Logiciels d'aide à la décision clinique dans le diagnostic in vitro : développement et cybersécurité

Mathilde Vouillot

▶ **To cite this version:**

Mathilde Vouillot. Logiciels d'aide à la décision clinique dans le diagnostic in vitro : développement et cybersécurité. Sciences pharmaceutiques. 2022. dumas-03624765

HAL Id: dumas-03624765

https://dumas.ccsd.cnrs.fr/dumas-03624765

Submitted on 30 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Faculté de Pharmacie
Aix*Marseille Université

THESE

PRESENTEE ET PUBLIQUEMENT SOUTENUE
DEVANT LA FACULTE DE PHARMACIE DE MARSEILLE

Le 4 Mars 2022

PAR

Mme Mathilde VOUILLOT

Née le 17/09/1996 à Marseille

EN VUE D'OBTENIR

LE DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

TITRE :

Logiciels d'aide à la décision clinique dans le diagnostic *in vitro* : Développement et Cybersécurité

JURY :

Président : Pr. Pascal RATHELOT

Membres : Pr. Romaric LACROIX (Directeur de thèse)

Dr. Pierre LEMERCIER

Liste des enseignants

ADMINISTRATION	
Doyen	Mme Françoise DIGNAT-GEORGE
Vice-Doyens	M. Jean-Paul BORG, M. François DEVRED, M. Pascal RATHELOT
Chargés de Mission	Mme Pascale BARBIER, Mme Alexandrine BERTAUD, M. David BERGE-LEFRANC, Mme Manon CARRE, Mme Caroline DUCROS, M. Philippe GARRIGUE, M. Guillaume HACHE, M. Thierry TERME
Conseiller du Doyen	M. Patrice VANELLE
Doyens honoraires	M. Patrice VANELLE, M. Pierre TIMON-DAVID
Professeurs émérites	M. José SAMPOL, M. Athanassios ILIADIS, M. Philippe CHARPIOT, M. Riad ELIAS
Professeurs honoraires	M. Guy BALANSARD, M. Yves BARRA, Mme Claudette BRIAND, M. Jacques CATALIN, Mme Andrée CREMIEUX, M. Gérard DUMENIL, M. Alain DURAND, Mme Danielle GARÇON, M. Maurice JALFRE, M. Joseph JOACHIM, M. Maurice LANZA, M. Patrick REGLI, M. Jean-Claude SARI
Chef des Services Administratifs	Mme Chloé SIMON
Chef de Cabinet	Mme Aurélie BELENGUER
Responsable de la Scolarité	Mme Nathalie BESNARD

DEPARTEMENT BIO-INGENIERIE PHARMACEUTIQUE
Responsable : Professeur Philippe PICCERELLE

PROFESSEURS	
BIOPHYSIQUE	M. Vincent PEYROT M. Hervé KOVACIC M. François DEVRED
GENIE GENETIQUE ET BIOINGENIERIE	M. Christophe DUBOIS
PHARMACIE GALENIQUE, PHARMACOTECHNIE INDUSTRIELLE, BIOPHARMACIE ET COSMETOLOGIE	M. Philippe PICCERELLE
MAITRES DE CONFERENCES	
BIOPHYSIQUE	Mme Odile RIMET-GASPARINI Mme Pascale BARBIER Mme Manon CARRE M. Gilles BREUZARD

	Mme Alessandra PAGANO
GENIE GENETIQUE ET BIOTECHNOLOGIE	M. Eric SEREE-PACHA Mme Véronique REY-BOURGAREL
PHARMACIE GALENIQUE, PHARMACOTECHNIE INDUSTRIELLE, BIOPHARMACIE ET COSMETOLOGIE	M. Pierre REBOUILLON M. Emmanuel CAUTURE Mme Véronique ANDRIEU Mme Marie-Pierre SAVELLI
BIO-INGENIERIE PHARMACEUTIQUE ET BIOTHERAPIES PHARMACO ECONOMIE, E-SANTE	M. Jérémy MAGALON Mme Carole SIANI Mme Muriel MASI
ENSEIGNANTS CDI	
ANGLAIS	Mme Angélique GOODWIN
A.H.U.	
PHARMACOTECHNIE	Mme Mélanie VELIER

DEPARTEMENT BIOLOGIE PHARMACEUTIQUE
Responsable : Professeur Françoise DIGNAT-GEORGE

PROFESSEURS	
BIOLOGIE CELLULAIRE	M. Jean-Paul BORG
HEMATOLOGIE ET IMMUNOLOGIE	Mme Françoise DIGNAT-GEORGE Mme Laurence CAMOIN-JAU Mme Florence SABATIER-MALATERRE Mme Nathalie BARDIN M. Romaric LACROIX
MICROBIOLOGIE	M. Jean-Marc ROLAIN M. Philippe COLSON
PARASITOLOGIE ET MYCOLOGIE MEDICALE, HYGIENE ET ZOOLOGIE	Mme Nadine AZAS-KREDER
MAITRES DE CONFERENCES	
BIOCHIMIE FONDAMENTALE, MOLECULAIRE ET CLINIQUE	M. Edouard LAMY Mme Alexandrine BERTAUD Mme Claire CERINI Mme Edwige TELLIER M. Stéphane POITEVIN Mme Sandra GHAYAD
HEMATOLOGIE ET IMMUNOLOGIE	Mme Aurélie LEROYER Mme Sylvie COINTE
MICROBIOLOGIE	Mme Anne DAVIN-REGLI Mme Véronique ROUX M. Fadi BITTAR Mme Isabelle PAGNIER Mme Sophie EDOUARD M. Seydina Mouhamadou DIENE

PARASITOLOGIE ET MYCOLOGIE MEDICALE, HYGIENE ET ZOOLOGIE	Mme Carole DI GIORGIO M. Aurélien DUMETRE Mme Magali CASANOVA Mme Anita COHEN
BIOLOGIE CELLULAIRE BIOLOGIE CELLULAIRE ET MOLECULAIRE	Mme Anne-Catherine LOUHMEAU Mme Alexandra WALTON
A.H.U.	
HEMATOLOGIE ET IMMUNOLOGIE	Mme Amandine BONIFAY
MAITRES DE CONFERENCE ASSOCIES A TEMPS PARTIEL (M.A.S.T.)	
PRATIQUE OFFICINALE	Mme Emmanuelle TONNEAU-PFUG

DEPARTEMENT CHIMIE PHARMACEUTIQUE
Responsable : Professeur Patrice VANELLE

PROFESSEURS	
CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION	Mme Catherine BADENS
CHIMIE PHYSIQUE – PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	M. David BERGE - LEFRANC
CHIMIE MINERALE ET STRUCTURALE – CHIMIE THERAPEUTIQUE	M. Pascal RATHELOT M. Maxime CROZET
CHIMIE ORGANIQUE PHARMACEUTIQUE	M. Patrice VANELLE M. Thierry TERME
MAITRES DE CONFERENCES	
BOTANIQUE ET CRYPTOGAMIE, BIOLOGIE CELLULAIRE	Mme Anne FAVEL M. Quentin ALBERT
CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION	Mme Catherine DEFOORT M. Alain NICOLAY Mme Estelle WOLFF Mme Elise LOMBARD Mme Camille DESGROUAS M. Charles DESMARCHELIER M. Mathieu CERINO
CHIMIE PHYSIQUE – PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	M. Duje BURIC M. Pascal PRINDERRE
CHIMIE THERAPEUTIQUE – CHIMIE MINERALE ET STRUCTURALE	Mme Sandrine ALIBERT Mme Caroline DUCROS M. Marc MONTANA Mme Manon ROCHE Mme Fanny MATHIAS
CHIMIE ORGANIQUE PHARMACEUTIQUE HYDROLOGIE	M. Arnaud GELLIS M. Christophe CURTI

	Mme Julie BROGGI M. Nicolas PRIMAS M. Cédric SPITZ M. Sébastien REDON
PHARMACOGNOSIE, ETHNOPHARMACOGNOSIE	Mme Valérie MAHIOU-LEDDET Mme Sok Siya BUN Mme Béatrice BAGHDIKIAN M. Elnur GARAYEV
MAITRES DE CONFERENCE ASSOCIES A TEMPS PARTIEL (M.A.S.T.)	
CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION CHIMIE PHYSIQUE – PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	M. Cyril PUJOL
DROIT ET ETHIQUE	Mme Laurie PAHUS
GESTION PHARMACEUTIQUE, PHARMACOECONOMIE ET ETHIQUE PHARMACEUTIQUE OFFICINALE, DROIT ET COMMUNICATION PHARMACEUTIQUES A L'OFFICINE ET GESTION DE LA PHARMAFAC	Mme Félicia FERRERA
DISPOSITIFS MEDICAUX	Mme Valérie MINETTI-GUIDONI

DEPARTEMENT MEDICAMENT ET SECURITE SANITAIRE
Responsable : Professeur Benjamin GUILLET

PROFESSEURS	
PHARMACIE CLINIQUE	M. Stéphane HONORE
PHARMACODYNAMIE	M. Benjamin GUILLET
TOXICOLOGIE ET PHARMACOCINETIQUE	M. Bruno LACARELLE M. Joseph CICCOLINI
TOXICOLOGIE GENERALE	Mme Caroline SOLAS-CHESNEAU
MAITRES DE CONFERENCES	
PHARMACIE CLINIQUE	M. Florian CORREARD Mme Marie-Anne ESTEVE
PHARMACODYNAMIE	M. Guillaume HACHE Mme Ahlem BOUHLEL M. Philippe GARRIGUE
PHYSIOLOGIE	Mme Sylviane LORTET
TOXICOLOGIE ET PHARMACOCINETIQUE	Mme Raphaëlle FANCIULLINO Mme Florence GATTACECCA Mme Anne RODALLEC M. Nicolas FABRESSE
TOXICOLOGIE GENERALE	M. Pierre-Henri VILLARD

A.H.U.	
PHYSIOLOGIE / PHARMACOLOGIE	Mme Anaïs MOYON M. Vincent NAIL

CHARGES D'ENSEIGNEMENT A LA FACULTE

Mme Valérie AMIRAT-COMBRALIER, Pharmacien-Praticien hospitalier
M. Pierre BERTAULT-PERES, Pharmacien-Praticien hospitalier
Mme Marie-Hélène BERTOCCHIO, Pharmacien-Praticien hospitalier
Mme Martine BUES-CHARBIT, Pharmacien-Praticien hospitalier
M. Nicolas COSTE, Pharmacien-Praticien hospitalier
Mme Sophie GENSOLLEN, Pharmacien-Praticien hospitalier
M. Sylvain GONNET, Pharmacien titulaire
Mme Florence LEANDRO, Pharmacien adjoint
M. Stéphane PICHON, Pharmacien titulaire
M. Patrick REGGIO, Pharmacien conseil, DRSM de l'Assurance Maladie
Mme Clémence TABELE, Pharmacien-Praticien attaché
M. Badr Eddine TEHHANI, Pharmacien – Praticien hospitalier
M. Joël VELLOZI, Expert-Comptable

Mise à jour le 13 décembre 2021

Remerciements

Au **Professeur Pascal RATHELOT**,

Je vous remercie de l'honneur que vous me faites en ayant accepté d'être président de ma thèse ; merci pour votre supervision pendant mon externat au sein du Service Central de la Qualité et de l'Information Pharmaceutiques (SCQIP) de l'AP-HM. Pour votre disponibilité, vos connaissances ainsi que votre pédagogie, je tenais à vous exprimer toute ma gratitude. Soyez assuré de ma profonde reconnaissance.

Au **Professeur Romaric LACROIX**,

Je vous remercie de l'honneur que vous me faites en ayant accepté d'être directeur de ma thèse. Pour votre temps, votre esprit critique et votre partage de connaissances, je vous adresse mes remerciements les plus sincères. Je vous remercie aussi pour vos précieux conseils, votre disponibilité ainsi que pour vos relectures tout au long de l'écriture de cette thèse.

À **Monsieur Pierre LEMERCIER**,

Je vous remercie d'avoir accepté de faire partie de mon jury de thèse, mais surtout un grand merci pour m'avoir embauché au cours de mes années d'études et pour m'avoir transmis vos connaissances. Je n'oublierai jamais la première pharmacie où j'ai débuté et tous ces bons moments passés ensemble avec l'équipe. Je suis très heureuse que vous aillez accepté de faire partie de mon jury.

*À **ma famille**,*

Et plus particulièrement mes parents et ma sœur : Papa et Anne, merci de m'avoir toujours soutenue durant ces six années d'études, parfois accompagnées de doutes, mais surtout de joie. Vous êtes un pilier dans ma vie, et sans vous, je ne serai pas devenue la femme et pharmacienne épanouie que je suis à présent. Merci de m'avoir encouragée sans cesse sur cette voie, qui aboutit aujourd'hui. Pour avoir toujours cru en mon potentiel, pour votre soutien en période d'examen et dans toutes les étapes importantes de ma vie et pour tout votre amour au quotidien, merci. Après une épreuve plus que difficile, nous avons su resté fort et soudé, le meilleur reste à venir avec notre petite merveille née il y a peu, Albane, je vous aime fort.

À **Julien**,

Je ne te remercierai jamais assez pour tout ce que tu m'apportes au quotidien. Merci d'être le meilleur homme possible chaque jour à mes côtés. Sans toi rien de tout ça n'aurait été possible, tu as été d'un soutien indéfectible pendant la période la plus difficile de ma vie. Depuis toutes ces années tu as cru en moi et c'est ce qui m'a permis d'accomplir toutes ces choses ! Nous avons vécu tant de

chose ensemble… tellement de beaux voyages aussi, et de très beaux à venir… Tu as été mon binôme de TP à la fac : cela n'aura pas toujours été facile, mais on y est arrivés ! Merci de nous avoir porté jusqu'à Tahiti pour notre stage de cinquième année, sans toi je n'aurai jamais osé partir loin de tout le monde et tu as su en faire la plus belle expérience de ma vie. Et enfin merci pour m'avoir apporté une deuxième famille. Je ne te le dirai jamais assez : merci pour tout, je t'aime.

*À **ma belle-famille**,*
Merci de m'avoir accueillie dans votre famille avec toute la gentillesse et la bienveillance possible. Mille mercis pour tout ce que vous faites pour nous au quotidien et pour votre soutien sans faille.

À **ma meilleure amie**,
Merci à toi, Fanny, d'être mon rayon de soleil au quotidien. Tu m'apportes tellement de bonheur, merci pour tous ces rires et toutes ces joies, que tu m'apportes chaque jour. Toujours ensemble aussi bien dans les études que dans la vie et je sais que l'avenir nous réserve de belles surprises… Merci pour ce lien mère-fille que Cath et toi continuaient à me faire vivre chaque jour, je vous aime.

À **tonton** et **tata Scotto**,
Je tenais à vous remercier pour tout ce que vous avez fait pour Anne et moi depuis toutes ces années. Je ne vous dirai jamais assez combien je tiens à vous et combien vous êtes importants à mes yeux. Merci d'avoir fait ce que je suis à présent, en m'élevant et en me supportant chaque jour.

À **mes amis et proches,**
À mes amis de longues dates, Marion, Cécile, Céline, Andréa, Louis, Édouard, Tristan, Alice et j'en passe, il s'en sera passé des choses depuis le temps… Plus de 20 ans après pour certains, toujours les mêmes, ne changez pas. C'est un pur bonheur d'avoir des amis exceptionnels comme vous.

À mes amis de la faculté, Grégoire, Tristan, Steven, Émeline, Léa… avec vous j'ai certes partagé les bancs de la fac et les paillasses de TP mais bien plus encore. Merci pour votre bonne humeur quotidienne et tous ces bons moments à vos côtés : la suite reste à écrire…

À mes amis de Tahiti, Steven, Carla, Adrien et Romain : Merci pour cette belle amitié qui s'est créée lors de notre stage à l'autre bout du monde. Certains étaient en stage de fin d'études, d'autres en stage de cinquième année mais quelle expérience ! Entre travail, colocation, confinement, voyages, pleurs et rires, nous avons vécu des choses inoubliables qui m'accompagneront tout au long de ma vie.

À **l'équipe de la Pharmacie de la Tour**,

Je n'oublie aucun de ces moments passés à vos côtés. Merci pour tout ce que vous m'avez appris professionnellement et mille fois merci pour les joies et les rires que vous m'avez quotidiennement apportés.

À **l'équipe du Laboratoire de Cosmétologie du Pacifique Sud** et à son **directeur Monsieur Olivier TOUBOUL**,

Je n'oublierai jamais mon stage tahitien, ni vous tous qui avaient permis que ce stage soit un véritable bonheur. Merci à toute l'équipe pour son accueil chaleureux et pour mon intégration, et plus particulièrement à Kelly, vous avez su mettre à l'honneur la convivialité polynésienne dans laquelle j'ai été plongée pendant toute la durée de mon stage.

Une pensée pour Maman, qui me manque chaque jour et qui, j'en suis sûre, veille sur nous, **et pour mon grand-père.**

Cette thèse vous est dédiée.

« L'Université n'entend donner aucune approbation, ni improbation aux opinions émises dans les thèses. Ces opinions doivent être considérées comme propres à leurs acteurs. »

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

AAMI	Association for the Advancement of Medical Instrumentation
ANSM	Agence Nationale de Sécurité du médicament et des produits de santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CBOM/SBOM	Software/Cybersecurity Bills of Materials
CEI	Commission électrotechnique internationale
CNEDiMTS	Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé
DM	Dispositifs médicaux
DMDIV	Dispositifs médicaux de diagnotic *in vitro*
DT	Documentation Technique
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité d'Information
EEE	Espace économique européen
EM	Méningite-Encéphalite
FDA	Food and Drug Administration
FISMA	Federal Information Security Management Act
GCDM	Groupe de Coordination en matière de Dispositifs Médicaux
HAS	Haute Autorité de Santé
HbA1c	Hémoglobine glyquée
IMDRF	International Medical Device Regulators Forum
INR	International Normalized Ratio
ISAO	Information Sharing and Analysis Organization
ISO	Organisation internationale de normalisation

IVDR	Règlement Européen 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (DMDIV)
IVD MDSW	In Vitro Diagnostic Medical Device Software
JOUE	Journal Officiel de l'Union Européenne
Marquage CE	Marquage Conformité Européenne
MAUDE	Manufacturer and User Facility Device Experience
MDCG	Medical Device Coordination Group
MDSW	Medical Device Software
MDR	Règlement Européen 2017/745 relatif aux dispositifs médicaux (DM)
NHS	National Health Service
NIST	National Institut of Standard and Technology
Normes EN	Normes Européennes
Normes NF	Normes Françaises
ON	Organisme Notifié
PMPF	Post-market performance follow-up
POCT	Point of Care Testing
QbD	Quality by Design
RGDP	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
SADM	Système d'aide à la décision médicale
SAFECode	Software Assurance Forum for Excellence in Code
SaMD	Software as a Medical Device
SAST	Static Application Security Testing
SbD	Security by Design
SDLC	Software Development Lifecycle

SIH	Systèmes d'information hospitalier
SIS	Système d'information de santé
SMQ	Système de Management de la Qualité
SSI	Sécurisation des systèmes d'information
STC	Spécifications Techniques Communes
TI	Technologies de l'information
TICS	Technologies de l'information et de la communication en santé
TIR	Rapport d'information technique
UDI	Unique Device Identification
UE	Union Européenne
UL	Underwriters Laboratories
VPN	Virtual Private Network

Introduction

La santé numérique, couramment appelé « e-santé », est aujourd'hui un secteur en plein essor, pourvoyeur d'innovations majeures. Selon la Commission Européenne, le terme e-santé fait référence à « l'application des technologies de l'information et de la communication (TIC) à l'ensemble des activités en rapport avec la santé ». Ainsi, elle modifie les usages des acteurs du système de santé dans son ensemble et ces outils, ou solutions numériques, présentent un fort potentiel de levier d'amélioration du système de soins. (1)

Ce secteur connaît une nette évolution en termes d'usage et de filière économique en France. Son marché est promis à un fort potentiel de croissance. En effet, une étude de l'Institut Montaigne estime que le déploiement de la e-santé pourrait générer en France jusqu'à environ 22 milliards d'euros par an. Au niveau mondial la valeur du marché de la santé numérique d'ici 2023 se situerait à 234,5 milliards de dollars. (1)

Il y a encore quelques années, la e-santé était considéré comme un secteur de technophiles avertis et précurseurs. La crise sanitaire a très largement accéléré l'adoption des services numériques en santé désormais entrés dans la plupart des foyers, comme en témoigne l'explosion des téléconsultations des médecins généralistes, passées de 0,1% avant le 1er confinement à 25% dès avril 2020. (2)

La santé numérique apparait donc naturellement comme une solution pertinente pour répondre aux défis que doit relever le système de santé : évolution de la démographie médicale, inégalités territoriales d'accès aux soins, amélioration de la démocratie sanitaire, hausse de la prévalence des maladies chroniques ou encore vieillissement de la population. Elle accélère ainsi la bascule vers une médecine dite des « 5P » : personnalisée, préventive, prédictive, participative et pertinente.

