents types de données sont produits et stockés dans des formats différents, dans une multitude d'outils non-communicants (**figure 19**).

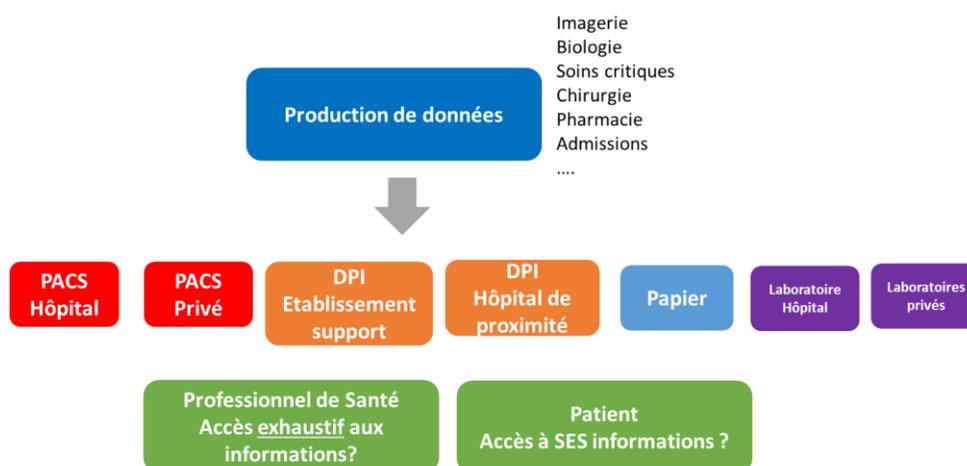


Figure 19 - Schématisation des silos de données biomédicales dans une architecture segmentée du système d'information

De fait, les professionnels de santé doivent se connecter sur chacun d'entre eux pour avoir accès aux informations : il y a autant d'interfaces que d'outils, ce qui ne rend pas l'ensemble utilisable au quotidien. Également, la structuration des données n'est pas homogénéisée en fonction des outils et des fabricants.

Ces disparités ne permettent pas l'analyse et le croisement des données, et par conséquent entravent l'implémentation et l'utilisation des outils d'intelligences artificielles à visés clinique et organisationnelle.

Face à ses constats, la DTS2IC a lancé à l'échelle du GHT, un chantier de réurbanisation augmentée de son système d'information en se dotant d'un concentrateur associé à un entrepôt de données de santé (**figure 20**).

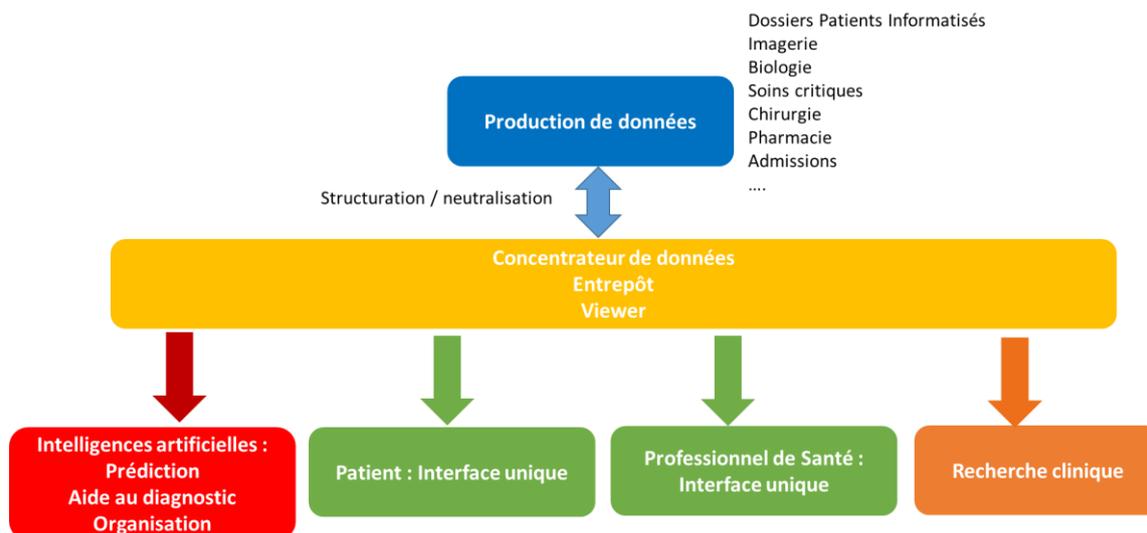


Figure 20 - Schématisation de l'urbanisation augmentée du système d'information

L'implémentation de cette nouvelle architecture a trois objectifs [51]:

- Collecter la totalité des données cliniques et les structurer ;
- Mettre à disposition les données de manière exhaustive aux professionnels de santé via une interface unique ;
- Valoriser les données (prédiction, exploitation, optimisation).

La valorisation des données concerne en particulier la recherche clinique, par la possibilité qu'offre le concentrateur d'établir des cohortes de patients sur diverses pathologies (cardiovasculaires, digestives, cancers, maladies infectieuses). Également, les données seront exploitées pour de la prédiction en alimentant des outils d'intelligences artificielles cliniques (analyse des signaux faibles sur les constantes vitales) ou organisationnelles (gestion des flux patients aux urgences selon la criticité, gestion en temps réel des lits disponibles). Enfin, les données seront également utilisées afin d'optimiser le Programme de Médicalisation des Systèmes d'Information (PMSI), dont dépend notamment le codage des actes médicaux [52].

1.5 Réglementation

En dépit du RGPD [19] qui encadre la protection des données à caractère personnel, le corpus réglementaire autour des dispositifs médicaux connectés au système d'information demeure restreint. En effet, contrairement aux risques physiques (électrique, mécanique, magnétique, etc...), les risques et contraintes numériques sont peu abordés dans le règlement européen 2017/745 relatif aux dispositifs médicaux [1] [53]:

- le paragraphe 14.5 du règlement stipule que « *Les dispositifs qui sont destinés à être mis en œuvre avec d'autres dispositifs ou produits sont conçus et fabriqués de manière à ce que leur interopérabilité et leur compatibilité soient fiables et sûres* ». Cependant, aucune norme nécessaire à l'obtention du marquage CE pour la mise sur le marché des dispositifs n'est relative à l'interopérabilité.
- l'article 103 qui impose la création d'un groupe de coordination européen des dispositifs médicaux [54], qui a produit en 2019 un guide à destination des fabricants relatif à la cybersécurité des dispositifs médicaux [55], qui n'a cependant pas de valeur légale.

A titre de comparaison, les industriels américains du dispositif médical se sont regroupés, à l'initiative de la National Electrical Manufacturers Association [56], pour construire un guide des bonnes pratiques autour de la sécurité des dispositifs médicaux (Medical Device Statement for Medical Device Security) [57]. Ce guide est décliné sous forme de questionnaire où les fabricants doivent exposer de manière transparente leurs choix en terme de sécurité. Largement adopté par les exploitants de dispositifs médicaux, ce questionnaire fait aujourd'hui consensus [53].

Concrètement, le niveau d'interopérabilité et de cybersécurité des dispositifs médicaux connectés demeurent à la libre appréciation des fabricants, où les établissements de santé n'ont d'autres choix que de s'y conformer. Ainsi, la DTS2IC a engagé l'internalisation des compétences correspondantes, en structurant l'informatique biomédicale comme un domaine d'expertise à part entière, qui doit s'intégrer dans la démarche de management de la qualité du service¹². C'est dans cette optique que la rédaction du document unique d'informatique biomédicale doit permettre de construire un socle commun entre les services supports, de soins et industriels.

¹² La direction des technologies en santé, de l'innovation et de l'ingénierie clinique est certifiée ISO 9001 sur le périmètre biomédical et en cours de certification ISO 270001 sur le périmètre du système d'information.

1.6 Document Unique

Le document unique d'informatique biomédicale vise à structurer et organiser la gestion de l'informatique biomédicale tant dans l'exploitation courante, que dans la gestion de nouveaux projets. Il doit permettre de cadrer les pratiques du point de vue technique, clinique, réglementaire et organisationnel entre toutes les parties prenantes. En effet, le but est que chaque professionnel (infrastructure, interopérabilité, sécurité, applicatif, biomédical, industriel) puisse s'y référer afin d'apporter un service de qualité, le plus rapidement possible, en vue de garantir la sécurité des patients et la continuité des soins. Le document unique est structuré en 4 grandes parties : la cartographie de la totalité de l'infrastructure d'informatique biomédicale, l'analyse de l'infrastructure avec les experts réseaux et le RSSI, la définition d'un plan d'action correctif et le transfert des compétences aux équipes supports.

Le plan d'action doit s'inscrire aussi bien sur le court terme avec mise en application immédiate pour les cas les plus urgents, qu'à plus long terme selon la politique générale de la DTS2IC.

2. Etude de l'architecture informatique biomédicale

A ce jour, onze cartographies de l'infrastructure informatique biomédicale ont été réalisées (imagerie, biologie, chirurgie, réanimation, unité de soins intensifs de cardiologie, unité kangourou, néonatalogie, cardiologie, dialyse, ECG connecté et échographie), et trois sont en préparation (bloc obstétrical, ophtalmologie et stérilisation). Elles sont visibles en annexes confidentielles.

2.1 Stratégie méthodologique

L'objectif du travail cartographique est d'être exhaustif sur les dispositifs médicaux connectés, les logiciels métiers, l'infrastructure réseau et les flux de données. Au regard de la taille du système d'information, il est impératif d'adopter une méthode d'investigation qui se décline ici en six phases :

- 1 - Inventaire des dispositifs médicaux connectés du service/plateau concerné ;
- 2 - Etude des usages cliniques des dispositifs avec les professionnels de santé ;
- 3 - Inventaire et étude de l'environnement applicatif avec les professionnels de santé, les référentes cliniques et les experts informatiques ;
- 4 – Etude de l'infrastructure informatique avec les experts réseaux ;
- 5 – Relevé des flux et formats de données avec les experts interopérabilité, applicatif et les éditeurs et fabricants ;
- 6 – Vérification de l'ensemble en sondant chaque composant de la chaîne d'information avec des profils de patients fictifs.

La qualité des résultats est conditionnée par la bonne compréhension des usages cliniques : il est nécessaire de passer du temps dans les services pour se saisir des pratiques.

2.2 Dispositifs médicaux connectés

Sur le site de Chalon, on dénombre une quinzaine de types de dispositifs médicaux connectés dont :

- Les équipements d'imagerie : échographie, radiologie conventionnelle, radiologie interventionnelle, mammographie, scanner et IRM ;
- Le parc d'échographes répartis dans tous les services ;
- Le monitoring multiparamétrique ;
- Le monitoring des signes vitaux ;
- L'électrocardiographie ;
- Les cardiographes ;
- La télémétrie en cardiologie ;
- La perfusion : pushes-seringues et pompes ;
- Les générateurs de dialyse ;
- Les pompes à nutrition ;
- La ventilation : soins critiques et anesthésie ;
- Les colonnes de coelioscopie ;
- Le système de routage d'images au bloc opératoire ;
- Les incubateurs ;
- Les automates du laboratoire : chaîne pré-analytique, biologie, biochimie, hémostase, hématologie, biologie moléculaire, bactériologie, spectrométrie de masse.

La majorité des équipements sont connectés physiquement au réseau par des câbles RJ45 qui supportent le protocole Ethernet, ou en WIFI. L'attribution des adresses IP est effectuée en accord avec le plan d'adressage et de segmentation réseau du GHT. En effet, les dispositifs médicaux sont connectés sur différents VLAN¹³ en fonction de leur type et de leur criticité clinique. Cette segmentation¹⁴ structure l'infrastructure biomédicale dans le système d'information et assure un premier niveau d'isolation en cas d'incident. Cependant, un second niveau de segmentation est mis en place par une technique de routage virtuel¹⁵ qui permet d'isoler des zones (composées de plusieurs VLAN). Par exemple, les moniteurs multiparamétriques et les pompes à perfusion sont connectés sur des VLAN différents mais routés virtuellement dans une même zone. Ainsi, les dispositifs médicaux des soins critiques, dont font parties les moniteurs et les pompes à perfusion, sont isolés du reste du réseau. Par conséquent, un incident interne à la zone est contenu donc ne se propage pas sur toute l'infrastructure, et inversement, un incident externe à la zone (sur un ordinateur du laboratoire de biologie par exemple) ne vient pas se propager sur l'infrastructure réseau des soins critiques. Les zones sont établies pour chaque SIE (exemple : imagerie, biologie, chirurgie, maternité, soins critiques, régulation du SAMU, pharmacie, etc...).

¹³ VLAN : Virtual Local Area Network

¹⁴ La répartition des dispositifs médicaux sur différents VLAN correspond à une segmentation au niveau 2 du modèle OSI [58].

¹⁵ Le routage virtuel correspond à une segmentation au niveau 3 du modèle OSI [58].

Les modalités d'intégration varient en fonction des dispositifs médicaux et de la capacité ou volonté des fabricants à rendre leurs équipements interopérables. Au sein du GHT, quatre méthodes de connexions sont utilisées :

- connexion directe entre le dispositif médical (DM) et l'EAI biomédical ;
- connexion du DM à un serveur applicatif intermédiaire ;
- connexion du DM à un module propriétaire ;
- connexion du DM à un réseau applicatif dédié.