Cette transformation dans la santé par le numérique, amplifiée par la crise sanitaire, contribue donc à améliorer la qualité de vie de ses utilisateurs, la coordination des soins et des parcours (en allégeant notamment la charge d'activité des structures et professionnels) et participe à limiter les inégalités d'accès aux soins. (1)

On constate une grande diversité des solutions numériques existantes et à venir, soutenue par leurs vastes champs d'application. Cette extraordinaire et riche hétérogénéité peut venir tant de leur nature technologique que de leurs usages au sein du système de santé.
En effet, une solution numérique en santé est définie comme tout système incluant une dimension numérique et utilisé au sein d'un écosystème de santé. Cette définition large permet d'inclure notamment les objets connectés, les applications mobiles, les logiciels types *serious game,* les thérapies numériques (= *digital therapeutics*) ou encore les systèmes d'information de santé type systèmes d'information hospitalier (SIH). Toujours dans le cadre de ces réflexions, les solutions numériques citées peuvent répondre, ou non, à la définition du dispositif médical au sens du règlement européen 2017/745 relatif aux dispositifs médicaux (DM) ou encore à la définition d'un dispositif médical de diagnostic *in vitro* (DMDIV) au sens du règlement européen 2017/746. (1)

Parmi cette pluralité de solutions numériques, les logiciels dans le domaine de la santé connaissent actuellement un essor important, qu'il s'agisse de leur nombre ou de leur diversité, notamment au regard des innovations technologiques. La finalité médicale des données ainsi obtenues représente un enjeu réglementaire majeur. Si ces données sont recueillies dans un but de diagnostic, de prévention ou de contrôle d'une pathologie, par exemple, alors le logiciel correspondant peut être qualifiée de dispositif médical au sens large. Correctement définir la finalité d'un logiciel représente donc un enjeu majeur pour le fabricant. Si son dispositif entre dans le champ d'application des règlements européens des DM ou des DMDIV, alors son produit devra faire l'objet de procédures qui impacteront sa mise sur le marché, nécessitant alors le marquage CE afin de garantir sa conformité aux exigences applicables en Europe et son évaluation selon les procédures prévues. Les règlements DM[1] ont fait l'objet d'une révision complète, l'objectif étant de renforcer la sécurité sanitaire et d'harmoniser les évaluations au sein de l'Union européenne (UE). (3) Ils introduisent maintenant des exigences propres aux logiciels de DM en termes de sécurité et de performances. (4)

Ainsi, les logiciels (applications mobiles ou sur ordinateur, système embarqué et même intelligence artificielle) sont de plus en plus proposés comme solutions médicales (aide au

[1] Règlements DM :
- MDR : Règlement Européen 2017/745 relatif aux dispositifs médicaux (DM)
- IVDR : Règlement Européen 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (DMDIV)

diagnostic, télésurveillance, suivi, mesures…). Ils peuvent fonctionner seuls comme un DM à part entière, c'est le cas des applications mobiles de diagnostic, ou en association avec un DM, comme par exemple un logiciel exploitant les mesures d'un capteur. (4)
Dans ce travail, nous nous concentrerons sur les logiciels d'aide à la décision clinique et, plus particulièrement, sur ceux répondant à la définition des DMDIV. En général, il s'agit d'outils informatiques qui combinent des bases de données d'informations médicales générales et des algorithmes avec des données spécifiques au patient. Ils sont destinés à fournir aux professionnels de santé et/ou aux utilisateurs, des recommandations pour le diagnostic, le pronostic, le suivi et le traitement des patients de façon individuelle. (5)

Cependant, ces évolutions technologiques ont rapidement été intégrées dans la pratique médicale quotidienne sans que les risques associés soient parfaitement maîtrisés. En effet, si les fabricants sont capables de garantir des produits sûrs en termes d'innocuité biologique et d'efficacité clinique, ils n'ont pas encore de culture spécifique dans le domaine de la sécurité informatique. (4)

La connectivité et la numérisation des technologies des logiciels de DMDIV, *aussi appelés In Vitro Diagnostic Medical Device Software (IVD MDSW) en anglais,* peuvent contribuer à améliorer ou à accroître la fonctionnalité des dispositifs et à apporter un bénéfice thérapeutique. Mais cette connexion des dispositifs à des réseaux ou à l'internet les exposent à des cybermenaces qui peuvent potentiellement conduire à un risque accru de préjudice pour les patients. Ces menaces peuvent inclure le refus d'un service ou d'un traitement prévu, ou encore l'altération de la fonction du logiciel de manière à ce qu'il puisse nuire au patient. Elles peuvent aussi inclure la perte de la confidentialité ou l'altération des données de santé personnelles.
Dans le secteur de la santé plus qu'ailleurs, la protection des biens et des données personnelles est une nécessité. En effet, l'exploitation de n'importe quelle vulnérabilité peut avoir des conséquences néfastes jusqu'à impacter directement la sécurité des soins et la santé des patients. (4) C'est particulièrement vrai dans le domaine des dispositifs médicaux, où la qualité des logiciels est étroitement liée à la sécurité, et où une défaillance logicielle peut causer des blessures voire la mort d'un patient.
Il devient donc essentiel que les fabricants de DM et DMDIV soient en capacité d'intégrer, dès la conception de leurs produits, des exigences de base permettant de garantir un niveau minimum de sécurité face à la malveillance informatique. (4)

Ainsi, la sécurité informatique face à des menaces est désignée sous le terme « cybersécurité ».
Contrairement à la mise sur le marché des DM et DMDIV, très bien encadrée d'un point de vue réglementaire, la culture de la cybersécurité est, quant à elle, très hétérogène au sein des fabricants de dispositifs médicaux. Cela s'explique notamment par une absence d'analyse de risque spécifique, une méconnaissance des exigences de cybersécurité ou encore un défaut de prise en compte de la cybersécurité dans le processus de conception et de développement du DM. (6)
De plus, il n'existe que depuis peu des textes réglementaires ou recommandations dédiés spécifiquement à la cybersécurité informatique.

Ainsi, dans cette thèse, nous étudierons l'impact de la cybersécurité sur le développement des logiciels d'aide à la décision clinique de diagnostic *in vitro*.
Pour se faire, la première partie de cette thèse présentera leur réglementation et leur mise en conformité en Europe. Puis, dans un second temps, nous aborderons la cybersécurité des logiciels de DMDIV à proprement parler. Enfin, une discussion sera proposée en exposant les perspectives de cette problématique.

PARTIE I : LES LOGICIELS DE DMDIV EN EUROPE

Les systèmes d'aide à la décision médicale (SADM) sont « des applications informatiques dont le but est de fournir aux cliniciens en temps et lieux les informations décrivant la situation clinique d'un patient ainsi que les connaissances appropriées à cette situation, correctement filtrées et présentées afin d'améliorer la qualité des soins et la santé des patients. » (7) Le potentiel des technologies de l'information et de la communication en santé (TICS) et des SADM en termes d'amélioration de la qualité, de la sécurité et de l'efficience des soins n'est aujourd'hui plus à démontrer. (8) Parmi les TICS, les logiciels d'aide à la décision médicale sont de plus en plus proposés comme solutions médicales. Ils peuvent relever, ou non, du statut de dispositifs médicaux au sens large. Seuls les logiciels ayant une finalité médicale sont considérés comme DM ou DMDIV, mais leur qualification demande une évaluation au cas par cas par le fabricant en fonction de la destination et des spécificités de chacun. En effet, tout produit entrant dans le champ de la réglementation européenne des DM ou des DMDIV doit s'y conformer pour pouvoir être marqué CE et bénéficier de la libre circulation au sein de l'UE. (9)

Dans cette partie, après avoir présenté différents logiciels représentatifs d'aide à la décision clinique de DMDIV, nous apporterons un éclairage réglementaire sur la qualification de ce type de produit en tant que DMDIV et sur les modalités de leur mise en conformité au regard de la réglementation applicable, à l'aide de différents exemples caractéristiques.

1.1. Exemples de logiciels d'aide à la décision clinique de DMDIV

D'après un des guides[2] élaboré par le groupe d'experts[3], responsable de la coordination des DM et institué par le Règlement (UE) 2017/746 relatif aux DMDIV, le GCDM en français, ces logiciels sont en général des outils informatiques qui combinent des bases de données d'informations médicales générales et des algorithmes utilisant des données spécifiques au patient. Ils sont destinés à fournir aux professionnels de santé et/ou aux utilisateurs, des

[2] Guide *MDCG 2019-11 : Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.*

[3] Le GCDM, aussi appelé MDCG en anglais, est un groupe d'experts représentant les autorités compétentes des États membres de l'UE. Le GCDM conseille et assiste la Commission Européenne et les pays de l'UE dans la mise en œuvre de l'IVDR.

recommandations pour le diagnostic, le pronostic, le traitement et le suivi des patients de façon individuelle.

Les logiciels d'aide à la décision clinique qui sont qualifiés de DMDIV peuvent être :

- Des dispositifs utilisés pour diagnostiquer ou évaluer le niveau de gravité d'une pathologie.

  Par exemple, un **logiciel permettant d'évaluer le niveau de fibrose hépatique**, comme par exemple le FibroMeter® VCTE de Echosens. Ce logiciel est une combinaison unique du test sanguin FibroMeter® et du résultat FibroScan® pour une évaluation optimale de la fibrose hépatique. En effet, grâce au dosage sérique des marqueurs hépatiques du patient et après report des résultats et analyse par le logiciel, ce dernier calculera et affichera des scores d'estimation de fibrose hépatique afin d'estimer le stade de la fibrose.

- Des dispositifs de surveillance qui sont utilisés pour mesurer les niveaux d'un analyte dans le but d'ajuster les traitements/interventions si nécessaire. Ces dispositifs peuvent être :
  - Utilisés pour évaluer si un analyte reste à des niveaux physiologiques ou dans une fourchette thérapeutique médicamenteuse établie. Ces types de dispositifs sont conçus pour évaluer l'état actuel d'un individu,
  - Utilisés pour des mesures en série, c'est-à-dire que plusieurs déterminations sont effectuées au fil du temps. Ces types d'appareils sont généralement utilisés pour la détection/évaluation de la progression/régression de la maladie, de la récurrence de la maladie, de la maladie résiduelle minimale, de la réponse/résistance au traitement, et/ou des effets indésirables dus à la thérapie. Ces types de dispositifs sont conçus pour évaluer les changements d'état d'un individu.

  On peut citer les **systèmes de planification des médicaments destinés à calculer la dose de médicament à administrer à un patient spécifique** : un logiciel de calcul de dose dans le cadre d'un traitement prescrit par un médecin intègre généralement des paramètres physiologiques du patient (poids, âge, clairance de la créatinine, etc).

L’exploitation de données des patients (paramètres physiologiques, symptômes), par le biais d’algorithmes spécifiques, permet de générer une information nouvelle, en vue de traiter le patient.

Par exemple, un **logiciel qui permet de calculer la dose d'insuline à s'injecter en fonction des données de la glycémie** du patient à différents moments de la journée (avant ou après les repas) selon les paramètres du protocole prescrit par le médecin. C’est le cas du lecteur FreeStyle® InsuLinx® avec calculateur d’insuline à action rapide intégré. Cette fonctionnalité aide le patient à calculer la dose d’insuline à action rapide en fonction de leur repas et de leur taux de glycémie. Ces calculs de doses font intervenir divers paramètres dont ceux établis par le médecin et les données issues de l'historique des données saisies de la glycémie du patient. Ce logiciel est destiné à aider le patient dans le calcul de la dose d'insuline rapide à s'administrer en fonction des données glycémiques à différents moments de la journée selon des paramètres fixés, au préalable, par le médecin. Ce type de logiciel est capable d'effectuer une analyse/exploitation des données existantes relatives au patient, en fonction des paramètres du protocole et de l'historique des glycémies, entre autre, et de générer une nouvelle information spécifique à un patient donné pour orienter son traitement thérapeutique, ce qui constitue une finalité médicale au sens des articles L.5211-1 et R.5211-1 du code de la santé publique.

- Des dispositifs de dépistage qui sont utilisés pour détecter la présence ou la prédisposition à une maladie, un trouble ou un autre état physiologique dans un échantillon provenant d'un individu, d'un embryon ou d'un fœtus ne présentant pas de signes cliniques évidents. En fonction de la nature de l’affection et de la population de patients visée, ces dispositifs peuvent être utilisés de manière systématique ou être limités aux patients « à risque ».

  Ici, nous pouvons citer l’exemple des **logiciels de calcul de risque de trisomie 21 fœtale**. Il en existe de différentes marques, de différents fabricants, comme par exemple le logiciel Fast Screen Pre I Plus de la société Thermo Fisher Scientific ou le logiciel SSDWLab6 de Roche, mais tous ont un principe de fonctionnement similaire. Un logiciel de DMDIV destiné à fournir des informations sur la prédisposition statistique au syndrome de Down (trisomie 21) fournit aux cliniciens un score de

facteur de risque pour la probabilité qu'un fœtus présente des mutations génétiques au cours du 1er trimestre de la grossesse. Pour se faire, le logiciel prend en compte 5 facteurs de risque :

- Le risque lié à l'âge de la mère,
- Le risque sérologique (concentrations des marqueurs sériques maternels du 1er trimestre de la grossesse : hCG et PAPP-A),
- Le risque lié à l'épaississement de la clarté nucale,
- Le risque intégré (risque sérologique combiné au risque lié à la clarté nucale),
- Le risque intégré après échographie morphologique.

Le score de risque indique si des tests diagnostiques supplémentaires sont nécessaires ou non pour confirmer la présence de mutations génétiques de la trisomie 21.

Pour être mis sur le marché européen, ces logiciels d'aide à la décision clinique de diagnostic *in vitro* doivent obtenir le marquage CE. Pour se faire, ils doivent répondre à la réglementation dont ils relèvent, à savoir celle des DMDIV.

1.2. La réglementation des logiciels de DMDIV

Jusqu'à présent, le cadre réglementaire des DMDIV était fourni par la directive 98/79/CE qui devait être transposée en législation nationale dans chaque état membre de l'UE. Ceci constituait une source d'interprétations différentes au sein même de l'UE. De plus, des incidents concernant la performance et la sécurité des produits ont mis en évidence certaines faiblesses dans ce système législatif.

Une révision de la législation a donc été nécessaire pour renforcer les normes en matière de qualité et de sécurité des DM. De plus, cette révision était nécessaire afin d'adapter la réglementation régissant les DMDIV, à l'évolution du secteur au cours des 20 dernières années, comprenant l'avancée technologique liée à l'émergence des objets connectés, des applications ou encore des logiciels en santé. La priorité était donc de garantir un cadre réglementaire solide, transparent et durable et de maintenir un niveau de sécurité élevé, tout en soutenant l'innovation.

Le nouveau Règlement (UE) 2017/746 sur les DMDIV, encore appelé IVDR, a été publié en mai 2017 et entrera en application le 26 mai 2022. Il remplacera progressivement la directive 98/79/CE existante après une période de transition afin de garantir :

- Un niveau constamment élevé de protection de la santé et de la sécurité pour les citoyens de l'UE utilisant ces produits ;
- Le commerce libre et équitable des produits dans l'ensemble de l'UE ;
- Une législation de l'UE adaptée aux importants progrès technologiques et scientifiques réalisés dans ce secteur depuis ces dernières années. (10)

Pour se faire, ce nouveau cadre réglementaire voit le niveau des exigences générales augmenter de manière significative et met en place une plus grande transparence et traçabilité du système.

L'IVDR fixe des exigences générales de sécurité et de performances auxquelles doivent se conformer les fabricants pour garantir la sécurité et la fiabilité de leurs dispositifs mis sur le marché européen. Afin d'apposer le marquage CE, le fabricant doit constituer une documentation technique (DT) présentant les preuves permettant de démontrer la qualité et la sécurité du dispositif. En fonction de la classe de risque du dispositif, un organisme notifié (ON) indépendant intervient dans le processus de marquage CE. Celui-ci évalue la conformité du dispositif et le système qualité du fabricant et délivre, en cas d'évaluation satisfaisante, un certificat de conformité, d'une durée maximale de 5 ans, permettant au fabricant d'apposer le marquage CE sur son dispositif et de mettre sur le marché le DMDIV dans l'ensemble des pays de l'UE. La pertinence de la DT et l'organisation du fabricant font l'objet d'évaluations périodiques par l'ON. Une fois mis sur le marché, le dispositif est sous la responsabilité du fabricant qui le commercialise. Celui-ci doit assurer une surveillance de ses performances et de sa sécurité, vérifier qu'aucun problème ne survient à l'utilisation pour, le cas échéant, prendre des mesures préventives ou correctives. Les autorités sanitaires dites « compétentes » sont, en Europe, responsables de la surveillance du marché et de la désignation des ON. (11)

1.2.1. Introduction des logiciels dans la définition des DMDIV

Un des changements majeurs de la nouvelle réglementation a été l'intégration des logiciels dans le champ des DMDIV. En effet, les logiciels spécifiquement destinés par le fabricant à une ou plusieurs des fins médicales visées dans la définition d'un DMDIV, doit répondre aux exigences du Règlement.