Les spécificités des différentes modalités de connexion sont abordées plus en détails dans la partie 2.4 *Echanges de données et orientation des flux* (p25).

2.3 Structuration des données

La qualité de structuration des données repose essentiellement sur l'application des standards internationaux DICOM et les différentes normes HL7. On distingue trois scénarios sur les dispositifs médicaux du GHT : l'interopérabilité totale des données, l'interopérabilité partielle et la non-interopérabilité.

Concernant les dispositifs médicaux totalement interopérables, aucune action n'est réalisée sur les données. Leur intégration est directe dans les logiciels métiers. Dans certains cas, les logiciels métiers produisent des comptes-rendus et/ou documents médicaux où les données sont mises en forme. Ces documents sont automatiquement envoyés dans le dossier patient informatisé, *Mon Espace Santé* ou dans les logiciels métiers d'autres spécialités médicales. Ces échanges de documents sont également structurés et construits sur les standards HL7. L'interopérabilité totale des dispositifs médicaux permet de les intégrer dans des logiciels édités par des industriels autres que le fabricant du DM. Au sein du parc d'équipements du GHT, les dispositifs concernés sont :

- La perfusion ;
- La dialyse (en réanimation) ;
- L'échographie (échographes + système de désinfection des sondes) ;
- L'imagerie ;
- Le laboratoire (automates de toutes spécialités confondues) ;
- L'ECG.

Certains dispositifs médicaux n'offrent qu'une interopérabilité partielle. En effet, leurs flux de données doivent être consolidés par diverses transformations afin de répondre aux standards internationaux en vue de leur intégration dans les logiciels métiers. Les transformations opérées sur la structure des données sont réalisées sur un EAI¹⁶ dédié aux applications biomédicales.

¹⁶ EAI : Enterprise Application Integration , système permettant de centraliser, de surveiller et de transformer les flux de données

Ce type d'architecture est pour l'instant utilisé dans les soins critiques pour l'alimentation automatique de la feuille de réanimation et pour l'externalisation des alarmes (**figure 21**), mais également au bloc pour l'alimentation de la feuille d'anesthésie.

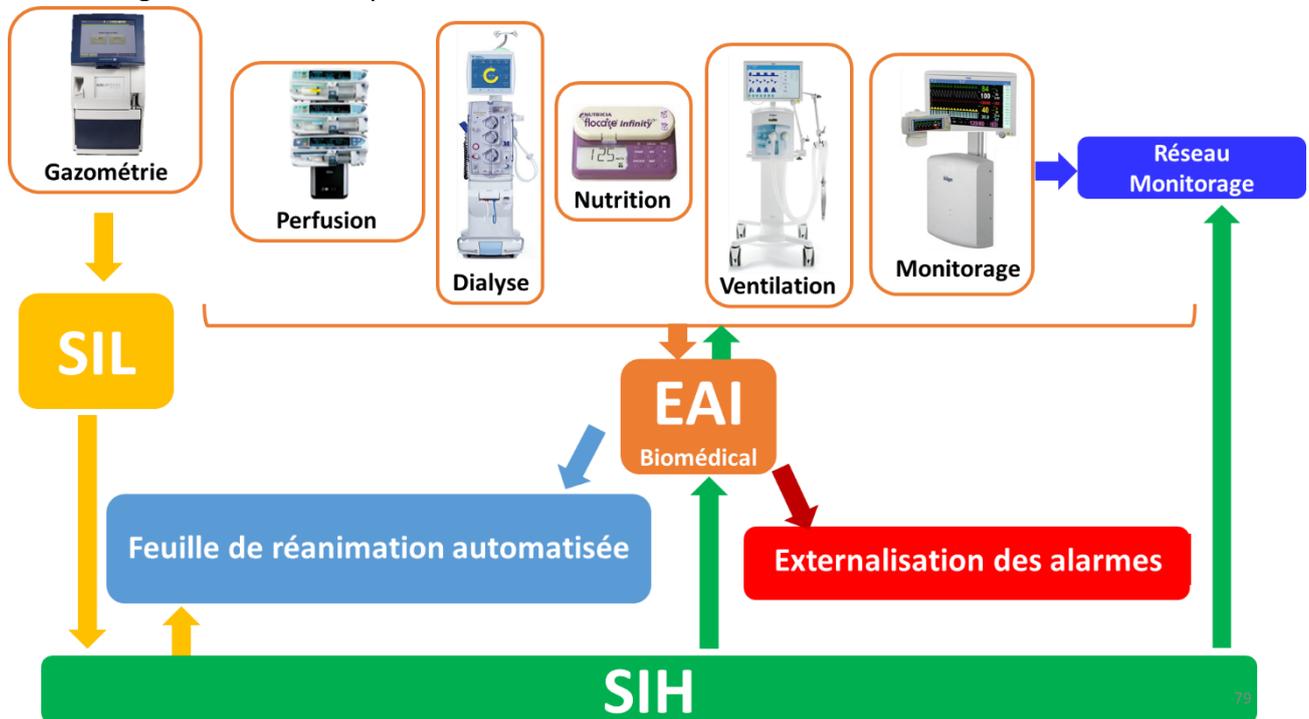


Figure 21 - Schématisation de l'architecture informatique biomédicale en réanimation – source : auteur

A noter que ce type d'architecture nécessite des pilotes et des bibliothèques informatiques fournis par les fabricants de dispositifs médicaux.

Enfin, certains dispositifs médicaux ou logiciels métiers demeurent non-interopérables. En effet, l'intégration des dispositifs n'est possible que par l'intermédiaire de commutateurs (box) propriétaires, vendus avec le dispositif ou avec le logiciel métier. De fait, l'exploitation des données est rendue captive par le fournisseur. Ce type de problématique est encore rencontrée sur le plateau de dialyse, pour l'envoi des données entre les générateurs et la feuille de dialyse automatisée.

2.4 Echanges de données et orientation des flux

Les flux de données transitant entre les dispositifs et les applications, ou entre deux applications sont orientés de manière centralisée. En effet ce type de routage est mis en œuvre par l'EAI qui, en plus de la transformation des données, permet de centraliser les flux afférents en un seul point de connexion, pour les redistribuer à autant d'applications et logiciels métiers que nécessaire. Ce procédé permet également de superviser en temps réel les flux, avec un système d'alerte lorsqu'une erreur d'adressage, d'intégration ou de format est détectée. Au niveau du GHT, le routage des flux via l'EAI est en voie de généralisation pour l'ensemble des dispositifs médicaux connectés, en remplacement des commutateurs (box) propriétaires qui ne permettent pas de superviser les flux de données en temps réel. De plus,

dans le but de fiabiliser l'identitovigilance¹⁷, les dispositifs médicaux connectés et les logiciels métiers sont systématiquement alimentés par un flux de données issues du logiciel de gestion administrative du malade (GAM), qui permet d'associer nativement l'identité du patient aux données biomédicales produites.