On désigne désormais comme « *dispositif médical de diagnostic in vitro*, tout dispositif médical qui consiste en un réactif, un produit réactif, un matériau d'étalonnage, un matériau de contrôle, une trousse, un instrument, un appareil, un équipement, un **logiciel** ou un système, utilisé seul ou en association, destiné par le fabricant à être utilisé in vitro dans l'examen d'échantillons provenant du corps humain, y compris les dons de sang et de tissus, uniquement ou principalement dans le but de fournir des informations sur un ou plusieurs des éléments suivants:

a) concernant un processus ou état physiologique ou pathologique;

b) concernant des déficiences congénitales physiques ou mentales;

c) concernant la prédisposition à une affection ou à une maladie;

d) permettant de déterminer si un traitement donné est sûr pour des receveurs potentiels et compatible avec eux;

e) permettant de prévoir la réponse ou les réactions à un traitement;

f) permettant de définir ou de contrôler des mesures thérapeutiques.

Les récipients pour échantillons sont également réputés être des dispositifs médicaux de diagnostic in vitro. » (12)

Afin de compléter cette définition et apporter des précisions sur cette catégorie de produit, le groupe de coordination en matière de dispositifs médicaux (GCDM) a défini différents termes utiles à notre réflexion dans son guide *MDCG 2019-11 : Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR. (5)*
D'après ce guide, un « logiciel » est défini comme un ensemble d'instructions qui traite des données d'entrée et crée des données de sortie.

Ainsi, toute donnée fournie au logiciel afin d'obtenir des données de sortie après calcul de ces données, peut être considérée comme une donnée d'entrée. Par exemple, on peut citer les données reçues du dispositif ou transmises par le dispositif et les données fournies par l'utilisation d'un dispositif humain de saisie de données tel qu'un clavier, un stylet, une souris ou un écran tactile. Nous pouvons donner comme exemple de donnée d'entrée d'un DM, la glycémie d'un patient renseignée dans un lecteur de glycémie.

Une donnée de sortie sera définie comme toute donnée produite par un logiciel. On peut citer par exemple les données d'affichage à l'écran (telles que la disposition avec le nombre, les caractères, l'image, les graphiques) ou encore les documents numériques formatés pour un usage général (fichier Word, PDF, image JPEG) ou formatés à des fins médicales (enregistrement ECG, dossier médical électronique). Par exemple, est considérée comme donnée de sortie la dose d'insuline calculée et suggérée par le logiciel intégré au glucomètre du patient (Figure 1).

Figure 1 : Exemple de dose d'insuline rapide suggérée par le logiciel dans le glucomètre FreeStyle® InsuLinx®

Par conséquent, la première étape pour un industriel va être d'évaluer si son logiciel est, ou non, un dispositif médical au sens large. En effet, les logiciels à usages généraux, même lorsqu'ils sont utilisés dans un environnement médical, ou les logiciels destinés à des fins ayant trait au bien-être, ne constituent pas des DM ou DMDIV. Par exemple, n'est pas qualifié de DM ou DMDIV un logiciel destiné à l'observance, permettant de s'assurer de la bonne prise du traitement par le patient. De plus, la modification de la représentation des données à des fins d'embellissement ou de compatibilité ne permet pas de qualifier d'emblée le logiciel de DM. Il en est de même pour les logiciels destinés à des fins non médicales, telles que la facturation ou la planification du personnel. Une tâche telle que l'envoi de courrier électronique, la messagerie Web ou vocale, l'analyse de données, le traitement de texte et la sauvegarde n'est pas considérée en soi comme ayant une finalité médicale. Ces logiciels ne relèvent donc pas du MDR ni de l'IVDR.

Pour résumer, n'est pas qualifié de DM ou DMDIV, un logiciel :

- Destiné à l'observance, permettant de s'assurer de la bonne prise du traitement par le patient ;
- Ayant pour seule destination la communication de données sans fonction d'alertes auprès d'un médecin ;
- Destiné à être utilisé pour la pratique d'entraînements sportifs ou physiques, ou dont les fonctionnalités sont à finalité esthétique, de confort ou d'amélioration sportive ;
- Dont le résultat aboutirait à un diagnostic générique, pour un groupe de patients à visée statistique par exemple, ou pour une étude épidémiologique ;
- Ayant pour seule destination la gestion administrative comme le stockage, l'archivage, telle une base de données ou bibliothèque numérique intégrant des données et informations, même si elles sont de nature médicale, sans les exploiter. (13)

Il est donc important de bien qualifier son logiciel afin de savoir à quelle réglementation il devra se conformer.

1.2.2. Qualification d'un logiciel de DM (MDSW)

Le statut d'un logiciel est défini par sa destination d'usage et l'exploitation de données entrantes. La destination, aussi appelée revendication, est fixée par le fabricant, aussi appelé éditeur, du logiciel. Elle est décrite dans la notice, l'étiquetage mais également dans le matériel promotionnel. (13)

Pour être qualifié de MDSW, le logiciel doit présenter les critères cumulatifs suivants :

- Être destiné à une utilisation à des fins médicales au sens de la définition du DM ou DMDIV. Il doit permettre, par exemple, un diagnostic, une aide au diagnostic, un traitement ou une aide au traitement.
- Donner un résultat propre au bénéfice d'un seul patient.
- Effectuer une action sur les données entrantes, telle qu'une analyse afin de fournir une information médicale nouvelle. Cette action doit être différente d'un stockage, une communication, ou une simple recherche telle une base de données ou une bibliothèque numérique intégrant des données dans un but exclusif d'archivage sans les exploiter. (13)

Afin d'être orientés dans cette qualification, les industriels peuvent s'appuyer sur le guide du MDCG 2019-11. Ce guide définit notamment les critères de qualification des logiciels entrant dans le champ d'applicabilité des nouvelles réglementations sur les DM[4]. L'objectif ici est de clarifier les logiciels qui sont en eux-mêmes soumis aux réglementations sur les DM.

Ce guide définit les 3 cas de figure possibles lors du développement d'un logiciel de santé : (5) (Tableau 1)

[4] Nouvelles réglementations sur les DM : Règlement (UE) 2017/745 (Regulation on medical devices - MDR) + Règlement (UE) 2017/746 (Regulation on in-vitro diagnostic medical devices - IVDR)

	Logiciel de DM (MSDW)	Logiciel pilotant ou influençant l'utilisation d'un DM, sans finalité médicale en soi	Accessoire de DM
Définitions	Logiciel destiné à être utilisé, seul ou en combinaison, dans un but spécifié dans la définition d'un « dispositif médical » dans le MDR ou l'IVDR. Ce logiciel peut être indépendant ou il peut piloter ou influencer l'utilisation d'un dispositif : - Un MDSW peut être indépendant, en ayant sa propre finalité médicale et en répondant ainsi à la définition d'un DM ou d'un DMDIV par lui-même (c'est-à-dire, seul). - Si le logiciel pilote ou influence un DM (matériel) et qu'il a également un objectif médical, il est qualifié de MDSW.	Logiciel qui est destiné à piloter ou à influencer l'utilisation d'un DM (matériel) et qui n'a pas de finalité médicale en soi, qui n'a pas ou n'accomplit pas d'objectif médical en soit, et ne crée pas d'information en soi pour une ou plusieurs des finalités médicales décrites dans la définition d'un DM ou d'un DMDIV. **Ce logiciel n'est donc pas considéré comme un DM ou un DMDIV en soi.** Ce logiciel peut, mais ne se limite pas à : ▪ Faire fonctionner, modifier l'état de, ou de contrôler le dispositif soit par l'intermédiaire d'une interface (matériel ou logiciel) ou par l'intermédiaire de l'opérateur de ce dispositif. ▪ Fournir une sorte liée au fonctionnement (matériel) de ce dispositif.	Tout article qui, **sans être lui-même un DMDIV**, est destiné par son fabricant à être utilisé avec un ou plusieurs DMDIV données pour permettre spécifiquement une utilisation de ce ou ces derniers conformes à sa ou leur destination ou pour aider spécifiquement et directement au fonctionnement médical du ou des DMDIV selon sa ou leur destination.
Remarques	Le MDSW peut être destiné à être utilisé par des professionnels de santé ou des personnes non spécialisées (par exemple, des patients ou d'autres utilisateurs). *Un logiciel peut être qualifié de MDSW indépendamment de son emplacement (par exemple, s'il fonctionne dans un cloud, sur un ordinateur, sur un téléphone mobile ou comme une fonctionnalité supplémentaire sur un DM matériel).*	Ces logiciels sont couverts par la réglementation sur les DM/DMDIV, soit en tant que partie/composant d'un dispositif, soit en tant qu'accessoire de celui-ci.	- Un accessoire logiciel peut conduire ou influencer l'utilisation d'un DMDIV. - Les fabricants doivent décrire dans la documentation technique les accessoires d'un DMDIV qui sont destinés à être utilisés en combinaison avec celui-ci. - Suivant cette définition, le logiciel en tant qu'accessoire n'est pas classé comme un logiciel de DM (MDSW) mais est destiné à être utilisé avec un DM ou un DMDIV particulier. En tant qu'accessoire, il doit être conforme à toutes les exigences pertinentes du MDR ou de l'IVDR et est donc couvert par la réglementation sur les DM/DMDIV en tant qu'accessoire de celui-ci.
Exemples	• MDSW indépendant : Un logiciel qui utilise des paramètres maternels tels que l'âge, la concentration de marqueurs sériques et des informations obtenues par l'échographie fœtale pour évaluer le risque de trisomie 21. • MDSW qui pilote ou influence un DM (matériel) : Un logiciel destiné à mesurer et à transmettre les niveaux de glucose dans le sang, à calculer la dose d'insuline nécessaire et à piloter une pompe à insuline pour administrer la dose calculée (système d'administration d'insuline en boucle fermée). • MDSW destiné à être utilisé par des professionnels de santé ou des personnes non spécialisées : Un logiciel qui fournit des recommandations de doses d'insuline à un patient, quelle que soit la méthode d'administration de la dose prescrite, que ce soit par une pompe à insuline, un stylo à insuline ou une seringue à insuline.	Un logiciel destiné à être utilisé pour faire fonctionner un analyseur de chimie clinique.	Un logiciel avec des contrôles électroniques intégrés pour les procédures de contrôle de qualité des DMDIV. Ces procédures de contrôle de qualité sont destinées à fournir aux utilisateurs l'assurance que le dispositif fonctionne conformément aux spécifications.

Tableau 1 : Les différents types possibles de logiciels en santé

Il faut souligner que le risque de préjudice pour les patients, les utilisateurs du logiciel, ou toute autre personne, lié à l'utilisation du logiciel dans le cadre des soins de santé, y compris un éventuel dysfonctionnement, n'est pas un critère de qualification du logiciel en tant que DM.

Pour une meilleure compréhension, ce guide contient un logigramme décisionnel (Figure 2) permettant d'aider les fabricants à définir si leur logiciel est un dispositif médical, au sens large, ou non.

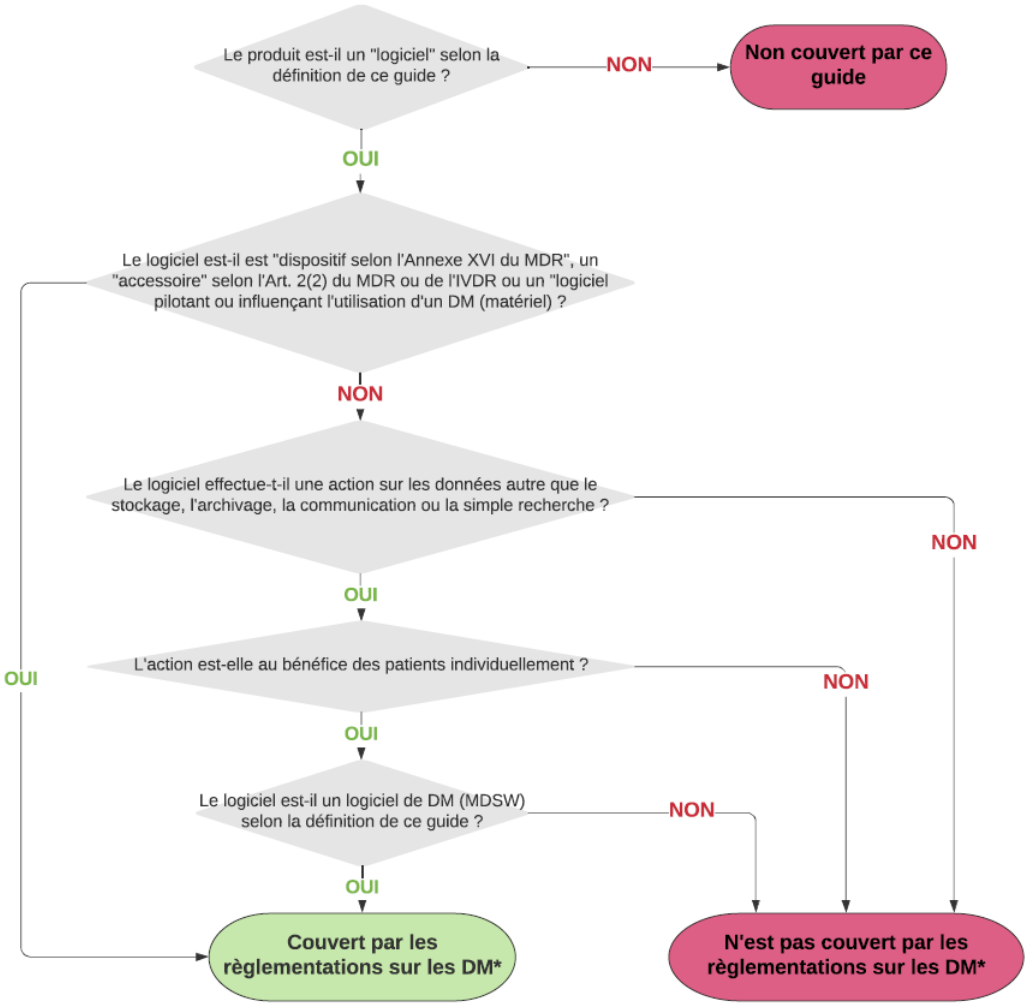

Figure 2 : Logigramme décisionnel pour la qualification d'un logiciel en tant que MDSW

*****_Règlementations sur les DM fait référence aux 2 règlements applicables :_

- Règlement (UE) 2017/745 sur les dispositifs médicaux (MDR)

- ET Règlement (UE) 2017/746 sur les dispositifs médicaux de diagnostic in vitro (DMDIV)

Cependant, certains logiciels peuvent être séparés en un certain nombre d'applications ; chacune de ces applications étant liées à un module. Certains de ces modules ont un but

médical, d'autres non. Cela soulève alors la question de savoir si l'ensemble du produit peut être marqué CE lorsque toutes les applications n'ont pas un objectif médical.
Ces modules peuvent être destinés à couvrir de nombreux besoins, par exemple :

- Collecter et maintenir les données administratives du patient,
- Conserver dans le dossier l'historique médical du patient,
- Facturation et autres fonctions comptables,
- Fournir un lien avec le système de sécurité sociale pour le remboursement,
- Fournir un lien avec les systèmes de prescription de médicaments (avec un lien possible avec les points de distribution de médicaments),
- Fournir un système expert d'assistance à la prise de décision médicale (par exemple, planificateur de dose de radiothérapie).

Dans ce cas, seuls les modules concernant les fonctionnalités à finalité médicale ont le statut de DM et devront alors être conformes aux exigences réglementaires des DM et devront porter le marquage CE.

Une fois le logiciel qualifié de dispositif médical au sens large (MDSW), il sera important de déterminer si celui-ci est un DM ou un DMDIV et donc de savoir s'il répond au MDR ou à l'IVDR.

1.2.3. Qualification d'un logiciel de DMDIV (IVD MDSW)

Les MDSW répondant à la définition d'un DMDIV relèvent de fait du Règlement (UE) 2017/746 relatif aux DMDIV.

Un logigramme décisionnel a aussi été élaboré par le MDCG dans son guide 2019-11 afin d'aider les fabricants à identifier si leur logiciel est un DMDIV ou non (Figure 3).

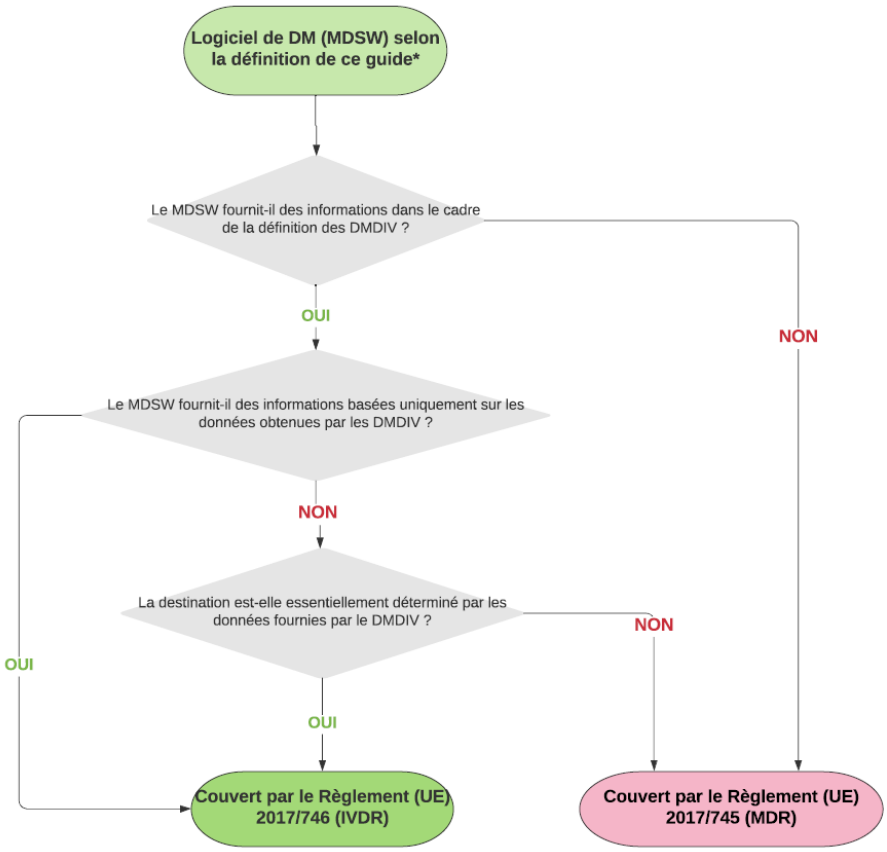

Figure 3 : Logigramme décisionnel pour aider à la qualification du MDSW en tant que DM ou DMDIV

*Guide MDCG 2019-11

Nous allons illustrer ce diagramme décisionnel par l'exemple d'un algorithme MDSW destiné à fournir des informations sur la prédisposition statistique au syndrome de Down (trisomie 21) au cours du premier et du deuxième trimestres de la grossesse. Le MDSW analyse les données d'entrée provenant de divers essais de DMDIV ainsi que des mesures échographiques de la clarté nucale. Le MDSW fournit aux cliniciens/obstétriciens un score de facteur de risque pour la probabilité qu'un fœtus présente des mutations génétiques au cours du premier ou du deuxième trimestre de la grossesse. Le score de risque indique si des tests diagnostiques supplémentaires sont nécessaires ou non pour confirmer la présence de mutations génétiques de la trisomie 21.

Appliquons cet exemple au logigramme décisionnel :

- La réponse à l'étape 1 est « OUI » car le logiciel a une finalité médicale et répond à la définition du MDSW. Le MDSW répond au critère (c) de la définition des

DMDIV au sens du Règlement (UE) 2017/746, car il fournit des informations concernant la prédisposition à une affection ou à une maladie.

- La réponse à l'étape de décision 2 est « NON » car une mesure d'imagerie est incluse dans le calcul.
- La réponse à l'étape 3 est « OUI », car l'objectif est essentiellement déterminé par des données sur les DMDIV, ce qui entraîne la qualification du logiciel en tant que IVD MDSW (car les données reçues des DMDIV (marqueurs) sont considérées comme déterminantes pour le résultat global du calcul (sortie) obtenu par le MDSW).

Dans le cas où un logiciel pilote ou influence l'utilisation d'un dispositif (matériel), le logiciel doit être considéré comme relevant de la réglementation respective du dispositif (matériel) piloté ou influencé.
Par exemple, on qualifiera d'IVD MDSW, le logiciel intégré dans le glucomètre FreeStyle® InsuLinx® avec calculateur d'insuline à action rapide intégré. Ce logiciel analyse et interprète la glycémie du patient, fournit par le lecteur, afin de suggérer au patient une dose d'insuline à s'administrer.

Nous venons de définir les logiciels de DMDIV et leur qualification en tant que tel. Nous allons à présent nous intéresser à leur classification d'après l'IVDR.

1.2.4. Classification des logiciels de DMDIV

La classification des DMDIV en général est basée sur le risque pour l'individu et le risque pour la santé publique. Conformément au Règlement (UE) 2017/746, les dispositifs sont répartis en 4 classes : classe A, classe B, classe C et classe D, en fonction de la destination des dispositifs et des risques pour l'individu et pour la santé publique qui leur sont inhérents : (Tableau 2)

Classe A	▪ Risque individuel **faible** ▪ **ET** Risque pour la santé publique **faible**
Classe B	▪ Risque individuel **modéré** ▪ ET/OU Risque pour la santé publique **faible**
Classe C	▪ Risque individuel **élevé** ▪ ET/OU Risque pour la santé publique **modéré**
Classe D	▪ Risque individuel **élevé** ▪ ET Risque pour la santé publique **élevé**

Tableau 2 : Les différentes classes règlementaire des DMDIV

Les critères de classifications sont énoncés à l'Annexe VIII de l'IVDR sous la forme de règles d'application et de règles de classification.

1.2.4.1. Règles d'application

Toutes les règles d'application de l'Annexe VIII de l'IVDR doivent être prises en compte lors de la classification d'un DMDIV.

Comme le stipule la Règle 1.1, l'application des règles de classification est régie par la destination des dispositifs. En d'autres termes, cela signifie que la classification d'un dispositif est définie par sa destination, telle que spécifiée par le fabricant.

Selon la Règle 1.2, *« Si un dispositif est destiné à être utilisé en combinaison avec un autre dispositif, les règles de classification s'appliquent séparément à chacun des dispositifs. »*

Il est important de noter, d'après la Règle 1.3, que les accessoires d'un DMDIV sont classés en soi, indépendamment des dispositifs avec lesquels ils sont utilisés.

Concernant les logiciels de DMDIV, une considération particulière doit être faite sur les règles d'application 1.4 et 1.9.
En effet, la Règle 1.4 stipule que : « *Le logiciel commandant un dispositif ou agissant sur son utilisation relève de la même classe que le dispositif. Si le logiciel est indépendant de tout autre dispositif, il est classé en soi.* » Cette règle ne s'applique donc qu'aux logiciels qui pilotent ou influencent l'utilisation d'un DMDIV. Elle doit être considérée au moins comme

une orientation pour trouver la bonne classification (minimale) des logiciels qui sont utilisés dans les DMDIV. Selon la 2ème phrase de cette règle, si le logiciel est indépendant de tout autre dispositif, il doit être classé dans sa propre catégorie en tant que telle. Par exemple, un logiciel qui intègre le génotype de plusieurs gènes pour prédire le risque de développement ou de récurrence d'une maladie ou d'un état pathologique est un IVD MDSW indépendant. Il est donc classé dans sa propre classe.
De plus, la Règle 1.9 énonce : « *Si plusieurs règles de classification s'appliquent au même dispositif, la règle qui s'applique est celle qui classe le dispositif dans la classe la plus élevée.* »

Pour classer les IVD MDSW indépendants de tout autre dispositif, un autre guide a été créé par le GCDM : *MDCG 2020-16 : Guidance on Classification Rules for in vitro Diagnostic Medical Devices under (EU) 2017/746 – IVDR*. Ce guide, relatif à l'application du Règlement (UE) 2017/746, traite de la classification des DMDIV et fournit des éclaircissements sur les règles de classification énoncées à l'Annexe VIII. L'objectif principal de ce document est de fournir des conseils aux fabricants, aux organismes notifiés et aux institutions de santé sur la manière de classer un DMDIV avant de le mettre sur le marché, de le rendre disponible sur le marché ou de le mettre en service dans l'UE.

1.2.4.2. Règles de classification

Pour déterminer la classification appropriée des MDSW dans le cadre de l'IVDR, le fabricant doit prendre en considération toutes les règles de classification et de mise en œuvre (Figure 4). Cette classification, dite réglementaire, permet ainsi de déterminer la procédure de marquage CE applicable au logiciel de DMDIV.

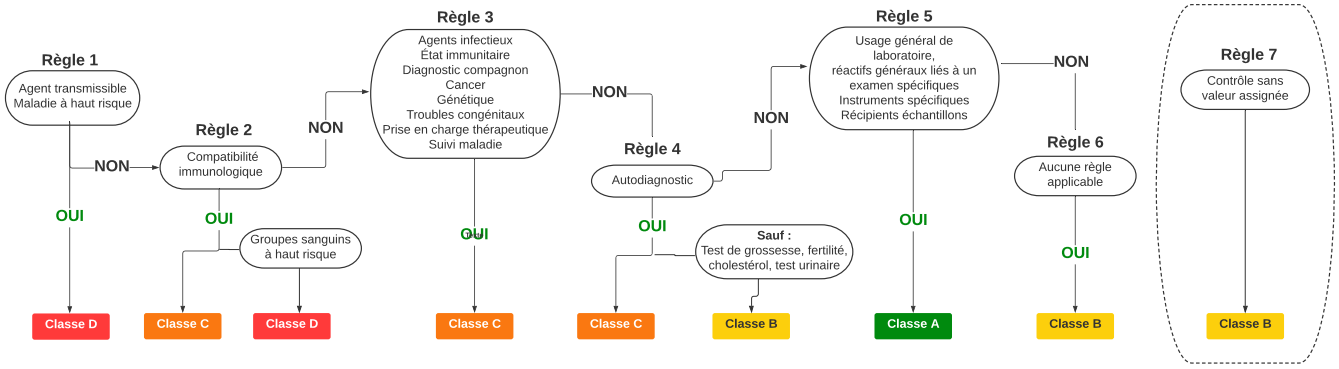

Figure 4 : Règles de classification des DMDIV

Il est important de noter que le risque lié à l'utilisation d'un logiciel n'est pas un critère de qualification. Cependant, il sera un critère de classification pour les logiciels disposant du statut de DMDIV (selon la classe de risque définie à l'Annexe VIII de l'IVDR). Il conditionnera la complexité des étapes réglementaires permettant la mise sur le marché du logiciel. Notamment, les logiciels de DMDIV de classes B, C et D, de même que les dispositifs de classe A stériles, seront soumis à l'évaluation d'un Organisme Notifié pour leur marquage CE. (14)

En outre, si le DMDIV ne suit aucune règle, il appartiendra de fait à la classe B (Règle 6).

Nous pouvons citer comme exemples :

- Un test de grossesse digital Clearblue®. C'est un test numérique qui fait appel à un logiciel dans un objectif d'autodiagnostic. Ce test suit la Règle 4 mais fait partie de l'exception « sauf : test de grossesse, fertilité, cholestérol, test urinaire » : il appartient donc à la classe B.

- Les logiciels qui utilisent des paramètres maternels tels que l'âge, la concentration en marqueurs sériques et les informations obtenues par échographie fœtale pour évaluer le risque de trisomie 21, doivent être classés dans la classe C selon la Règle 3(l) de

l'IVDR : *« Les dispositifs relèvent de la classe C s'ils sont destinés : au dépistage de troubles congénitaux chez l'embryon ou le fœtus. »*

- Un logiciel destiné à évaluer le niveau de fibrose hépatique grâce au dosage sérique des marqueurs hépatiques du patient et après report des résultats et analyse par le logiciel, ce dernier calculera et affichera des scores d'estimation de fibrose hépatique afin d'estimer le stade de la fibrose. Il doit être classé dans la classe C selon la Règle 3(g) de l'IVDR : *« Les dispositifs relèvent de la classe C s'ils sont destinés : à être utilisés pour évaluer le stade de la maladie, lorsqu'un résultat erroné risque de conduire à une décision de prise en charge du patient qui mettrait en danger sa vie ou celle de sa descendance. »*

- Le système Biofire® Filmarray® est un système de PCR multiplex qui fonctionne grâce à un logiciel qui analyse et rapporte les résultats dans un format simple et facile à lire. Dans le panel Méningite-Encéphalite (EM), il teste directement dans le liquide céphalo-rachidien les 14 pathogènes les plus pertinents associés à l'EM, y compris des bactéries, des virus et un parasite. L'EM étant une maladie à haut risque, ce logiciel répond à la Règle 1 et est donc de classe D.

De plus, il convient de noter qu'une modification ou l'ajout d'une fonctionnalité d'un logiciel peut conduire à le qualifier de IVD MDSW ou à réviser la classification de ce dernier. Les fabricants doivent donc évaluer l'impact potentiel de toute modification de la fonction, de l'utilisation, de la conception essentielle et des caractéristiques de fabrication sur la qualification du logiciel en tant que DMDIV et sur sa classification (y compris la classification de la combinaison de l'IVD MDSW avec un autre DM).
De même, un module qui est ajouté à un logiciel peut être qualifié de IVD MDSW en tant que tel.
Pour déterminer la classe règlementaire d'une combinaison d'un IVD MDSW modifié et d'un DM, il faut tenir compte de la destination et de la fonctionnalité de cette nouvelle combinaison.

Nous venons de voir la classification réglementaire, nous allons maintenant voir la classification de sécurité qui s'applique à tous les logiciels de DM (Tableau 3).

Type de logiciel de DM	Classification réglementaire	Classification de sécurité
Logiciel incorporé dans un DM	Dépend du DM	✓
Logiciel DM en soi	✓	✓

Tableau 3 : Classification applicable en fonction du type de MDSW

1.2.5. Classes de sécurité du logiciel de DM

Cette classification de sécurité permet de préciser les exigences pour la conception et le développement d'un logiciel de DM ou de DMDIV. De ce fait, elle est applicable à tous les logiciels de DM en général.

La classification de sécurité des logiciels de DM est établie suivant les critères définis par la norme EN 62304 : *Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel.*

Suivant le paragraphe 4.3 de cette norme harmonisée, les logiciels de DM sont répartis en 3 classes de sécurité : classe de sécurité A, B et C.

Les règles de classification de sécurité sont fondées sur les risques liés aux défaillances potentielles du logiciel. Ainsi, la classe de sécurité d'un logiciel de DM est une conclusion de son analyse de risque. Ainsi, une gestion des risques faite à bon escient peut permettre d'abaisser sa classe de sécurité et d'alléger considérablement le travail nécessaire pour la conception et le développement du logiciel. (15)

Ainsi, le fabricant doit attribuer à chaque système logiciel une classe de sécurité du logiciel (A, B ou C) en fonction des effets possibles sur le patient, l'opérateur ou d'autres personnes résultant d'un phénomène dangereux auquel le système logiciel peut contribuer.

Les classes de sécurité du logiciel doivent au départ être attribuées en se basant sur le degré de sévérité suivant : (Tableau 4)

- Classe A : Aucune blessure ou atteinte à la santé n'est possible
- Classe B : Une blessure non grave est possible
- Classe C : La mort ou une blessure grave est possible (16)

Si le phénomène dangereux peut résulter d'une défaillance du système logiciel à se comporter conformément aux spécifications, la probabilité d'une telle défaillance doit être supposée de 100%.

Si le risque de mort ou de blessure grave provenant d'une défaillance logicielle est ensuite ramené à un niveau acceptable (tel que défini par l'ISO 14971) par des mesures de maîtrise des risques matériels, soit en réduisant les conséquences de la défaillance, soit en réduisant la

probabilité de mort ou de blessure grave provenant de cette défaillance, la classe de sécurité du logiciel peut être ramenée de C à B. Si le risque de blessure non grave provenant d'une défaillance logicielle est ramené à un niveau acceptable par des mesures de maîtrise des risques matériels, la classe de sécurité du logiciel peut être ramenée de B à A.

Classe de sécurité	Niveau de risque	Exemples
Classe A	Une défaillance du système logiciel ne peut pas contribuer à une situation dangereuse ou une défaillance du système logiciel peut contribuer à une situation dangereuse qui n'engendre pas un risque inacceptable.	Un logiciel avec des contrôles électroniques intégrés pour les procédures de contrôle de qualité des DMDIV. Ces procédures de contrôle de qualité sont destinées à fournir aux utilisateurs l'assurance que le dispositif fonctionne conformément aux spécifications.
Classe B	Une défaillance du système logiciel peut contribuer à une situation dangereuse qui engendre un risque inacceptable et qui ne peut pas entraîner une blessure grave*.	Un logiciel qui analyse et interprète la densité optique fournie par un lecteur ELISA, le motif des lignes ou des points d'un blot.
Classe C	Une défaillance du système logiciel peut contribuer à une situation dangereuse qui engendre un risque inacceptable et qui peut entraîner une blessure grave*.	- Une défaillance du MDSW qui évalue le risque de trisomie 21 engendre un risque inacceptable et qui menace la vie du fœtus. - De même, une défaillance d'un MDSW qui fournit des recommandations de doses d'insuline à un patient engendre un risque inacceptable et qui menace la vie du patient en provoquant une hypoglycémie ou une hyperglycémie.

Tableau 4 : Classes de sécurité des logiciels de DM suivant la norme EN 62304 et exemples associés

***Blessure grave : blessure ou maladie qui, directement ou indirectement :**

(a) menace la vie, ou

(b) entraîne une carence permanente d'une fonction physiologique ou endommage de manière définitive une structure du corps, ou

(c) nécessite une intervention médicale ou chirurgicale pour prévenir une carence permanente d'une fonction physiologique ou un endommagement définitif d'une structure du corps.

NOTE : Carence permanente signifie une carence irréversible ou un endommagement d'une structure du corps ou d'une fonction, à l'exclusion des carences ou préjudices insignifiants.

Ainsi, le fabricant doit attribuer à chaque système logiciel, qui contribue à la mise en œuvre des mesures de maîtrise des risques, une classe de sécurité du logiciel, fondée sur les effets possibles du phénomène dangereux qui sont couverts par la mesure de maîtrise du risque.

Le fabricant doit consigner la classe de sécurité du logiciel attribuée à chaque système logiciel dans le dossier de gestion des risques.
Lorsqu'un système logiciel est décomposé en éléments logiciels, ces derniers héritent de la classe de sécurité du logiciel de l'élément logiciel initial (ou du système logiciel) à moins que le fabricant ne justifie par écrit une classification dans une classe différente de sécurité du logiciel. Une telle justification doit expliquer la manière dont les nouveaux éléments logiciels sont différenciés pour pouvoir être classés séparément. Le fabricant doit consigner la classe de sécurité du logiciel de chaque élément logiciel si cette classe est différente de la classe de l'élément logiciel à partir duquel il a été créé par décomposition.
Pour la conformité à la présente norme, lorsqu'un processus est exigé pour les éléments logiciels d'une classe spécifique, le fabricant doit utiliser les processus et tâches qui sont exigés par la classe de sécurité de l'élément logiciel la plus élevée définie dans le groupe, à moins que le fabricant ne justifie par écrit, dans le dossier de gestion des risques, l'utilisation d'une classification plus basse.
Pour chaque système logiciel, les exigences de la classe C doivent être appliquées jusqu'à attribution d'une classe de sécurité du logiciel.

D'après l'Annexe B.4.3 de la norme EN 62304, le risque associé au logiciel en tant que partie constituante d'un DM, en tant qu'accessoire d'un DM, ou en tant que DM à part entière, est utilisé comme l'élément d'entrée d'un plan de classification de la sécurité logicielle qui permet alors de déterminer les processus à utiliser au cours du développement et de la maintenance du logiciel.
Le risque est défini comme étant une combinaison de la gravité du dommage et de la probabilité de sa survenue. Cependant, il n'existe pas de consensus quant à la manière de déterminer la probabilité des défaillances logicielles sur la base de méthodes statistiques conventionnelles. Par conséquent, dans la présente norme, la classification du système logiciel est fondée sur la gravité du danger résultant de la défaillance du logiciel, en supposant que la défaillance aura lieu. Les systèmes logiciels qui contribuent à la mise en œuvre des mesures de maîtrise du risque sont classés en fonction de la gravité du danger correspondant.

Après ces étapes de qualification et classification du logiciel de DMDIV, le fabricant devra mettre en conformité son dispositif afin d'obtenir le marquage CE nécessaire à sa mise sur le marché européen.

1.3. Mise en conformité des logiciels

Pour obtenir le marquage CE, le fabricant doit suivre la réglementation dont relève ce dispositif. Pour se faire, les IVD MDSW devront répondre aux exigences générales en matière de sécurité et de performances contenues dans l'Annexe I de l'IVDR.
Ainsi, après avoir déterminé quelles exigences seront applicables à notre logiciel de DMDIV, le fabricant devra prouver le respect à ces exigences, en s'appuyant par exemple sur le cadre normatif constitué des normes européennes harmonisées, des normes de la Commission électrotechnique internationale (CEI), ou encore des normes internationales ISO.
Afin de démontrer la conformité de son produit à la réglementation européenne, le fabricant devra alors :

- Élaborer une documentation technique (ou dossier technique). Ce dossier est un élément important, car il regroupe toutes les informations concernant le dispositif et permettra son accès au marché une fois le marquage CE apposé. La DT est maintenue tout au long du cycle de vie du produit et sera, en fonction de la classification réglementaire du logiciel, évaluée par l'ON.
- Établir son système de management de la qualité (SMQ). Celui-ci sera alors audité par l'ON et, une fois approuvé, un certificat UE relatif au système de gestion de la qualité sera alors délivré par l'ON.

1.3.1. La documentation technique

Les fabricants souhaitant développer et mettre sur le marché des logiciels entrant dans le champ d'application de la définition d'un DMDIV doivent établir une DT conséquente autour du logiciel.

C'est l'élément central qui permet d'attester de la conformité des dispositifs médicaux, en général, aux exigences qui leur sont applicables et de justifier ainsi le marquage CE. Tout DMDIV quelle que soit sa classe doit faire l'objet d'une documentation technique. Cette documentation est un élément essentiel puisqu'elle regroupe toutes les informations sur le dispositif dans tout son cycle de vie : depuis sa conception jusqu'à la fin de sa mise sur le marché, en passant par les étapes de production et de recueil des informations « post-market ». (17)
Le contenu de ce dossier est énoncé dans les Annexes II et III de l'IVDR.