2.5 Stockage des données

Le stockage des données biomédicales et documents médicaux associés sont stockés dans trois types de systèmes différents :

- Le Dossier Patient Informatisé (DPI) ;
- Les logiciels métiers à travers des bases de données dédiées ;
- Le PACS pour les images.

Ces systèmes de stockage sont actuellement en cours de déploiement à l'identique dans la totalité des établissements du GHT afin de mutualiser les outils cliniques sur tout le territoire. Comme évoqué précédemment en partie 1.4 *Urbanisation (p19)*, l'implémentation d'un concentrateur de données, couplé à un entrepôt de données de santé homologué par la CNIL, va permettre de croiser les données entre-elles, indépendamment de leur système de production. Aussi, l'entrepôt de santé offrira une simplification de gestion et de gouvernance dans la mesure où les données seront toutes standardisées, stockées et structurées de façon identique. Par conséquent, si un jour la DTS2IC vient à changer d'éditeur de DPI, l'antériorité des données produites sous l'ancien système sera conservée dans l'entrepôt de données. Il en va de même pour les changements de logiciels métiers qui ne permettent que rarement le transfert de bases de données entre l'ancien et le nouveau logiciel. Cette problématique d'accessibilité à l'historique des données en cas de changement de version ou d'éditeur de logiciel est fréquente et peu induire des difficultés juridiques.

En effet, l'article R1112-7 du Code de la Santé Publique [60] stipule que les établissements de santé ont l'obligation de conserver les données médicales du patient en base active¹⁸ sur une durée de 20 ans à compter du dernier passage du patient dans l'établissement pour une hospitalisation ou une consultation externe. Une première exception est faite pour les patients décédés moins de 10 ans après leur dernier passage à l'hôpital où les données sont à conserver 10 ans à compter de la date du décès. Une seconde exception concerne les mineurs, où les données doivent être conservées 10 ans à compter de leur majorité [60].

Concrètement, le développement technologique actuel fait qu'il est peu probable qu'un logiciel clinique ne soit pas renouvelé avant 20 ans d'exploitation : d'où l'urgente nécessité de stocker les données biomédicales neutralisées dans un entrepôt de données de santé indépendant.

¹⁷ Identitovigilance : ensemble de mesures garantissant la bonne identité du patient auprès des professionnels de santé durant tout son parcours de soins [59]

¹⁸ Données en base active : données accessibles rapidement (pas de compression, etc...)

3. Préconisations et plan d'action

Le travail cartographique a permis de dresser un premier bilan de l'état de l'infrastructure d'informatique biomédicale et d'engager rapidement des actions correctives pour les cas les plus à risque.

3.1 Criticité et corrections

A ce jour, plusieurs points de criticité ont été identifiés sur l'infrastructure informatique biomédicale : la disponibilité, le maintien opérationnel, l'obsolescence et les dépendances techniques interservices.

La disponibilité caractérise la capacité technique d'un système informatique à assurer un service dans le temps. Plus la disponibilité est haute, moins l'utilisateur est impacté par des interruptions (indisponibilité) de l'équipement ou du logiciel.

Elle est jugée insuffisante pour un certain nombre de logiciels métiers dont l'infrastructure n'est pas à minima doublée. Cela peut entraîner une indisponibilité du logiciel en cas de défaillance technique. Les impacts sur les patients et les professionnels de santé sont doubles :

- une désorganisation massive du service de soins qui peut induire des erreurs et donc des pertes de chance pour le patient ;
- une perte de données cliniques durant le temps mort (**figure 22**), qui peut être préjudiciable au patient en fonction de la durée et du système.

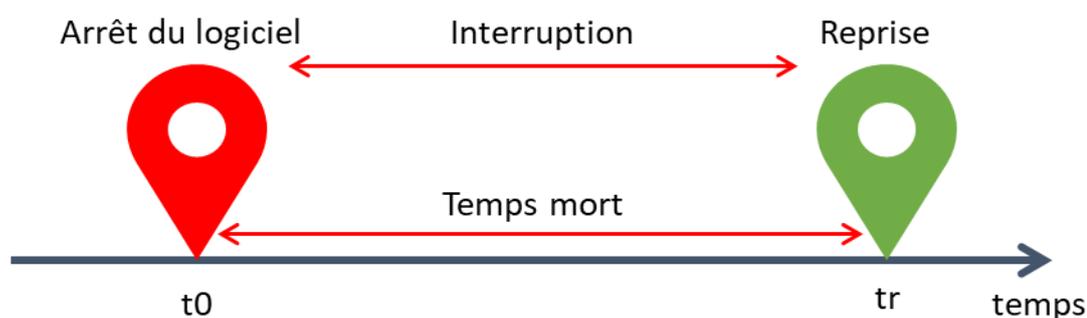


Figure 22 - Illustration du temps mort lors de l'interruption d'un service, logiciel ou équipement – source : auteur

L'objectif en terme d'ingénierie clinique, est de minimiser les durées d'interruption et de faire évoluer l'infrastructure des logiciels cliniques vers de la haute disponibilité afin que les durées d'interruption soient transparentes pour les soignants.

L'infrastructure informatique biomédicale subit également des difficultés de maintien opérationnel. En effet, les logiciels cliniques ne sont pas systématiquement implémentés sur des serveurs doublés : un de production et un de secours, avec un processus de bascule

automatique ou manuel entre les deux machines. Par conséquent, les techniciens informatiques rencontrent des difficultés à maintenir à jour les serveurs concernés puisqu'ils ne peuvent pas interrompre le fonctionnement des logiciels pour effectuer les montées de version. A terme, le risque est l'obsolescence du logiciel concerné, ce qui représente une vulnérabilité conséquente dans le système d'information. Face à ce genre de situation, tous les nouveaux logiciels cliniques seront installés sur une infrastructure doublée (exigence dans le cahier des charges), permettant d'effectuer les mises à jour sans interruption pour les professionnels de santé.

L'absence de mises à jour effectives conduit l'infrastructure à un état d'obsolescence dont le support n'est plus assuré par les fabricants. L'obsolescence informatique constitue un risque majeur pour la sécurité de l'établissement face à la cybermenace, puisque les failles techniques non corrigées (plus de support) sont des points d'entrées dans le système d'information. Au niveau de l'infrastructure informatique biomédicale, l'obsolescence affecte certains logiciels cliniques et leurs serveurs, mais également des dispositifs médicaux.