Les DMDIV de classe A sont assujetti à une simple auto-déclaration du fabricant, contrairement à ceux de classes B, C et D qui nécessiteront l'intervention d'un ON afin d'évaluer cette DT.
Cette évaluation implique une analyse précise et exhaustive de documents. L'ON évalue donc la conformité du dispositif par un examen complet de ce dossier. Il a pour objectif notamment de vérifier la validité des preuves cliniques concernant les performances du dispositif et de valider les conclusions tirées par le fabricant quant à la conformité avec les exigences générales.
L'ON fournit alors au fabricant un rapport sur l'évaluation de la documentation technique. Si le dispositif est conforme aux dispositions de l'IVDR, l'ON délivre un certificat d'évaluation UE de la documentation technique. En revanche, si cette évaluation soulève des interrogations de la part de l'ON, des preuves supplémentaires concernant l'applicabilité des exigences seront à fournir.

D'après l'article 6.4 de l'Annexe II, la DT contient les preuves de la validation du logiciel tel qu'il est utilisé dans le dispositif fini. Ainsi, cet article porte sur la vérification, la validation du logiciel, la description de la conception et du processus de développement du logiciel. Ces informations incluent en règle générale un résumé des résultats de l'ensemble de la vérification, de la validation et des essais réalisés en interne et applicables dans un environnement d'utilisation réel avant la libération finale. (4)

1.3.2. Choix des procédures d'évaluation de la conformité

Les procédures d'évaluation de la conformité sont conçues pour évaluer la conformité aux exigences générales de l'IVDR. Elles constituent les obligations principales du fabricant pour la mise sur le marché de logiciels de DMDIV dans l'EEE. Lorsque la conformité d'un logiciel de DMDIV est acquise selon les procédures, le fabricant peut apposer le marquage CE sur le dispositif concerné et ainsi le mettre sur le marché.
Le choix de la procédure, qui incombe au fabricant, doit être effectué selon les modalités décrites dans l'IVDR pour les logiciels de DMDIV, en fonction de la classe du dispositif.
Le choix de la procédure la plus adaptée aux besoins du fabricant peut être guidé par les critères suivants :

- Le fonctionnement de l'entreprise en termes d'organisation permettant de garantir la qualité requise (système qualité) ; et

- Le mode de conception et de fabrication du DMDIV en tenant compte des processus externalisés.

L'IVDR indique quelles sont les procédures envisageables pour chaque classe de DMDIV (Tableau 5) :

<table>
<tr><td>Classe A</td><td>Classe B</td><td colspan="2">Classe C</td><td colspan="2">Classe D</td></tr>
<tr><td>Déclaration de conformité CE (Annexe IV)</td><td>Audit système qualité du fabricant (Annexe IX)</td><td>Audit système qualité du fabricant (Annexe IX)</td><td>Examen CE de type (Annexe X)</td><td>Audit système qualité du fabricant (Annexe IX)</td><td>Examen CE de type (Annexe X)</td></tr>
<tr><td rowspan="2"></td><td>ET</td><td>ET</td><td>ET</td><td>ET</td><td>ET</td></tr>
<tr><td>Évaluation de la documentation technique (Annexe IX)</td><td>Évaluation de la documentation technique (Annexe IX)</td><td>Évaluation de l'assurance de la qualité de la production (Annexe XI)</td><td>Évaluation de la documentation technique (Annexe IX)</td><td>Évaluation de l'assurance de la qualité de la production (Annexe XI)</td></tr>
<tr><td>Pas d'intervention de l'ON</td><td colspan="5">Intervention d'un Organisme Notifié</td></tr>
</table>

Tableau 5 : Procédures d'évaluation de la conformité selon la classe du DMDIV

Le fabricant a l'obligation de respecter le processus réglementaire qu'il a choisi avant de mettre le dispositif sur le marché et il doit impérativement être capable de démontrer son approche. En outre, selon le type de DMDIV, il peut également être nécessaire de faire vérifier la conformité de ce processus par un tiers : l'ON. La seule procédure qui ne nécessite pas d'ON est la « Déclaration CE de conformité ». Cette procédure ne peut être utilisée que pour les DMDIV de classe A. (18)

Quelle que soit la procédure d'évaluation de la conformité choisie par le fabricant, il y aura toujours deux composantes essentielles pour prouver la conformité du dispositif :

- L'un qui a trait au produit : la DT, le but étant de prouver que les produits sont sûrs et performants.

- L'autre qui a trait à l'organisation interne du fabricant : la mise en place d'un SMQ, le but étant de prouver le maintien de la sécurité et de la performance des dispositifs dans le temps. (19)

Ce qui va différer en fonction de la procédure choisie, c'est le niveau d'implication de l'ON :

- Annexe IX : Évaluation de la conformité sur la base d'un système de gestion de la qualité et de l'évaluation de la documentation technique. Ici, l'ON réalise une revue complète du SMQ incluant la conception, ainsi qu'une évaluation de la DT.
- Annexe X : Évaluation de la conformité sur la base de l'examen de type. C'est la procédure par laquelle l'ON évalue la DT, et vérifie que le type (échantillon représentatif du dispositif) a été fabriqué en conformité avec la DT.
  Cette annexe doit obligatoirement être combinée avec l'Annexe XI.
- Annexe XI : Évaluation de la conformité sur la base de l'assurance de la qualité de la production. Ici, l'ON vérifie que le SMQ est de nature à garantir que le dispositif est conforme au type et aux dispositions applicables du Règlement. La revue du SMQ exclut ici la conception. (19)

Ainsi, les IVD MDSW peuvent être mis sur le marché de 2 manières différentes :

- En tant que DMDIV à part entière,
- OU en tant que composant intégral ou en partie d'un DMDIV.

Option 1 : Comme un DMDIV à part entière :

C'est le cas des IVD MDSW pouvant être mis sur le marché ou mis en service en tant que tel, indépendamment de tout autre produit.
Nous pouvons prendre ici l'exemple d'un logiciel qui calcule la dose d'anticoagulant pour les patients sous traitement anticoagulant oral, à partir des résultats des tests INR saisis par les instruments IVD et d'autres données patients saisies manuellement.

Concernant l'évaluation de la conformité de ces IVD MDSW mis sur le marché en tant que dispositif ou mis en service en tant que tel, ils doivent faire l'objet d'un processus réglementaire approprié qui tient compte de la qualification, de la classification et de la destination de l'usage prévu du logiciel. Si il est couvert par une des règlementations sur les DM, le fabricant devra s'assurer que toutes les exigences règlementaires pour la mise sur le

marché et l'évaluation de la conformité ont été remplies. Comme indiqué à l'article 7 du MDR et de l'IVDR, cela implique également que toute allégation relative à l'objectif médical prévu de leur MDSW soit étayée par des preuves cliniques. Si ce n'est pas le cas, le logiciel ne répond pas aux exigences de la réglementation et ne pourra donc pas être marqué CE en tant que DM ni DMDIV, ni présenter lesdites revendications. (5)

Option 2 : Comme composant/partie intégrante d'un dispositif :

C'est le cas des IVD MDSW qui sont mis sur le marché ou mis en service en tant que composant/partie intégrante d'un appareil.

Par exemple, un glucomètre calculateur de dose, composé de matériel et d'un logiciel, destiné à suggérer au patient une dose d'insuline rapide à s'administrer à partir de la glycémie journalière du patient.

Concernant leur évaluation de la conformité, ces IVD MDSW destinés spécifiquement à remplacer une partie ou un composant d'un dispositif et qui modifient de manière significative les caractéristiques de performance ou de sécurité ou la destination du dispositif doivent être considérés comme relevant de la réglementation respective du dispositif (matériel) piloté ou influencé. Dans ce cas, le logiciel sera évalué dans le cadre du processus réglementaire appliqué au dispositif dans son ensemble, lorsqu'il est mis sur le marché.
L'application des règles de classification à ces dispositifs matériels, qui sont de facto une combinaison du dispositif médical matériel et de l'IVD MDSW, nécessite un examen attentif de la finalité du logiciel. Concernant notre exemple, le logiciel inclus dans le glucomètre FreeStyle® InsuLinx® se doit de répondre aux exigences de l'IVDR car il relève de la règlementation du glucomètre lui-même qualifié de DMDIV et de classe C, car suit la Règle 3(j) de l'IVDR : *« Les dispositifs relèvent de la classe C s'ils sont destinés : à la surveillance des niveaux de médicaments, de substances ou de composants biologiques, lorsqu'un résultat erroné risque de conduire à une décision de prise en charge du patient qui mettrait en danger sa vie ou celle de sa descendance. »*

1.3.3. Démonstration de la conformité des logiciels de DMDIV

1.3.3.1. Les exigences générales

L'IVDR entend par « exigences générales » les conditions auxquelles les DMDIV doivent impérativement satisfaire pour pouvoir être mis sur le marché.

L'Annexe I de l'IVDR décrit ces exigences générales de sécurité et de performances. (18) (Tableau 6)
Comme évoqué précédemment, afin de prouver la conformité de son dispositif, le fabricant doit établir une liste des exigences applicables à son logiciel de DMDIV. En effet, les exigences réglementaires peuvent parfois varier selon la désignation du dispositif ainsi que sa classification. Certaines de ces exigences générales en matière de sécurité et de performances visent spécifiquement les logiciels de DMDIV.

	CONTENU	EXEMPLES
CHAPITRE I	Il décrit les exigences générales applicables à tout DMDIV, incluant la gestion des risques et l'évaluation des performances.	*8. « Tous les risques connus et prévisibles ainsi que tous les effets indésirables sont réduits au minimum et sont acceptables au regard des bénéfices potentiels évalués que présentent pour le patient et/ou l'utilisateur les performances prévues du dispositif dans des conditions normales d'utilisation. »*
CHAPITRE II	Il définit les exigences relatives aux performances, à la conception et à la fabrication du dispositif en question.	*13.2. « Les dispositifs sont conçus et fabriqués de manière à éliminer ou à réduire autant que possible : (…)* *d) tout risque associé à une éventuelle interaction négative entre les logiciels et l'environnement informatique dans lequel ceux-ci fonctionnent et avec lequel ils interagissent (…) »*
CHAPITRE III	Il définit les exigences relatives aux informations fournies avec le dispositif.	*20.4.1. « La notice d'utilisation contient toutes les informations suivantes : (…)* *a h) pour les dispositifs comportant des systèmes électroniques programmables, notamment des logiciels, ou des logiciels qui sont des dispositifs à part entière, les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la*

	protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu. »

Tableau 6 : Contenu de l'Annexe I de l'IVDR

Au sein du chapitre II, le point 16 des exigences essentielles est dédié spécifiquement aux logiciels de DMDIV. Il indique que leur conception doit garantir la répétabilité, la fiabilité, ainsi que les performances conformes à l'usage qui en est prévu. Des mesures doivent être prises afin d'éliminer ou de réduire tous les risques ou dégradations des performances de ces dispositifs. Les éléments suivants sont détaillés :

- Article 16.1 : « Les dispositifs comportant des systèmes électroniques programmables, notamment des logiciels, ou des logiciels qui sont des dispositifs à part entière sont conçus de manière à garantir la répétabilité, la fiabilité et les performances eu égard à leur utilisation prévue. En condition de premier défaut, des moyens adéquats sont adoptés pour éliminer ou réduire autant que possible les risques qui en résultent ou la dégradation des performances. »

Cette exigence sera démontrée par les performances analytiques du produit dans la vérification et validation du dispositif *(cf. 1.3.3.6 Évaluation des performance*s).

- Article 16.2 : « Pour les dispositifs qui comprennent des logiciels ou pour les logiciels qui sont des dispositifs à part entière, ces logiciels sont développés et fabriqués conformément à l'état de l'art compte tenu des principes du cycle de développement, de gestion des risques, y compris la sécurité de l'information, de vérification et de validation. »
- Article 16.3 : « Les logiciels visés à la présente section qui sont destinés à être utilisés en combinaison avec des plateformes informatiques mobiles sont conçus et fabriqués en tenant compte des caractéristiques spécifiques de la plateforme mobile (par exemple, taille et rapport de contraste de l'écran) et des facteurs externes liés à leur utilisation (variation du niveau sonore ou de la luminosité dans l'environnement). »
- Article 16.4 : « Le fabricant indique les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu. » (4)

1.3.3.2. Gestion des risques

Le concept selon lequel un fabricant doit éliminer ou réduire les risques autant que possible lors de la conception et de la fabrication du dispositif est inclus dans les exigences générales. Les fabricants énumèrent ces risques, ainsi que les mesures prises pour les éliminer ou les réduire au maximum dans un dossier de gestion des risques, qui fait partie de la documentation technique du dispositif. (20)

1.3.3.3. Exigences de sécurité logicielles

La sécurisation d'un logiciel de DMDIV nécessite de nombreuses considérations. Voici des exemples clés d'exigences de sécurité qui pourraient aller au-delà des exigences générales existantes :

- Authentification de l'utilisateur – validation de l'accès de l'utilisateur et application de privilèges pour différentes classes d'utilisateurs.
- L'inviolabilité – empêcher les modifications physiques et logicielles de l'appareil qui permettent de contourner les fonctions de sécurité.
- Stockage sécurisé – garantir que les données stockées sont protégées contre l'accès en ligne et hors ligne, notamment par des techniques telles que le stockage de fichiers cryptés et la gestion des droits numériques.
- Communications sécurisées – assurer la sécurité du transfert des données tout en empêchant les accès indésirables par le biais des canaux connectés (réseau, USB, etc.). Bien que la connectivité du réseau soit la priorité absolue, les autres canaux sont vulnérables aux attaques.
- Fiabilité et disponibilité – maintenir un fonctionnement sûr de l'appareil face à des attaques continues. (18)

1.3.3.4. Spécifications techniques communes

De manière spécifique, la directive 98/79/CE avait déjà introduit pour les dispositifs les plus critiques, le concept de « spécifications techniques communes » (STC). Ces spécifications établissent les critères appropriés d'évaluation et de réévaluation des performances, les critères de libération des lots, les méthodes de référence et les matières de référence. Ces STC sont préparées par les experts des autorités des États membres et elles sont adoptées officiellement et publiées dans le Journal Officiel de l'UE (JOUE). Les fabricants sont, en

règle générale, tenus de respecter ces STC. Si, pour une raison dûment justifiée, ils ne se conforment pas à ces spécifications, ils doivent adopter des solutions d'un niveau équivalent. (20)

1.3.3.5. Normes européennes harmonisées

En raison de la nature globale des exigences générales, qui s'appliquent à l'ensemble des dispositifs médicaux, et de la difficulté à garantir une approche commune de la part de tous les fabricants et organismes notifiés, la « nouvelle approche »[5] attribue un rôle et une importance particulière aux normes. Alors que les exigences générales européennes fournissent des objectifs en terme de démonstration de la sécurité et de la performance de fonctionnement d'un DMDIV, les normes harmonisées fournissent des **méthodes pour atteindre ces objectifs**. Ainsi, elles sont utiles pour les fabricants dans le développement de leur dispositif et l'évaluation des performances associés. Leurs applications n'est pas obligatoire pour mettre un produit sur le marché dans l'EEE. Toutefois, conformément à l'article 8 de l'IVDR, la conformité à toutes les normes européennes harmonisées est une présomption de conformité aux exigences générales. (20)

Exigences générales pour la sécurité des produits

La norme CEI EN 82304-1 *(Logiciels de santé – Partie 1 : exigences générales pour la sécurité des produits)*, datant de 2016, est harmonisée pour la réglementation européenne sur les dispositifs médicaux. Sa mise en œuvre confère donc aux fabricants de DMDIV une présomption de conformité par rapport à des exigences réglementaires. Cette norme traite de logiciel de santé. Elle a pour objet d'assurer la sécurité et la sûreté des produits logiciels de santé autonomes conçus pour fonctionner sur des plateformes informatiques générales. Par exemple, certains logiciels de calcul de risque de trisomie 21 fœtale sont installés directement sur un ordinateur du réseau hospitalier.

Gestion des risques

La norme EN ISO 14971 est la norme européenne harmonisée relative à la gestion des risques. Dans le cadre des MDSW, elle sera complétée par la norme CEI EN 62304 qui introduit des exigences complémentaires en terme de gestion de risques des logiciels.

[5] Le concept de « Nouvelle approche » est une méthode d'élaboration des directives européennes qui date de 1985. Ces directives « Nouvelle approche » doivent se référer aux normes européennes harmonisées pour les spécifications techniques du produit lors de sa mise sur le marché.

1.3.3.6. Évaluation des performances

Un élément critique de la documentation technique qui démontre la conformité du DMDIV aux exigences générales est l'évaluation des performances du dispositif. Cette évaluation démontre que les performances du dispositif satisfont aux allégations du fabricant et à la destination indiquée, en tenant compte de l'état de la technique généralement reconnu. Le type d'évaluation des performances est directement lié à :

- La nature du DMDIV (détermination qualitative ou quantitative)
- La destination (diagnostic, dépistage, contrôle, prédisposition, pronostic, prédiction, etc.)
- Le type d'échantillon
- La population ciblée testée
- L'utilisateur et l'environnement prévus
- Les caractéristiques de performances analytiques et cliniques attendues, et
- La technologie mise en œuvre. (20)

D'après l'article 56(1) de l'IVDR : « Le fabricant doit spécifier et justifier le niveau de PREUVES CLINIQUES nécessaire pour démontrer la conformité aux exigences générales de sécurité et de performance pertinentes. Ce niveau de preuves cliniques doit être approprié compte tenu des caractéristiques du dispositif et de sa destination. »
De plus, l'article 2(36) de l'IVDR définit les preuves cliniques comme : « les données cliniques et les résultats de l'évaluation des performances (IVDR) concernant un dispositif, en quantité et qualité suffisantes pour permettre une évaluation qualifiée de la sécurité du dispositif et de la réalisation des bénéfices cliniques prévus, lorsqu'il est utilisé comme prévu par le fabricant. »

L'évaluation des performances est un processus continu, mené tout au long du cycle de vie d'un MDSW. Il s'agit d'un processus structuré, transparent, itératif et continu qui fait partie du système de gestion de la qualité d'un dispositif.
Trois éléments déterminants sont à prendre en compte lors de la compilation des preuves cliniques pour chaque logiciel de DMDIV :

- La **validité scientifique**,
- La **performance analytique**,
- La **performance clinique**. (21)

Validité scientifique

La validité scientifique s'entend comme la mesure dans laquelle le résultat du DMDIV, basé sur les entrées et les algorithmes sélectionnés, est associé à l'état physiologique ou à la condition clinique ciblée. Cette association doit être bien fondée ou cliniquement acceptée (par exemple, existence d'un cadre scientifique ou d'un niveau de preuve suffisant). La validité scientifique d'un IVD MDSW doit démontrer qu'il correspond à la situation clinique, à l'état, à l'indication ou au paramètre défini dans l'objectif prévu du logiciel.