Concernant les logiciels, la cause identifiée porte sur le développement du logiciel en lui-même, qui ne supporte pas les dernières versions de système d'exploitation. La solution technique la plus simple est de remplacer le logiciel par un système plus récent. Cependant, pour un besoin clinique bien identifié, il n'existe pas forcément d'alternative sur le marché des logiciels cliniques à fonctionnalités égales. Là est toute la complexité de l'informatique biomédicale : les besoins cliniques ne sont pas systématiquement compatibles avec les exigences techniques. L'arbitrage doit reposer sur une pondération rigoureuse et objective des impacts et des risques associés au maintien d'un logiciel clinique obsolète mais utilisé.

A propos des dispositifs médicaux, la problématique est identique : certains dispositifs très spécifiques ne répondent plus aux exigences de sécurité informatique.

Enfin, le dernier point critique identifié sur l'infrastructure informatique biomédicale est la dépendance technique entre les services de soins. En effet, certains logiciels cliniques utilisés dans différents services de soins partagent une infrastructure commune.

Par exemple le logiciel A et le logiciel B partagent le même serveur d'interface. Une mise à jour du logiciel A a été programmée sur un créneau de fermeture du service de soins A . Cependant, la mise à jour du logiciel A entraîne une panne sur le serveur d'interface commun : c'est le logiciel B qui est impacté, or le service de soins B est en pleine activité. Ainsi, ces liens de dépendance technique entre plusieurs services de soins représentent un risque élevé pour les patients. Historiquement, ce type d'architecture a été mise en place dans un objectif de rationalisation technique et financière, sans analyse de risque. Sur le site de Chalon, quatre logiciels sont concernés (2x2). Un chantier de dédoublement de l'infrastructure pour chacun des logiciels est en cours d'élaboration.

Les différents points de criticité évoqués ci-dessus mettent en évidence les divergences voire les contradictions qu'il a existé jusqu'à présent entre la vision technique et la vision clinique de l'infrastructure informatique biomédicale. Objectivement, il ne s'agit pas de les opposer mais bien d'analyser les risques inhérents à chacune afin de trouver le meilleur compromis

entre usages cliniques et sécurité du système d'information. Néanmoins, il est impératif que les besoins cliniques guident les besoins techniques et non l'inverse.

3.2 Analyse des risques

Comme évoquée précédemment, la vision des risques cliniques s'entrechoque avec celle des risques techniques. Pour pallier à ces difficultés, il a été décidé, avec le RSSI du GHT, de réaliser des analyses de risques sur toute la chaîne de traitement des données biomédicales. Ainsi, les dispositifs médicaux et leurs usages ne sont plus analysés indépendamment, mais de manière intégrée dans le système d'information.

Chaque composant de la chaîne d'information est analysé selon une échelle de risques pour le patient et une échelle de risques liés aux systèmes d'information (**figure 23**)

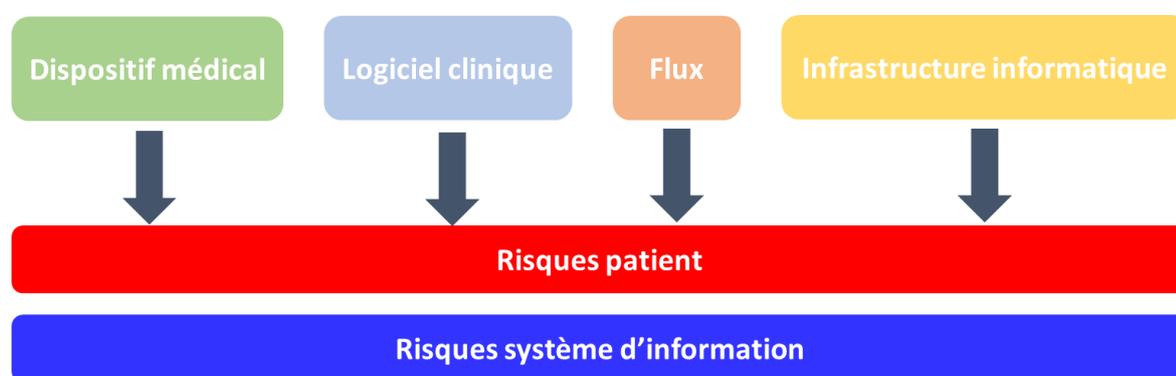


Figure 23 - Principe d'analyse des risques sur toute la chaîne de données biomédicales – source : auteur

Dans ce processus d'analyse, les risques patients ne sont pas limités aux dispositifs médicaux mais intègrent également les usages des technologies par les professionnels de santé et l'organisation du service autour des données biomédicales. Prenons par exemple le cas de l'ECG numérique (**figure 24**)

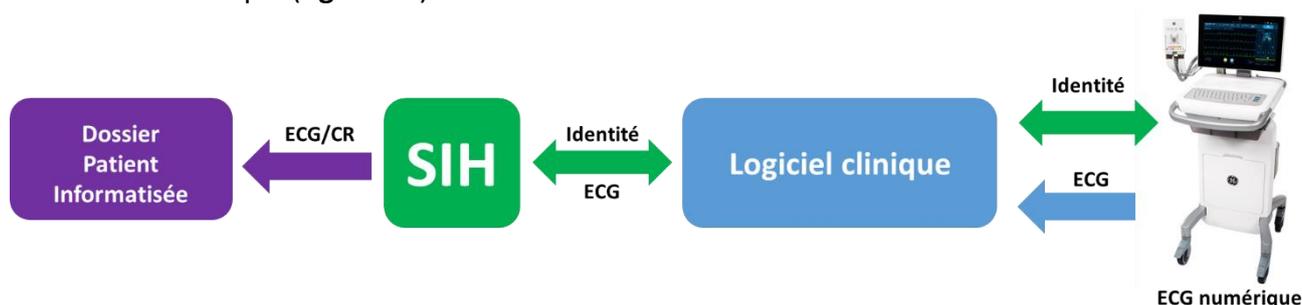


Figure 24 - Schéma de la chaîne d'information biomédicale pour l'ECG numérique – source : auteur

Au sein de l'établissement, les professionnels de santé peuvent réaliser des électrocardiogrammes numériques : une fois l'acquisition des signaux cardiaques effectuée, le tracé est automatiquement envoyé dans un logiciel de post-traitement permettant de réaliser des mesures et d'éditer le compte-rendu. Une fois finalisé, le document (tracé ECG + compte-rendu) est envoyé dans le dossier informatisé du patient. A noter que l'équipement peut imprimer les tracés à tout moment. Dans ce cas, l'analyse de risques patient sur le dispositif médical ne doit pas se limiter à sa capacité de réaliser ou non le tracé. Elle doit

également évaluer les conséquences qu'aurait un défaut d'envoi des tracés numériques dans le dossier patient, obligeant les services de soins à se réorganiser autour des tracés en format papier.