Les preuves de l'existence de la validité scientifique peuvent être générées, par exemple, par des recherches documentaires, des directives professionnelles, des études de validation du concept ou des enquêtes cliniques/études de performance clinique propres au fabricant.

Par exemple, pour un logiciel de calcul de dose d'insuline, intégré à un glucomètre, la validité scientifique pourrait porter sur la corrélation de la mesure du glucose sanguin avec la dose d'insuline que le patient diabétique devrait s'administrer.

Performance analytique

Les performances analytiques déterminent la capacité d'un DMDIV à détecter/mesurer correctement un analyte/marqueur donné. La validation des performances analytiques est la démonstration de la capacité du dispositif à générer avec exactitude, fiabilité et précision les résultats attendus, à partir des données d'entrée.

Les preuves à l'appui des performances analytiques peuvent être générées par des activités de vérification et de validation, par exemple des essais au niveau de l'unité, de l'intégration et du système, ou en générant de nouvelles preuves par l'utilisation de bases de données sélectionnées, de registres sélectionnés, de bases de données de référence ou de données de patients collectées précédemment.

Concernant la validation d'un glucomètre par exemple, on détermine, dans un premier temps, sa précision par une étude de répétabilité. Le sang total d'un patient va être analysé 30 fois de suite, dans les mêmes conditions, afin de déterminer sa glycémie avec le même glucomètre. Puis, on cherche à déterminer l'exactitude de ce glucomètre. On détermine 10 fois de suite, dans les mêmes conditions, à l'aide du même glucomètre, la glycémie d'un échantillon de sang total que l'on compare à la valeur réelle de la glycémie du même échantillon de sang total (obtenue à l'aide d'une méthode de référence comme un automate de biochimie par exemple). A l'aide des résultats obtenus, l'exactitude peut être déterminée par la mesure du biais. (22) Il faut donc confirmer que le lecteur peut détecter de manière fiable et précise le

glucose sanguin afin que l'IVD MDSW suggère au patient une dose d'insuline à s'administrer correcte.

Performance clinique

Les performances cliniques déterminent la capacité d'un DMDIV à produire des résultats en corrélation avec un état physiologique/une pathologie en fonction de la population cible et de l'utilisateur auquel le dispositif est destiné. La validation des performances cliniques est la démonstration de la capacité d'un dispositif à produire des résultats cliniquement pertinents conformément à l'objectif visé (sensibilité diagnostique, spécificité diagnostique, valeur prédictive positive/négative…). Elle doit être envisagée à chaque nouvelle version du logiciel. La pertinence clinique d'un IVD MDSW est d'un impact positif :

- Sur la santé d'un individu, exprimé en termes de résultats cliniques mesurables et pertinents pour le patient, y compris des résultats liés au diagnostic, à la prédiction du risque, à la prédiction de la réponse au traitement, ou
- Liés à sa fonction, telle que celle de dépistage, de surveillance, de diagnostic ou d'aide au diagnostic des patients, ou
- Sur la prise en charge des patients ou la santé publique.

Les preuves de la performance clinique peuvent être obtenues en testant le logiciel évalué, ou un dispositif équivalent, dans la population cible et pour l'utilisation prévue. La méthodologie appliquée doit être appropriée aux caractéristiques de l'appareil et de l'utilisation prévue et peut inclure des tests précliniques, une enquête clinique ou une étude de performance clinique. (23)

Continuons avec le même exemple, le fabricant devra démontrer par une investigation clinique par exemple, que le logiciel a été testé pour cette utilisation (calculateur de dose), dans la population cible (patients diabétiques), dans les conditions d'utilisation prévues, dans l'environnement de fonctionnement et d'utilisation et avec tous les groupes d'utilisateurs prévus. Cette validation des performances cliniques comprendra aussi l'évaluation de la sécurité et de l'efficacité et pourra appuyer la démonstration des avantages cliniques du logiciel. Il sera donc démontré que les utilisateurs peuvent obtenir des résultats cliniquement pertinents grâce à une utilisation prévisible et fiable du MDSW.

Un guide a été élaboré par le GCDM concernant l'évaluation clinique et l'évaluation des performances des logiciels de DM et de DMDIV : le *MDCG 2020-1 : Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software.* Il fournit

un cadre pour la détermination du niveau approprié de preuve clinique requis pour que les logiciels de DM et DMDIV répondent aux exigences présentées dans le MDR ou l'IVDR. Ce document s'applique uniquement aux logiciels destinés à être utilisés, seuls ou en combinaison, à des fins médicales conformément à la définition d'un dispositif médical dans le MDR ou l'IVDR. En effet, un logiciel ayant une finalité médicale possède à un avantage clinique, et nécessite donc des preuves cliniques associées dans le cadre de l'évaluation de sa conformité.

En revanche, dans le cas d'un logiciel pour lequel le fabricant ne revendique aucune finalité médicale, qui est destiné à piloter ou influencer un dispositif médical, les preuves cliniques sont fournies dans le contexte du dispositif piloté ou influencé et sont donc hors du champ d'application de ce guide MDCG 2020-1 (Tableau 7).

Modèle de logiciel	**Évaluation clinique (MDR) / Évaluation des performances (IVDR)**
MDSW (avec une finalité indépendante et un avantage CLINIQUE revendiqué)	MDSW uniquement
MDSW (dont l'objectif et l'avantage CLINIQUE revendiqué sont liés à la conduite ou à l'influence d'un dispositif médical dans un but médical)	MDSW et le dispositif médical piloté ou influencé
	NOTE : Si un logiciel pilote ou influence plus d'un dispositif médical, une ÉVALUATION CLINIQUE (MDR) / ÉVALUATION DE PERFORMANCE (IVDR) indépendante est requise pour chaque combinaison prévue et cliniquement viable entre le logiciel et le dispositif.
Logiciel pilotant ou influençant l'utilisation d'un dispositif médical (sans finalité indépendante ni avantage clinique indépendant revendiqué)	Dispositif médical piloté ou influencé, y compris le logiciel (composant ou accessoire)
	NOTE : Hors champ d'application de ce guide MDCG 2020-1.

Tableau 7 : Différentes exigences en matière de MDSW et d'évaluation clinique (MDR) / évaluation des performances (IVDR)

Prenons l'exemple du logiciel permettant d'évaluer le niveau de fibrose hépatique, le FibroMeter® VCTE. Il est destiné à fournir un score d'estimation de la fibrose hépatique afin d'en estimer le stade. Ce logiciel possédant un avantage clinique, l'évaluation de sa conformité nécessite donc des preuves cliniques certaines.

À l'inverse, un logiciel qui fournit une interface utilisateur supplémentaire pour contrôler une pompe à insuline, est destiné à virtualiser les commandes d'une pompe à insuline en se connectant sur une application pour smartphone. Étant donné que le logiciel pilote la pompe à insuline, il n'accomplit pas lui-même un objectif médical et ne crée pas non plus d'informations en lui-même à des fins médicales. L'évaluation clinique du logiciel de DM ne doit pas être réalisée de manière indépendante, mais doit être réalisée avec la pompe à insuline pilotée.

La démonstration des performances cliniques et analytiques est un élément essentiel dans la validation des preuves cliniques du logiciel. En effet, dans le cas des logiciels d'aide à la décision clinique, les répercussions pour la santé du patient peuvent être importantes voire fatales. Prenons l'exemple du logiciel de calcul de dose d'insuline intégré au glucomètre ; le manque d'exactitude, de précision ou de fiabilité du dispositif peut entraîner, par l'administration d'une dose erronée d'insuline, une hypo ou hyperglycémie pouvant être fatale pour le patient.

Ainsi, différentes sources de données sont possibles afin de démontrer la validité des preuves cliniques (Tableau 8).

Source de données	Exemples
Littérature scientifique pertinente évaluée par des pairs	- Données existantes d'études menées avec le dispositif en question ou un dispositif équivalent
Investigations cliniques / Études de performance clinique	- Études prospectives ou rétrospectives - Données existantes du fabricant - Données provenant de dispositifs équivalents - Données provenant de bases de données/registres/bases de données de référence - Données provenant de l'extérieur de l'UE avec justification de l'applicabilité
Expérience publiée acquise par les tests de diagnostic de routine	- Données sur les performances dans le monde réel - Données obtenues après post-market performance follow-up (PMPF)

Tableau 8 : Les différentes sources possibles pour la validation des preuves cliniques et exemples associés

1.3.4. Démonstration de la conformité du système qualité

L'IVDR exige que le fabricant mette en œuvre un SMQ pour certains types de DMDIV. (20)
Les principes de SMQ se retrouvent dans la norme ISO 9000, pour de nombreux secteurs industriels. Elle constitue la base des bonnes pratiques pour maintenir et contrôler la qualité des produits.

Dans le domaine des dispositifs médicaux, c'est la norme EN ISO 13483 (Dispositifs médicaux – Systèmes de management de la qualité – Exigences à des fins réglementaires) qui prévoit les exigences pour le SMQ des organismes impliqués dans le cycle de vie d'un dispositif médical. Il s'agit d'une norme internationale qui a été harmonisée par l'UE et publiée au JOUE. Ainsi, conformément à l'article 8 de l'IVDR, sa mise en œuvre confère aux fabricants de dispositifs médicaux une présomption de conformité aux exigences règlementaires applicables aux DMDIV relevant de cette norme. (24)

En outre, le forum international des organismes de réglementation des dispositifs médicaux[6] (IMDRF) a mis en évidence, dans un document nommé Software as a Medical Device

[6] L'IMDRF est un groupe formé d'organismes de réglementations des dispositifs médicaux du monde entier qui se réunissent volontairement dans le but d'accélérer la convergence réglementaire internationale en matière de DM afin de promouvoir un modèle réglementaire efficace et efficient pour les DM, qui réponde aux nouveaux défis tout en protégeant et en maximisant la santé et la sécurité publique.

(SaMD) : Application of Quality Management System, les éléments de bonnes pratiques en matière de qualité et d'ingénierie des logiciels de DM. (25)

1.3.5. Le marquage CE

L'étape finale avant la mise sur le marché du logiciel de DMDIV sera le marquage CE. Il sera la preuve fournie par le fabricant selon laquelle son produit répond aux exigences légales du règlement européen et peut être ainsi commercialisé sur le marché dans l'UE. Sans ce marquage, le produit ne pourra pas être commercialisé sur le territoire européen.
Ce marquage CE s'applique dans tout l'espace européen, c'est-à-dire dans tous les pays membres de l'UE ainsi qu'en Islande, Norvège, Liechtenstein, en Suisse et Turquie.

Cependant, contrairement à leur mise sur le marché très bien encadrée d'un point de vue réglementaire, ces logiciels, de par leur connectivité importante, se retrouvent particulièrement exposés aux menaces informatiques. Il est donc nécessaire d'intégrer la notion de cybersécurité au développement de ces produits.

PARTIE II : CYBERSÉCURITÉ DES LOGICIELS DE DMDIV

La cybersécurité ne s'applique pas uniquement aux domaines de la défense ou de l'industrie : elle concerne également la santé et notamment les dispositifs médicaux. En effet, les DM étant maintenant souvent capables de communiquer via un réseau sans fil (wifi, radiofréquence, bluetooth…), cela les rend alors plus accessibles à une intrusion externe malveillante, ce qui nécessite une attention plus sérieuse en matière de sécurité et de confidentialité.

Il en va de même pour les logiciels de DMDIV qui peuvent être directement connectés sans fil à un DM matériel ou à des dispositifs de gestion des données.

Les menaces qui pèsent sur le flux précis d'informations et de commandes peuvent compromettre le fonctionnement sûr des logiciels et mettre en danger la santé des utilisateurs. Il peut s'agir de systèmes corporels portables ou implantables qui surveillent et transmettent les données d'une personne et les envoient à un concentrateur (tel qu'un contrôleur/moniteur portatif, un autre dispositif, un smartphone, une tablette ou le cloud) pour analyse, présentation, agrégation avec d'autres flux de données et stockage. Ces logiciels peuvent également recevoir des données ou des commandes à transmettre au patient. Il peut aussi s'agir de logiciels influençant l'utilisation de dispositifs non portables pour le diagnostic (par exemple, des équipements d'imagerie IRM et des moniteurs de soins intensifs) ou pour le traitement (par exemple, des pompes à perfusion, des ventilateurs et des lasers médicaux situés dans des établissements de santé). (26)

Les conséquences d'une cyberattaque contre un logiciel de DMDIV sont donc loin d'être négligeables car elles peuvent concerner la santé immédiate du patient, sa vie privée ou encore engendrer un suivi médical inapproprié.

Actuellement, la priorité en matière de sécurité concerne en premier lieu les données de santé personnelles, alors que la règlementation concernant la protection des logiciels de DMDIV eux-mêmes évolue peu, et, que de nouveaux risques apparaissent. (27)

Il est donc important d'inclure la cybersécurité dans le développement et le cycle de vie de tout logiciel de DMDIV et d'y associer une mesure des risques adaptée à cette problématique. Ainsi, après avoir brièvement défini ce qu'est le Règlement général sur la protection des données (RGPD), nous nous attarderons sur les problèmes de cyber-attaques que rencontrent

les logiciels de DMDIV. Puis, en réponse à cette problématique, nous introduirons le concept de cybersécurité en proposant son intégration au sein du cycle de vie des logiciels de DMDIV dans la dernière partie.

2.1. Confidentialité et protection des données (RGPD)

La confidentialité des données dans le sens « protection de la vie privée » doit être au centre des préoccupations des fabricants de DM. Plusieurs référentiels traitent de la protection de la confidentialité des données. Le fabricant pourra notamment se référer au Référentiel Général de Sécurité (RGS), qui est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Ce référentiel comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité ». À titre d'exemple, il est indiqué que « tout dispositif connecté doit embarquer un dispositif de chiffrement des données afin de garantir la confidentialité des données médicales personnelles lors de leur stockage ou de leur transfert. »

Le RGPD de l'Union Européenne est entré en vigueur le 24 mai 2016 et en application le 25 mai 2018 dans le but de donner aux individus un meilleur contrôle sur les données qu'ils fournissent aux organisations en tant que personnes concernées. Il définit ce que sont les données à caractère personnel et impose les dispositions pour leur protection. Les organisations du monde entier peuvent être amenées à suivre le RGPD si elles fournissent des services aux personnes concernées au sein de l'UE.

La confidentialité et la protection des données dans le sens de protection de la vie privée étant déjà largement encadrées par le RGPD, cette problématique ne sera pas développée dans cette thèse. Par contre, la notion de confidentialité, dans le sens de protection des données en lecture contre une divulgation non autorisée et de protection des accès à des éléments techniques, sera développée dans la suite de cette partie. (4)

2.2. Cyber-attaques

La première décennie du 21ème siècle a entraîné des changements importants dans le paysage des DM. Leur connectivité toujours plus grande composée ou commandée par logiciel a suscité de nombreuses inquiétudes quant aux vulnérabilités liées à la cybercriminalité, qui

n'ont fait que s'accentuer avec l'attaque récente contre le National Health Service (NHS) au Royaume-Uni par « rançongiciel », attaque par un logiciel malveillant qui verrouille les fichiers des utilisateurs et les force à payer une somme d'argent pour en recouvrer l'usage.
Concernant l'estimation de la probabilité d'une cyber-attaque, l'approche recommandée dans la norme ISO 14971 consiste à utiliser le résultat le plus défavorable possible, indiquant que les scénarios les plus défavorables déterminent le niveau de cyber-protection du dispositif. Pour évaluer la gravité de l'impact sur la santé, la FDA suggère l'approche basée sur des niveaux de gravité qualitatifs, tels que décrits dans la norme ISO 14971. (28)

2.2.1. Définition et types de cyber-attaques

D'après le gouvernement, une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes. Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage. (29) Le plus souvent, sont qualifiés de « malwares », les programmes malveillants utilisés pour violer un réseau (logiciels espions, de rançon ou encore les virus). Ils sont introduits par des accès non autorisé aux systèmes informatiques.

2.2.1.1. Cybercriminalité

Des attaques peuvent cibler les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants à des sites marchands, etc.). Hameçonnage (« *phishing* ») et « rançongiciel » sont des exemples connus d'actes malveillants portant préjudice aux internautes.

- **Attaque par hameçonnage *(« phishing »)***

L'hameçonnage, « phishing » ou filoutage, est une technique malveillante très courante en ligne. L'objectif étant d'opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

- **Attaque par rançongiciel *(« ransomware »)***

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus. L'objectif étant de crypter des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les décrypter. (29)

2.2.1.2. L'atteinte à l'image

Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

- **Attaque par déni de service *(ddos)***

Le déni de service peut porter atteinte à l'image de la victime et constitue une menace pour toute organisation disposant d'un système d'information en ligne.

L'objectif étant de rendre le site, et donc le service attendu, indisponible. Les motivations des attaquants sont diverses, allant des revendications idéologiques à la vengeance, en passant par les extorsions de fonds.

Le cybercriminel peut :

- Exploiter une vulnérabilité logicielle ou matérielle
- Solliciter une ressource particulière du système d'information de la cible, jusqu'à « épuisement ». Cette ressource peut être la bande passante du réseau, la capacité de traitement globale d'une base de données, la puissance de calcul des processeurs, l'espace disque, etc.

Plusieurs indices classiques se manifestent : accroissement de la consommation de la bande passante sans explication légitime ; allongement des files d'attente des serveurs de messagerie ou le retard dans le temps de transit des messages ; des ruptures de communications sur délai de garde ou signalées par message d'erreur ; etc.

Plusieurs méthodes aboutissent à un résultat unique : le dysfonctionnement ou la paralysie complète d'un ou de plusieurs services de la victime.

- **Attaque par « défiguration » *(« defacement »)***

Généralement revendiqué par des hacktivistes, ce type d'attaque peut être réalisé à des fins politiques ou idéologiques, ou à des fins de défi technique (défis entre attaquants). L'objectif étant de modifier l'apparence ou le contenu d'un site, et donc d'altérer l'intégrité des pages.
Le cybercriminel exploite souvent des vulnérabilités connues (défaut de sécurité), mais non corrigées du site. Visible ou bien plus discrète pour le visiteur, l'atteinte réussie du site peut prendre différentes formes : ajouts d'informations sur une page ou remplacement intégral d'une page par une revendication. (29)

2.2.1.3. L'espionnage

Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.

- **Attaque par point d'eau *(watering hole)***

La technique du « point d'eau » consiste à piéger un site en ligne afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant. L'objectif étant d'infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données.