Dans le cadre de l'organisation interne à la DTS2IC, les analyses de risques de bout en bout sur l'informatique biomédicale seront obligatoires pour la qualification de nouveaux projets comprenant des dispositifs médicaux connectés, et leur mise en production. De plus, ce processus d'analyse de risque sera intégré dans le système de management de la qualité sous les deux périmètres (ISO 9001 pour le biomédical et ISO 27001 pour le système d'information), et dans la politique de sécurité des systèmes d'information du GHT.

Enfin, ces analyses de risques seront intégrées aux déclarations périodiques des SIE à l'ANSSI dans le but de les rendre les plus exhaustives possibles.

3.3 Partenariats

La maîtrise des risques en informatique biomédicale ne peut être effective sans l'appui des industriels du dispositif médical, des données biomédicales et des systèmes d'information. L'intégration des dispositifs médicaux doit faire l'objet d'un travail collectif tant sur le développement que sur l'exploitation. Les sujets d'interopérabilité et de sécurité doivent faire l'objet d'intérêts communs entre toutes les parties prenantes, sans quoi les projets ne peuvent aboutir. Dans cette optique, la DTS2IC a réuni ses partenaires industriels historiques pour mettre en œuvre et solutions techniques et financières adaptées.

III. Organisation des fonctions supports et évolution de l'ingénierie biomédicale

1. Organisation

Historiquement, les responsabilités et les champs d'applications des fonctions supports (informatique et biomédical) étaient définies selon une logique d'infrastructure : le service biomédical s'occupait des dispositifs médicaux et le service informatique des ordinateurs, serveurs et autres périphériques réseaux. Cependant, cette vision occultait les problématiques sous-jacentes spécifiques aux données biomédicales : la sécurité, l'interopérabilité, le stockage et les usages cliniques associés. Ainsi, la considération de la donnée biomédicale appelle les services informatiques et biomédicaux à ne pas se contenter de collaborer mais bien à faire converger leurs expertises et à les hybrider sur tout un périmètre commun.

La direction du GHT Saône et Loire Bresse Morvan a opté pour une organisation mutualisée et intégrée, avec à sa tête un directeur définissant une politique générale commune, basée sur une stratégie territoriale. Cette organisation offre l'avantage d'une transversalité totale entre tous les professionnels et une cohérence des projets technologiques. Les chantiers en cours montrent que des problématiques initialement spécifiques aux dispositifs médicaux ont catalysé une réflexion globale qui a été étendue au système d'information et inversement. La

proximité des deux spécialités dans la gestion de projet, l'obligation de résultats envers les professionnels et les patients et la démarche qualité, permet de mutualiser des outils, de transférer des compétences et de confronter des cultures technologiques différentes. Ce décloisonnement montre aujourd'hui ses premiers résultats qui confortent la DT2IC à poursuivre son développement sur la même voie.

Néanmoins, même si le rapprochement entre les services biomédicaux et informatiques est aujourd'hui inexorable, ce modèle d'organisation n'est pas la seule réponse possible. En effet, même si dans le cas de la DTS2IC, c'est le biomédical qui a « absorbé » le service informatique, l'inverse est également totalement envisageable pour un autre GHT. L'enjeu n'est finalement pas de savoir quel service va absorber l'autre, mais bien d'avoir à la tête de l'ensemble un directeur dont la vision est suffisamment ouverte et stratégique pour porter un projet mutualisé des technologies en santé ambitieux et à la hauteur de la qualité de service à apporter aux professionnels des établissements de santé.

2. Compétences

En terme de compétences, les directions des fonctions supports (indépendamment de leur modèle organisationnel) doivent intégrer de nouveaux profils en adéquation avec l'évolution technologique (très rapide) en santé, autour de deux axes :

- L'habilitation aux usages des technologies en santé ;
- L'informatique biomédicale et le numérique en santé.

Le niveau technologique des dispositifs médicaux et logiciels devenant de plus en plus élaboré, il est nécessaire de garantir aux professionnels de santé un socle minimal de compétences et connaissances autour de leurs usages. C'est la mission des référents cliniques, qui sont des professionnels de santé (médecins, infirmiers, aides-soignants), dont une partie de leur temps dans l'établissement est dédié à l'accompagnement de leurs pairs sur les usages technologiques. Ces référents cliniques assurent un lien de communication solide entre les services de soins et les experts de la DTS2IC, ce qui permet de faire remonter rapidement certaines problématiques ou difficultés rencontrées au quotidien. Les référents cliniques bénéficient de formations régulières et approfondies de la part des industriels, afin de maintenir leur niveau d'expertise. Ils organisent également des formations autour du dispositif médical et logiciel clinique en lien avec les centres de formations du GHT : l'IFSI¹⁹, le CESU²⁰ et le CESITECH²¹.

L'intégration des dispositifs médicaux dans le système d'information et l'exploitation des données biomédicales implique aujourd'hui de développer des profils à doubles compétences entre l'ingénierie biomédicale et l'informatique hospitalière. Il s'agit d'être capable de

¹⁹ IFSI : Institut de Formation en Soins Infirmiers.

²⁰ CESU : Centre d'Enseignement des Soins d'Urgence.

²¹ CESITECH : Centre d'Enseignement et de Simulation du Territoire Chalonais.

maîtriser la totalité de la chaîne de traitement des données biomédicales en gérant au quotidien des problématiques spécifiques aux dispositifs médicaux ou au système d'information. Au-delà des compétences technologiques, il est impératif de se saisir des exigences relatives à l'organisation des services de soins, des pratiques cliniques et des attentes des professionnels de santé. En effet, la bonne intégration des technologies est la garantie de leur utilisabilité. Les ingénieurs et techniciens en informatique biomédicale doivent donc établir un lien important avec les professionnels de santé, avec l'aide des référents cliniques.

3. Réglementation

Le développement de l'informatique biomédicale et plus généralement du numérique en santé ne dépend pas seulement de l'évolution des fonctions supports. Il doit également être accompagné d'une adaptation du cadre réglementaire autour de l'interopérabilité et de la sécurité. La feuille de route du numérique portée par la Délégation ministérielle au numérique en santé (DNS) [12] va dans le bon sens mais mériterait cependant que le législateur se saisisse de ses questions en profondeur afin de poser un cadre facilitant l'implémentation des outils numériques cliniques dans les établissements de santé. Cette évolution est également attendue au niveau européen pour en faire un critère de mise sur le marché des dispositifs médicaux.

Concernant les systèmes d'information hospitaliers, la création d'un corpus réglementaire spécifique aux établissements de santé permettrait de structurer de manière homogène l'activité des fonctions supports et des industriels du secteur, au même titre que cela est effectif pour les exploitants de dispositifs médicaux.

Conclusion

L'objectif de cette année d'alternance était de profiter de la création de la DTS2IC pour développer des compétences hybrides entre l'ingénierie biomédicale et le système d'information. Mon projet portait sur la création du document unique d'informatique biomédicale qui a pour but de structurer la nouvelle activité d'informatique biomédicale, autour de quatre axes : la cartographie exhaustive de l'infrastructure, son analyse pour identifier les points de vulnérabilité, l'engagement des corrections dans les cas les plus critiques et enfin le transfert de la maîtrise en exploitation aux techniciens biomédicaux et informatiques.

A date, onze cartographies ont été réalisées (imagerie, biologie, chirurgie, réanimation, unité de soins intensifs de cardiologie, unité kangourou, néonatalogie, cardiologie, dialyse, ECG connecté et échographie), et trois sont en préparation (bloc obstétrical, ophtalmologie et stérilisation). Les vulnérabilités les plus importantes ont été corrigées en imagerie, échographie, soins critiques et biologie. Une méthode d'analyse des risques spécifique à l'informatique biomédicale a été établie, les premières analyses sont en cours de réalisation. De plus, des groupes de travail avec les industriels partenaires ont été initiés en vue de l'évolution et de la sécurisation de l'infrastructure. En outre, les procédures de maîtrise en exploitation sont en cours de rédaction pour la totalité du plateau technique. La finalisation du document unique sera effective début 2024.

Parallèlement, j'ai développé des compétences en gestion de projet, ayant à charge la restructuration de l'infrastructure informatique en imagerie, le redéploiement d'un logiciel clinique en cardiologie et le développement de nouvelles solutions d'interopérabilité. Enfin, j'ai pu prendre part à la gestion de crise et à la mise en œuvre du plan de continuité de l'activité médicale.

Je retire de cette année d'alternance une grande satisfaction professionnelle et personnelle, qui me conforte dans ma volonté d'accompagner les établissements de santé publics dans leur modernisation et leur sécurisation, et les professionnels de santé dans leurs usages.

Je ne peux que recommander aux étudiants de se lancer dans l'alternance au sein des établissements de santé où les missions ne manquent pas.

Enfin, je souhaite vivement continuer à porter l'informatique biomédicale au sein du GHT Saône et Loire Bresse Morvan, qui demeure pour moi, un modèle inspirant de management des technologies en santé.

Bibliographie

- [1] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (Texte présentant de l'intérêt pour l'EEE.), Journal officiel de l'Union européenne, <https://eur-lex.europa.eu>, mai 2017. [En ligne]. Disponible sur: <http://data.europa.eu/eli/reg/2017/745/oj/fra>
- [2] Ministère de la Santé et de la Prévention, « GHT: Saône-et-Loire-Bresse Morvan ». 2017. [En ligne]. Disponible sur: <https://solidarites-sante.gouv.fr/IMG/pdf/bfc-01.pdf>
- [3] Centre hospitalier Chalon-sur-Saone, « Le Groupement Hospitalier de Territoire ». <https://www.ch-chalon71.fr/le-groupement-hospitalier-de-territoire/> (consulté le 4 janvier 2023).
- [4] *LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé*. 2016.
- [5] Santé Bourgogne-Franche-Comté, « Projet régional de santé (PRS) 2018-2028 », 2018. <https://www.bourgogne-franche-comte.ars.sante.fr/projet-regional-de-sante-prs-2018-2028> (consulté le 4 janvier 2023).
- [6] Centre hospitalier Chalon-sur-Saone, « Chiffres clés 2021 ». 2022. [En ligne]. Disponible sur: <https://allisapp.fr/wp-content/uploads/2021/09/Chiffres-cles-2021-web.pdf>
- [7] A. Weider, « Le numérique au service du parcours de soins : un enjeu du projet managérial du directeur des soins », déc. 2014, [En ligne]. Disponible sur: <https://documentation.ehesp.fr/memoires/2013/ds/franzi.pdf>
- [8] Direction de l'Hospitalisation et de l'Organisation des Soins et Ministère de la Santé, de la Famille et des Personnes handicapées, « Hôpital 2007 : un plan réformateur et innovant ». juin 2003. [En ligne]. Disponible sur: https://sante.gouv.fr/IMG/pdf/lettre_h2007_1.pdf
- [9] Ministère de la Santé et de la Prévention, « Le programme hôpital numérique ». <https://sante.gouv.fr/systeme-de-sante/e-sante/sih/hopital-numerique/Hopital-Numerique>
- [10] Ministère de la Santé et de la Prévention, « Ma santé 2022 : un engagement collectif », septembre 2018. <https://sante.gouv.fr/systeme-de-sante/masante2022/>
- [11] Agence du numérique en santé, « Le Ségur du numérique en santé ». <http://esante.gouv.fr/segur> (consulté le 20 juin 2023).

- [12] Délégation ministérielle au numérique en santé (DNS), « Feuille de route du numérique en santé 2023-2027 ». mai 2023. [En ligne]. Disponible sur:
https://esante.gouv.fr/sites/default/files/media_entity/documents/dns-feuille-de-route-2023-2027.pdf
- [13] Mon Espace Santé, « Mon espace santé - Vous avez la main sur votre santé ». <https://www.monespacesante.fr/> (consulté le 21 juin 2023).
- [14] Ministère de la Santé et de la Prévention et Agence du numérique en santé, « Comprendre le Ségur du numérique en santé - Présentation, objectifs et périmètre ». avril 2023. [En ligne]. Disponible sur:
https://esante.gouv.fr/sites/default/files/media_entity/documents/Segur_ChantierD_DocCommun_VF.pdf
- [15] Institut national de la statistique et des études économiques (INSEE), « Répertoire national d'identification des personnes physiques », octobre 2022.
<https://www.insee.fr/fr/information/5019311>
- [16] Ministère de la Santé et de la Prévention et Agence du numérique en santé, « Répertoire RPPS », *Agence du Numérique en Santé*. <http://esante.gouv.fr/produits-services/repertoire-rpps>
- [17] Groupement d'Intérêt Economique SESAM-Vitale, « L'ordonnance numérique ». <https://www.sesam-vitale.fr/e-prescription>
- [18] Ministère de la Santé et de la Prévention et Agence du numérique en santé, « Le partage national d'imagerie médicale ». <http://esante.gouv.fr/segur/imagerie/imagerie-DRIM-M>
- [19] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)*, vol. 119. 2016. [En ligne]. Disponible sur: <http://data.europa.eu/eli/reg/2016/679/oj/fra>
- [20] Ministère de la Santé et de la Prévention et Agence du numérique en santé, « Dispositifs médicaux numériques (DMN) ». <http://esante.gouv.fr/dispositifs-medicaux-numeriques>
- [21] Assurance Maladie, « Liste des produits et prestations - LPP », juin 2023.
http://www.codage.ext.cnamts.fr/codif/tips/index_presentation.php?p_site=AMELI
- [22] Article L1111-8-2 - Code de la santé publique .
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036515017/2020-10-01
- [23] *Décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information*. 2022.