- **Attaque par hameçonnage ciblé *(spearphishing)***

Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée. L'objectif étant d'infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé. (29)

2.2.1.4. Le sabotage

Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique. Le sabotage s'apparente à une « panne organisée », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée –

désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance.
Le sabotage et la destruction de systèmes informatiques peuvent avoir des conséquences dramatiques sur l'économie d'une organisation, sur la vie des personnes, voire sur le bon fonctionnement de la Nation s'ils touchent des secteurs d'activité clés.
Afin d'éviter ce type de menace, l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, met l'accent sur la prévention. (29)

Les logiciels de DMDIV, quant à eux, ne sont soumis qu'à certains types de cyber-attaques.
Les conséquences d'une cyber-attaque contre un logiciel de DMDIV sont loin d'être négligeables. Elles peuvent concerner la santé immédiate du patient, sa vie privée ou encore engendrer un suivi médical inapproprié. Ainsi, la santé du patient peut être mise en danger par une modification des propriétés du logiciel de DMDIV pouvant résulter en un ralentissement, un blocage ou alors une reprogrammation de celui-ci. (27)

2.2.2. Cyber-attaques appliquées aux logiciels de DMDIV

Plus précisément, les logiciels de DMDIV sont principalement soumis à trois types de cyber-attaques (Tableau 9) : (27)

Accès non autorisé	Un accès non autorisé correspond à l'interception du flux de données sans fil entre le dispositif et un capteur ou ordinateur par un individu malveillant qui peut alors les conserver, les modifier, voire les crypter.
Logiciel malveillant (malware)	Un malware est un programme destiné à perturber les fonctionnalités du logiciel de DMDIV, pouvant entraîner une perte de contrôle, un ralentissement, etc.
Attaques par « déni de service »	Ces attaques consistent en une surcharge de requêtes faites au logiciel de DMDIV (demande d'actions à réaliser, tentatives de connexion…), entraînant une interruption du service ayant pour conséquence un ralentissement, un déchargement de la batterie ou un blocage complet du système.

Tableau 9 : Types de cyber-attaques contre les logiciels de DMDIV

Les mesures de sécurité d'un logiciel de DMDIV peuvent donc non seulement concourir à la protection du logiciel en tant que destination d'une attaque, mais aussi en tant que relai ou

point d'entrée d'une intrusion au sein du système d'information de l'établissement de santé qui l'héberge.

- Les attaques ciblant uniquement le logiciel de DMDIV sont destinées à modifier son fonctionnement ou sa disponibilité.
    - Attaques contre la disponibilité du logiciel par les attaques par « déni de service »
    - Attaques contre l'intégrité par accès non autorisé ou introduction de malware
- Les attaques ciblant le logiciel de DMDIV comme point d'entrée ont pour objectif d'altérer le fonctionnement de l'infrastructure.
    - La perturbation de fonctionnement du logiciel à partir du système d'information de santé (SIS) ou de son réseau, et vice versa
    - La capture ou la modification de données échangées entre le logiciel et le SIS. (4)

2.2.3. Exemples de cyber-attaques

Une cyber-attaque peut être à l'origine d'un suivi médical inapproprié. En effet, certains pirates peuvent rendre temporairement indisponibles des équipements de monitorage ou d'imagerie ainsi que les logiciels de prescription, pouvant alors entraîner des erreurs de diagnostic et de traitement. Ainsi, des chercheurs ont montré qu'il est possible de pirater une pompe à insuline jusqu'à une distance de 45 mètres en délivrant une dose inadéquate d'insuline ou en coupant la connexion entre la pompe et l'unité de commande du patient ou bien encore de vider la batterie d'un défibrillateur implantable ou de délivrer un choc inapproprié au patient. (27)

Nous pouvons prendre l'exemple des pompes à perfusion Symbiq de Hospira, aux États-Unis, qui ont fait l'objet d'un rappel en raison d'une faille de sécurité. Celle-ci pouvait permettre à des personnes non autorisées de changer des modalités d'administration des médicaments aux patients via le réseau internet des hôpitaux.

De plus, en 2016, une pompe à perfusion dotée d'une fonction WIFI a été retirée du marché par la société Johnson & Johnson pour cause de vulnérabilité pouvant permettre son piratage. La même année, des failles de sécurité ont été identifiées sur les DM implantables connectés de la société St Jude Medical. L'exploitation des failles pouvait permettre à une personne non autorisée d'accéder à l'appareil et de modifier les commandes du pacemaker en déchargeant rapidement la batterie de l'appareil implanté ou encore en provoquant des chocs inopportuns

qui pourraient entraîner la mort du patient. Une mise à jour logicielle a été ordonnée par la FDA. (4)

Pour l'instant, les réelles cyber-attaques n'ont été lancées que dans le but de récupérer des données fournies ou stockées par un dispositif médical connecté. En effet, ces données sont un moyen pour les hackers de procéder à une demande de rançon. Il leur suffit de crypter les données récupérées et de proposer contre une comme d'argent, la clé de décryptage nécessaire à la restauration des données. Par exemple, aux États-Unis, en 2012, un pirate a attaqué le réseau informatique d'un centre hospitalier et crypté les données de 7.000 patients, exigeant une rançon contre leur décryptage et empêchant momentanément leur prise en charge. Ces vols de données constituent un risque financier pour les établissements mais surtout un risque sanitaire pour les patients. (27)

Cependant, il ne peut être exclu la potentialité qu'un jour ses cyber-attaques soient lancées à l'encontre directe des patients.

2.3. Définition, critères et objectifs de la cybersécurité

D'après la norme ISO 81001-1, publiée en 2021 et portant sur la sécurité, l'efficacité et la sûreté des logiciels de santé et des systèmes de technologie de l'information (TI) de santé, la cybersécurité est définie comme l'état dans lequel les informations et les systèmes sont protégés contre les activités non autorisées, telles que l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction, à un degré tel que les risques connexes pour la confidentialité, l'intégrité et la disponibilité sont maintenus à un niveau acceptable tout au long du cycle de vie.

Au sens large, la cybersécurité peut se définir comme l'état d'un système lui assurant une protection vis-à-vis des intrusions malveillantes. Ces intrusions ont pour but de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées. (27)
Dans le domaine des dispositifs médicaux, la cybersécurité comprendra l'ensemble des mesures techniques ou organisationnelles mise en place pour assurer l'intégrité et la disponibilité d'un dispositif ainsi que la confidentialité des informations contenues ou issues de ce dispositif contre le risque d'attaque dont il pourrait faire l'objet. (4)

Du fait de leur connectivité importante, les logiciels de DMDIV peuvent être considérés comme des systèmes TI. Ainsi, le Federal Information Security Management Act (FISMA) aux États-Unis, a défini trois objectifs de sécurité pour les systèmes d'information. (27)
Ainsi, une bonne cybersécurité des IVD MDSW peut être obtenue en maintenant :

- La **confidentialité** en protégeant ces dispositifs contre toute divulgation non autorisée, en préservant des accès uniquement pour les personnes autorisées,
- L'**intégrité** en protégeant ces produits contre toute modification non autorisée ou contre la destruction des informations,
- La **disponibilité** des données en protégeant ces produits contre toute perte de fonction, en assurant un accès permanent aux informations. (26)

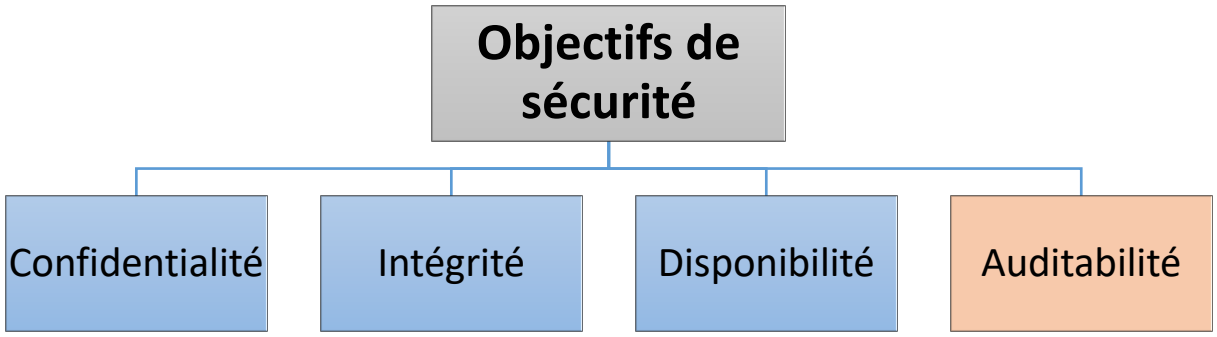

Figure 5 : Objectifs de sécurité appliqués à la cybersécurité

A ces objectifs de sécurité (Figure 5), on peut ajouter différents critères de qualité tels que la sûreté, la sécurité, la fiabilité et la robustesse (Figure 6). (27)

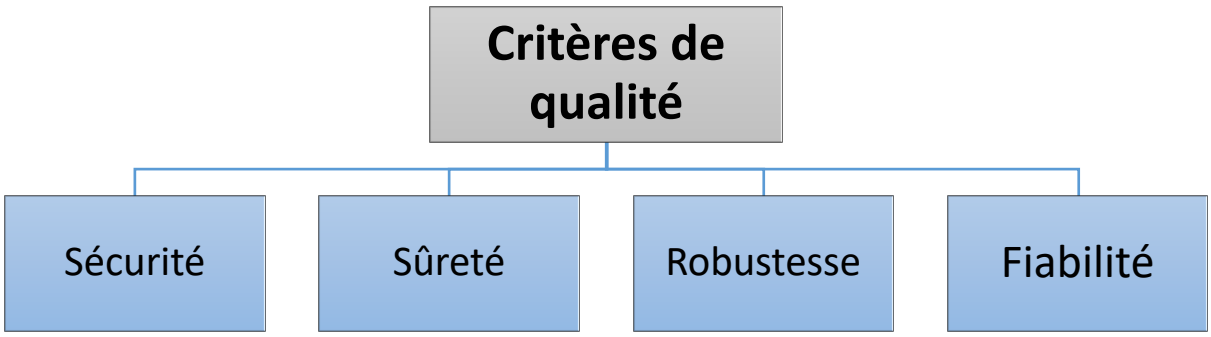

Figure 6 : Critères de qualité appliqués à la cybersécurité

2.3.1. Définition des objectifs de sécurité

Selon le Référentiel Général de Sécurité (RGS), ces critères, disponibilité, intégrité et confidentialité, représentent les objectifs de base à atteindre en matière de sécurité.

La **disponibilité** est la faculté d'un système à rendre un service (par exemple, l'accès à une information ou une ressource) dans des conditions prédéterminées d'exploitation et de maintenance, en respectant des contraintes de performance et de temps de réponse. Les atteintes à la disponibilité d'un système sont généralement qualifiées d'attaques en déni de service. La résilience est la capacité d'un système à continuer de fonctionner (en adoptant, le cas échéant, un fonctionnement en mode dégradé) dans des conditions hostiles, et à revenir à un mode de fonctionnement nominal après un incident.

La **confidentialité** est la propriété d'une information de n'être connue que des personnes, entités ou processus dûment autorisés à le connaître : restriction des accès en lecture.

L'intégrité est la propriété d'un système ou d'une information de ne pas être modifié, altéré ou supprimé de façon illégitime. Lorsque l'intégrité d'une donnée ne peut pas être garantie (par exemple, lors de son transfert sur un canal de transmission non de confiance), il doit être possible de détecter le défaut d'intégrité. (4)

Ces objectifs de sécurité sont complétés par un critère additionnel : l'auditabilité qui correspond à la faculté d'un système à conserver les traces des opérations effectuées sur les biens à protéger (par exemple, les accès ou tentatives d'accès à des informations) et à garantir l'exploitabilité de ces traces à des fins de contrôle ou d'investigation : enregistrement des actions avec leur date dans un fichier journal.

2.3.2. Définition des critères de qualité

Pour aborder la problématique de la sécurisation des logiciels de DMDIV, il est nécessaire de définir en amont deux notions fondamentales qui peuvent se rejoindre : la sûreté et la sécurité (Tableau 9). Souvent confondues, elles se différencient pourtant par la nature des risques contre lesquels lutter. (4)

	SÉCURITÉ	SÛRETÉ
DÉFINITIONS	La sécurité consiste à s'assurer que le logiciel de DMDIV est protégé contre les attaques extérieures pouvant compromettre le fonctionnement du logiciel. Elle fait référence à l'absence de risque inacceptable, indépendamment de l'objet du risque.	La sûreté de fonctionnement d'un logiciel de DMDIV consiste à s'assurer qu'il fonctionne correctement et à prévenir les risques aléatoires et involontaires. Elle prend également en compte les erreurs d'utilisation. Elle correspond à la protection du logiciel par rapport à l'environnement avec lequel il est en contact ou en communication, cela comprend donc les connexions avec internet ou les autres systèmes.
PRÉVENTION	Le fabricant doit appliquer toutes les exigences générales de sécurité et de performance à son logiciel afin d'être conforme à la réglementation européenne et ainsi obtenir le certificat de marquage CE.	L'obtention d'un système sûr de fonctionnement passe par l'utilisation d'une combinaison de méthodes visant à contrer des actions, internes ou externes, pouvant conduire à la survenue d'une défaillance du système.
NATURE DES ERREURS IDENTIFIÉES	La sécurité prend en compte les actions intentionnelles, c'est-à-dire créées dans l'intention de nuire.	La sûreté de fonctionnement s'intéresse majoritairement aux erreurs accidentelles.
EXEMPLES	Le piratage d'un lecteur de glycémie calculateur de dose, avec prise de contrôle à distance de l'affichage numérique peut conduire à l'administration d'un mauvais dosage d'insuline rapide par le patient.	Par exemple, s'assurer qu'un lecteur de glycémie, avec système de planification de dose de médicament à administrer, calcule correctement la dose d'insuline rapide à s'injecter par le patient, avec la précision prévue par le fabricant.
LIEN SÛRETÉ/SÉCURITÉ	Un système peut donc être sûr de fonctionnement parce que la probabilité d'occurrence d'un événement redouté est jugée négligeable ; ce système ne sera pas nécessairement sécurisé, parce qu'un attaquant cherche précisément à déclencher l'événement redouté. (4) Un problème de sûreté peut donc devenir un problème de sécurité quand une attaque prend le contrôle du logiciel de DMDIV et intervient dans la décision clinique finale en rapport avec le patient. (27)	

Tableau 10 : Comparaison sécurité / sûreté : deux critères de qualité fondamentaux en cybersécurité

Les notions de sécurité et de sûreté ne sont évidemment pas antinomiques. Les méthodes préconisées dans le domaine de la sûreté de fonctionnement permettent de satisfaire de nombreuses exigences de sécurité (Figure 7). Néanmoins, il est utile de préciser que quelles que soient les mesures de sûreté et de sécurité mises en place, l'innocuité d'un logiciel de DMDIV sur le plan médical est un prérequis. Ceci doit être vrai tout au long du cycle de vie du logiciel. (4)

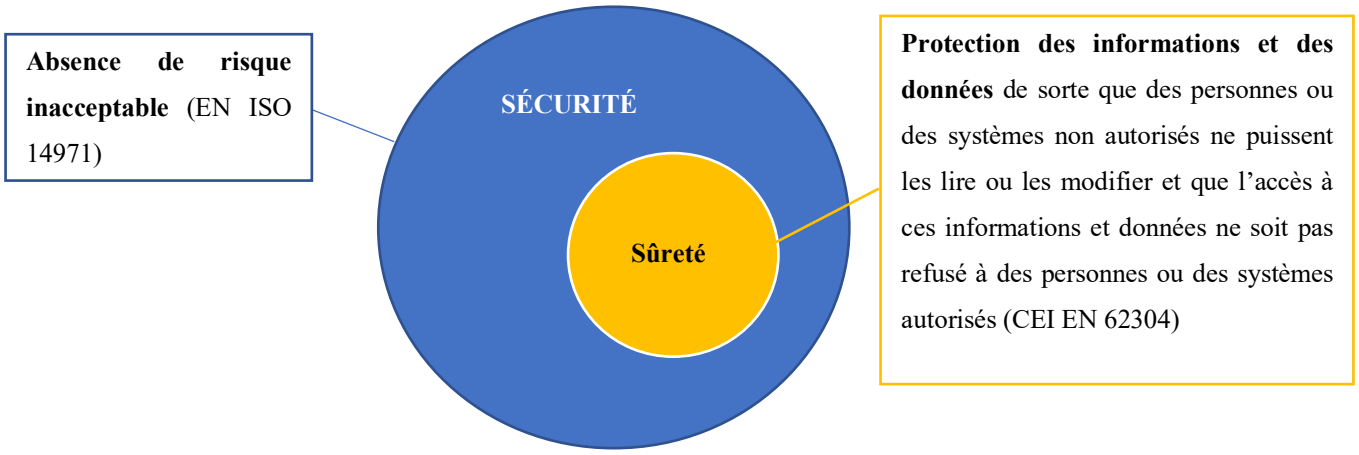

Figure 7 : Schéma explicatif des notions de sécurité et de sûreté

On trouve ensuite le critère de fiabilité, c'est-à-dire la précision des données qui sont rapportées par le logiciel. Une perte de précision pourrait rendre dangereuse l'utilisation du logiciel. Une diminution de la fiabilité d'un logiciel peut correspondre par exemple à une modification des données transmises par un capteur, ce qui rend caduque la décision clinique finale.
Enfin, la robustesse est la capacité d'un DM à fonctionner malgré les anomalies présentes dans son logiciel. (27)

Une violation de données médicales, c'est-à-dire la divulgation d'informations sécurisées ou privées/confidentielles dans un environnement non fiable, peut représenter un risque pour la sécurité, la sûreté voire les deux. (26) Il sera donc important d'inclure, dans le développement des logiciels de DMDIV, un plan de gestion des risques adapté afin d'améliorer leur cybersécurité.

2.4. La cybersécurité au sein du cycle de vie des logiciels de DMDIV

La protection des logiciels de DMDIV contre les menaces cybernétiques en constante évolution nécessite une approche continue du cycle de vie, dans laquelle la cybersécurité est intégrée au cycle de développement du produit, complète et renforce les processus de gestion des risques de sécurité.

Le NIST (National Institut of Standard and Technology) donne aux fabricants les bases de la conception et du développement de la sécurité informatique des dispositifs médicaux au sens large (Figure 8). Il s'agit essentiellement de concevoir un appareil capable :

- D'identifier les attaques et les menaces
- De protéger les systèmes contre les dénis de service
- De détecter les intrusions
- De répondre en cas d'attaque
- De récupérer ses capacités ou les services altérés. (30)

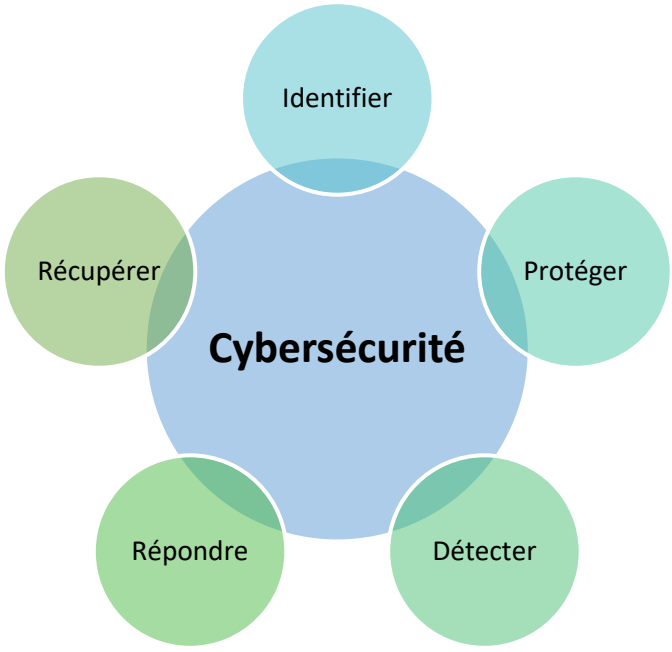

Figure 8 : Cycle des fonctions de base de cybersécurité

Pour mener à bien la définition et les spécifications des fonctions de base, il est indispensable de caractériser les différents constituants du système. Pour cela, il est nécessaire d'effectuer une liste de toutes les composantes, sous composantes et les unités logicielles du système, aussi appelé Software Cybersecurity Bills of Materials (CBOM/SBOM).