- [24] Agence du numérique en santé, Ministère de la Santé et de la Prévention, et CERT Santé, « Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social Rapport public ». juin 2023.
- [25] Ministère de l'économie, des finances et de la souveraineté industrielle et numérique et Direction générale de la concurrence de la consommation et de la répression des fraudes, « Phishing (hameçonnage) », mars 2022. <https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage> (consulté le 15 juin 2023).
- [26] Agence nationale de la sécurité des systèmes d'information, « Rançongiciel », *Cybercriminalité*. <https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiel/> (consulté le 15 juin 2023).
- [27] Agence nationale de sécurité du médicament des produits de santé, « Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel Au cours de leur Cycle de Vie ». septembre 2022.
- [28] J. C. Laprie, B. Courtois, M. C. Gaudel, et D. Powell, *Sûreté de fonctionnement des systèmes informatiques*. in Dunos-Bordas. 1989.
- [29] Régime juridique des dispositifs médicaux (Articles R5211-1 à R5211-71) - Code de la santé publique . juin 2023. [En ligne]. Disponible sur: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006178665/
- [30] *Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique*. 2018.
- [31] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, vol. 194. 2016. Consulté le: 14 juin 2023. [En ligne]. Disponible sur: <http://data.europa.eu/eli/dir/2016/1148/oj/fra>
- [32] *LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*. 2018.
- [33] *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE)*, vol. 333. 2022. Consulté le: 14 juin 2023. [En ligne]. Disponible sur: <http://data.europa.eu/eli/dir/2022/2555/oj/fra>

- [34] Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ». <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012> (consulté le 15 juin 2023).
- [35] Agence nationale de la sécurité des systèmes d'information, « FAQ – Opérateurs de services essentiels (OSE) ». <https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/> (consulté le 15 juin 2023).
- [36] Healthcare Information and Management Systems Society, « Interoperability in Healthcare », aout 2020. <https://www.himss.org/resources/interoperability-healthcare> (consulté le 16 juin 2023).
- [37] Norme ISO/IEC/IEEE 8802-3:2021, Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks — Part 3: Standard for Ethernet , février 2021.
- [38] Norme ISO/IEC/IEEE 8802-11:2018 Télécommunications et échange entre systèmes informatiques — Exigences pour les réseaux locaux et métropolitains — Partie 11: Spécifications du contrôle d'accès du milieu sans fil (MAC) et de la couche physique (PHY) , mai 2018.
- [39] « Introduction to HL7 Standards | HL7 International ». <http://www.hl7.org/implement/standards/index.cfm?ref=nav>
- [40] « The DICOM standard - Current Edition », janvier 2023. <https://www.dicomstandard.org/current>
- [41] « LOINC (Logical Observation Identifiers Names & Codes) ». <https://loinc.org/>
- [42] « SNOMED International (Systematized Nomenclature of Medicine - Clinical Terms) ». <https://www.snomed.org/?lang=fr>
- [43] « Integrating the Healthcare Enterprise (IHE) », *IHE International*. <https://www.ihe.net/>.
- [44] Healthcare Information and Management Systems Society Analytics, « Medical devices landscape : current and future adoption, integration with EMRs, and connectivity ». décembre 2010.
- [45] Institute of Medicine (US) Committee on Quality of Health Care in America, *To Err is Human: Building a Safer Health System*. Washington (DC): National Academies Press (US), 1999. [En ligne]. Disponible sur: www.doi.org/10.17226/9728

- [46] West Health Institute, « The value of medical device interoperability : Improving patient care with more than \$30 billion in annual health care savings ».
- [47] Haute Autorité de Santé, « abrEIGés, Un condensé du rapport annuel sur les évènements indésirables graves associés aux soins (EIGS) de 2021 ». novembre 2022. [En ligne]. Disponible sur: https://www.has-sante.fr/jcms/p_3388885/fr/evenements-indesirables-graves-associes-a-des-soins-eigs-bilan-annuel-2021
- [48] Committee on the Learning Health Care System in America et Institute of Medicine, *Best Care at Lower Cost: The Path to Continuously Learning Health Care in America*. Washington (DC): National Academies Press (US), 2013. [En ligne]. Disponible sur: www.doi.org/10.17226/13444
- [49] C. Cartau, *La sécurité du système d'information des établissements de santé*. Presses de l'École des hautes études en santé publique, 2018.
- [50] C. Godé, J.-F. Lebraty, et P. Barbaroux, « D'un système d'information résilient à un système d'information anti-fragile ? Illustrations à partir des organisations militaires : Les Cahiers Risques et Résilience. hal-04032465 ». mars 2023. [En ligne]. Disponible sur: <https://hal.science/hal-04032465>
- [51] Agence nationale de la performance sanitaire et médico-sociale (ANAP), « Concentrateur de données », *Data Management*, mars 2023. <https://ia.anap.fr/concentrateur-de-donnees/> (consulté le 22 juin 2023).
- [52] Agence nationale de la performance sanitaire et médico-sociale (ANAP), « Concentrateur de données - CH de Valenciennes ». mars 2023. [En ligne]. Disponible sur: https://ia.anap.fr/wp-content/uploads/2022/03/ANAP-_BC-concentrateur-de-donnres-CH-Valenciennes.pdf
- [53] C. Cartau, C. Millet, et Association pour la Sécurité des Systèmes d'Information de Santé (APSSIS), « Guide Cyber résilience opus 5 - Contrôles, indicateurs & tableaux de bord - Opus 5 guide Cyber résilience Par Cédric CARTAU opus 5 Contrôles, indicateurs & tableaux de bord ». mai 2022. [En ligne]. Disponible sur: <https://www.apssis.com/upld/2022/05-mai/Guide-cyberresilience-opus5.pdf>
- [54] Commission européenne, « Groupes de travail du groupe de coordination en matière de dispositifs médicaux », mai 2023. https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties/medical-device-coordination-group-working-groups_fr
- [55] Medical Device Coordination Group (MDCG), « MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices ». juillet 2020. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

[56] « National Electrical Manufacturers Association (NEMA) ». <https://www.nema.org/>

[57] National Electrical Manufacturers Association, « Manufacturer Disclosure Statement for Medical Device Security », *NEMA*, octobre 2019. <https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security>

[58] Norme ISO/IEC 7498-1:1994 Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Modèle de référence de base: Le modèle de base . juin 1996.

[59] Ministère de la Santé et de la Prévention, « Identitovigilance », *Ministère de la Santé et de la Prévention*, janvier 2023. <https://sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance>

[60] Article R1112-7 - Code de la santé publique , mars 2018.
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036658351