Malgré les défis, l'importance d'une évaluation continue de la sécurité tout au long du cycle de vie du logiciel de DMDIV est désormais acceptée. La Figure 9 illustre des activités de sécurité dédiées superposées au cycle de vie de la conception du logiciel. L'évaluation complète des menaces, effectuée après l'étape des exigences, est l'activité la plus fondamentale.

L'utilisation de tests statiques de sécurité des applications (outils SAST), dans le cadre du cycle de vie de la sécurité logicielle, est fortement recommandée par les normes de sécurité logicielle car ils permettent d'appliquer des normes de codage strictes afin de prévenir les défauts. Les arguments en faveur de l'analyse statique sont si forts que la FDA a utilisé CodeSonar de GrammaTech pour analyser des logiciels de dispositifs médicaux afin d'évaluer la qualité du code de source à la suite d'une série de défaillance de pompes à perfusion.

Les outils SAST fournissent un soutien essentiel lors des phases de codage et d'intégration du développement. Assurer la qualité continue du code, tant dans les phases de développement que de maintenance, réduit considérablement les coûts et les risques liés aux problèmes de sécurité et de qualité des logiciels.

Ainsi, ces outils jouent un rôle important dans l'accélération de la mise sur le marché des logiciels de DMDIV. (18)

Une approche de conception axée sur la sécurité consiste à intégrer la sécurité comme une priorité absolue dans le cycle de vie du développement logiciel (Software Development Lifecycle : SDLC), comme le montre la Figure 9 : (18)

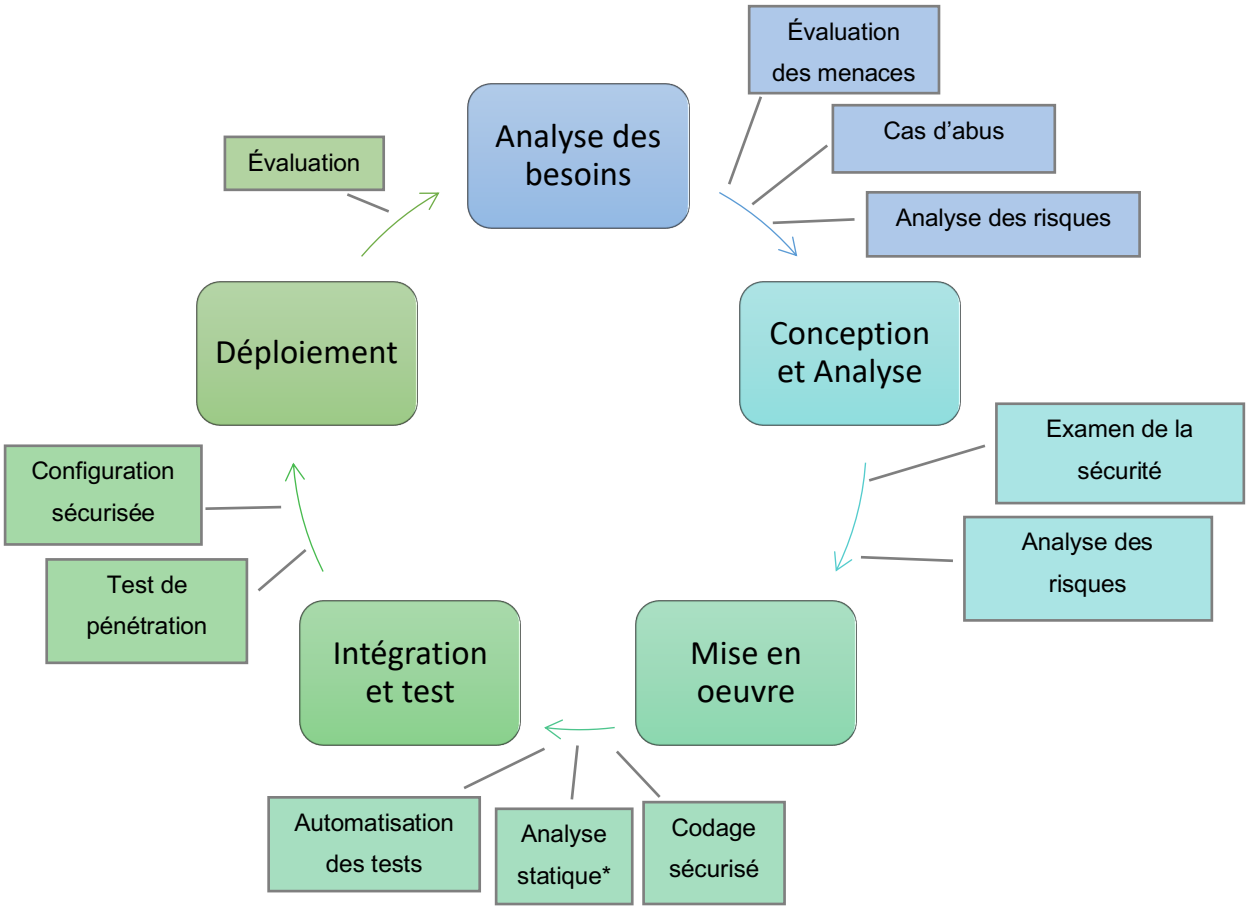

Figure 9 : Processus de sécurité superposées au cycle de vie de la conception logicielle

L'analyse statique consiste à analyser le texte d'un programme pour en extraire de l'information.

Les fabricants de logiciels de DMDIV peuvent s'attendre au moins aux types d'activités suivantes à ces étapes clés :

- Analyse des besoins : Une fois que l'on dispose d'une évaluation de la menace à l'échelle du système, on peut comprendre l'étendue de menace du dispositif. Les exigences spécifiques de sécurité peuvent être introduites, ainsi que les « cas d'abus » connus (cas d'utilisation qu'un attaquant pourrait suivre) et une analyse des risques. Les exigences de sécurité sont introduites et prises en compte. Cette étape est cruciale car c'est le moment où la sécurité devient un objectif connu du projet de développement avec le niveau approprié de gestion des risques, de programmation et de calcul des coûts.
- Conception et Analyse : Au fur et à mesure de la conception du logiciel, les analyses doivent inclure les aspects de sécurité. L'évaluation de la conception du logiciel doit se faire simultanément à l'évaluation des menaces connus et des exigences de sécurité.
- Mise en œuvre (Développement du code) : Au stade de codage, le respect des directives de sécurité et des normes de codage est essentiel. L'utilisation d'outils

d'automatisation tels que l'analyse statique est essentielle pour garantir que les vulnérabilités ne sont pas introduites dans le logiciel. L'automatisation des tests (qui comprennent une analyse de sécurité) est importante à ce stade.

- Intégration et test : Lorsque le système dans son ensemble commence à prendre forme, les tests permettent de déceler les vulnérabilités avant l'intégration et le déploiement sur le marché. Les outils de test de pénétration[7] automatisés peuvent être très utiles à ce stade, pour découvrir des vulnérabilités qui n'ont peut-être pas été prises en compte lors des étapes précédentes du développement. La configuration du produit final en vue de son déploiement est essentielle aux dernières étapes de cette phase. En veillant à ce que le produit prêt à l'emploi soit aussi sûr que possible, on évite bon nombre des problèmes de sécurité que l'on rencontre aujourd'hui dans les appareils connectés.
- Déploiement et maintenance : Lorsqu'un produit entre sur le marché et commence à être largement déployé, les vulnérabilités de sécurité deviennent exponentiellement plus coûteuses à corriger. Un produit conçu selon une approche axée sur la sécurité est moins susceptible de se retrouver avec une faille de sécurité, mais les entreprises doivent être préparées à gérer la sécurité de manière continue. La conception du produit avec la possibilité de mettre à jour le logiciel est essentielle pour résoudre rapidement les nouveaux problèmes. Cependant, à mesure qu'un produit fait l'objet d'une maintenance et d'une révision, la sécurité est une préoccupation constante et les nouvelles vulnérabilités et menaces doivent être réintégrées dans le système selon une approche itérative.

Pour réduire le risque de cybersécurité tout au long des phases de conception et de développement, il existe 2 approches qui permettent de comprendre le risque de cybersécurité le plus tôt possible. En effet, une réflexion en amont permet une conception du produit plus axée sur cet aspect. Le fait de se préoccuper du risque de cyber-attaque seulement à la fin de l'élaboration du produit empêche de mettre réellement en œuvre des mesures appropriées (27). Il s'agit des approches suivantes :

- **Sécurité par la conception** (Security by Design en anglais, SbD) : une évaluation précoce permet d'intégrer des mesures de cybersécurité adaptables dans la conception

[7] Un test d'intrusion, aussi appelé « test de pénétration » ou « pentest » en anglais) est une méthode d'évaluation de la sécurité d'un système d'information ou d'un réseau informatique. Cette méthode consiste généralement à analyser l'infrastructure d'un réseau informatique, afin de simuler l'attaque d'un utilisateur mal intentionné, voire d'un logiciel malveillant (« malware »).

du dispositif, telles que la minimisation de la surface d'attaque potentielle, un code sécurisé, etc.

Le Software Assurance Forum for Excellence in Code (SAFECode) publie des informations concernant le développement de logiciels sécurisés.

- **Qualité par la conception** (Quality by Design en anglais, QbD) : en s'appuyant sur l'approche SbD, la qualité par conception implique de comprendre et d'atténuer les risques potentiels introduits par chaque fonction du DM, son processus de fabrication et l'environnement dans lequel le dispositif est utilisé. Ces risques peuvent inclure la cybersécurité, la confidentialité, la facilité d'utilisation, la sécurité et d'autres risques associés. Si l'augmentation du nombre de fonctions (par exemple, la connectivité Bluetooth) peut améliorer la facilité d'utilisation, la façon dont la fonction est conçue, fabriquée ou utilisée peut également accroître l'exposition du dispositif aux vulnérabilités en matière de cybersécurité. Une plus grande exposition augmente la probabilité qu'une faille de cybersécurité soit exploitée, ce qui entraîne des risques potentiellement inacceptables. L'évaluation précoce permet de trouver un meilleur équilibre entre la fonctionnalité et la cybersécurité. (31)

Dans un deuxième temps, il faudrait appliquer des systèmes de cryptage de transmission des données plus évolués. En effet, les systèmes de cryptage les plus simples, largement utilisés actuellement, peuvent être compromis en quelques secondes. Il est donc recommandé d'utiliser des systèmes de cryptage plus complexes qui offrent une meilleure sécurité. Cette sécurité pourra encore être améliorée par l'utilisation d'un réseau privé virtuel, aussi appelé VPN.

Par exemple, dans le cas d'un DM implantable, l'accès aux données en cas d'urgence peut être problématique si le système de cryptage est trop complexe à désactiver. Prenons l'exemple d'un pacemaker, où l'accès des données de l'activité cardiaque d'un patient peut être très important en cas d'accident. C'est pourquoi des clés de décryptage via les paramètres biométriques (couleur de l'iris, taille du patient, empreintes digitales…) sont à l'étude.

Le processus de conception prend également comme entrées les aspects règlementaires, qui viennent ici cadrer le cycle de vie des produits. C'est pour cette raison qu'il est important d'identifier toutes les spécifications règlementaires et de les croiser aux spécifications techniques. (30)

2.4.1. Identification de la classe de sécurité du logiciel de DMDIV

Comme détaillé dans la première partie de cette thèse, il est important dans un premier temps d'identifier, d'après l'IVDR, la classe réglementaire de son logiciel de DMDIV. De plus, notre dispositif étant un logiciel, il sera aussi important de déterminer la classe de sécurité du logiciel de DMDIV d'après la norme IEC 62304.

Globalement les autorités réglementaires de chaque territoire (États-Unis, Europe, Australie…) utilisent les mêmes règles de classification, chacune avec des spécifications propres à sa région.

Aux États-Unis, une nouvelle classification de risque va être introduite dans la nouvelle version de son guide sur le contenu des soumissions avant commercialisation pour la gestion de la cybersécurité des DM : c'est le « Tier ». Il a été créé pour proportionner les efforts des fabricants en fonction des risques dans le processus de conformité aux exigences règlementaires de cybersécurité. Il classe les appareils et les logiciels en 2 niveaux :

- Le Tier 1 "Higher cybersecurity risk" : ce sont des DM capables de se connecter par réseau filaire, sans fil (Wifi, Bluetooth...) ou internet à d'autres DM ou des systèmes non médicaux. Et donc, un incident de cybersécurité sur le DM peut entraîner un préjudice sur le patient ou son environnement. Par exemple, un défibrillateur cardiaque implantable est considéré par exemple comme un dispositif médical de Tier 1.
- Le Tier 2 "Standard cybersecurity risk" : tous les DM qui ne respectent pas les règles du Tier 1 sont classés comme les DM avec les risques standards. (30)

Cette classification permet de mettre plus ou moins d'accent dans la documentation technique liée à la cybersécurité.

Une fois le logiciel de DMDIV classé, les fabricants peuvent passer à l'identification des exigences de cybersécurité qui sont fortement liées à la classe de risque du dispositif et du Tier.

2.4.2. Exigences générales en matière de cybersécurité

L'identification des exigences règlementaires applicables au produit en matière de cybersécurité devra prendre en compte tous les territoires où il doit être commercialisé.

En Europe, le nouveau Règlement (UE) 2017/746 rappelle que les fabricants doivent développer les logiciels qui garantissent la sécurité de l'information durant tout le cycle de vie du produit. C'est pour cette raison que le Medical Devices Cordination Group (MDCG) a publié le « MDCG 2019-16 : Guidance on Cybersecurity for medical devices » qui reprend, analyse et détaille toutes les exigences/recommandations du règlement.

En 2019, la FDA a mis sur pied 2 guides à vocation d'aider les entreprises dans les activités de conformité : « Content of Premarket Submissions for Management of Cybersecurity in Medical Devices » et « Postmarket Management of Cybersecurity in Medical Devices ». Le premier standard met en évidence les attentes et le contenu du dossier de soumission pour l'approbation de la mise sur le marché. Le second initie et s'inscrit dans un processus d'amélioration continue des activités que prône l'ISO 13485 dans la version de 2016 ; il traite également toutes les activités de la surveillance après commercialisation.

Le laboratoire indépendant UL (Underwriters Laboratoires), compagnie indépendante américaine de consultance et de certification de sécurité des produits, délivre un label qui garantit la conformité d'un produit aux exigences de sécurité et de qualité applicables aux États-Unis et au Canada en vue de sa libre circulation sur les marchés internationaux. Cette certification UL possède un caractère volontaire et représente une garantie pour les consommateurs. Un produit certifié UL signifie que le laboratoire effectue des audits réguliers et continus chez les fabricants et effectue des essais sur des échantillons représentatifs de ces produits afin de vérifier leur conformité aux exigences établies par les normes en vigueur. (32) En outre, ils fournissent en plus aux fabricants les recommandations sur les tests de reproductibilités, ils couvrent les tests de vulnérabilités, les logiciels malveillants et les faiblesses logicielles pour les appareils en réseau. La conformité aux exigences de la norme UL 2900-1 fait la présomption de conformité aux États-Unis.
Toutes ces raisons permettent de prendre les normes de cybersécurité développées par le laboratoire UL comme le squelette sur lequel viendront se greffer les autres standards durant tout le cycle de vie des produits. Ainsi, les normes UL 2900-1 et L-UL2900-2-1 traite respectivement de la cybersécurité des logiciels pour les produits connectables et les exigences particulières pour les composants connectables au réseau des systèmes de santé et de bien-être. (30)

2.4.3. Analyse des risques de sécurité informatique du produit

Dans le processus de gestion des risques des DM au sens large, le norme NF EN ISO 14971:2019 est une référence. Elle spécifie une procédure pour permettre d'identifier les phénomènes et situation dangereuses, d'analyser et évaluer les risques, de maîtriser et surveiller l'efficacité de ces moyens de maîtrise. C'est une norme internationale qui traite tous les risques. Son caractère généraliste va la rendre moins adaptée pour les risques liés à une spécialisation bien spécifique. C'est pour cette raison qu'une multitude de standards ont été développées pour traiter de manière précise des thèmes particuliers, comme la cybersécurité et accompagner la norme ISO 14971 dans cette procédure. Parmi les standards ou les méthodes développés pour traiter les vulnérabilités ou les menaces de cybersécurité, nous avons :

- L'AAMI TIR 57 : Principes de sécurité des dispositifs médicaux – Gestion des risques
- La méthode EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité d'Information) conforme à la norme ISO/IEC 27001 : Management de la sécurité de l'information. Elle permet d'analyser et traiter les menaces sur un produit ou une organisation.
- La CEI 80001-1 : Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux.
- Très récemment, en décembre 2021, une nouvelle norme a vu le jour et traite de la sécurité, de l'efficacité et de la sûreté des logiciels de santé et des systèmes IT de santé. La partie 1 de cette norme ISO 81001-1:2021 fournit les principes, les concepts, les termes et les définitions relatifs aux logiciels de santé et aux systèmes d'information sur la santé, ainsi que les propriétés essentielles de sûreté, d'efficacité et de sécurité, tout au long du cycle de vie. (30)

De plus, afin de fournir des principes généraux et de meilleures pratiques pour faciliter la convergence réglementaire internationale de tous ces standards, l'IMDRF a élaboré un document qui se concentre exclusivement sur la cybersécurité des DM. Ce document, appelé « Principes et pratiques pour la cybersécurité des dispositifs médicaux », a été conçu pour fournir des recommandations concrètes à toutes les parties prenantes en matière de cybersécurité des DM (y compris les DMDIV). Il a été élaboré dans le but de minimiser les risques de cybersécurité qui pourraient découler de l'utilisation du dispositif aux fins prévues et d'assurer le maintien et la continuité de la sécurité et des performances du dispositif. Ce document constitue donc un autre référentiel sur lequel le fabricant peut choisir de s'appuyer

ou non dans le développement de son logiciel de DMDIV. Un des concepts clés de ce document est la mise en place d'une gestion des risques adaptée, afin de réduire au maximum le risque de cybersécurité.

Plus globalement, il sera essentiel pour les fabricants de définir une gestion des risques adaptée au logiciel de DMDIV : en prenant en compte le fait que c'est un dispositif médical et, de surcroît, une technologie de l'information (IT).

2.4.3.1. Gestion des risques en matière de dispositifs médicaux

Comme abordé dans la partie 1 de cette thèse, la gestion des risques appliquée aux DM est définie dans la norme ISO 14971 publiée en janvier 2013 et développée spécifiquement à l'attention des fabricants de DM.
Elle traite des processus de gestion des risques concernant principalement le patient, mais également l'opérateur ou d'autres intervenants, les équipements ainsi que l'environnement d'utilisation. L'analyse de risque est réalisée aux différentes étapes du cycle de vie du DM (Figure 10). (4)

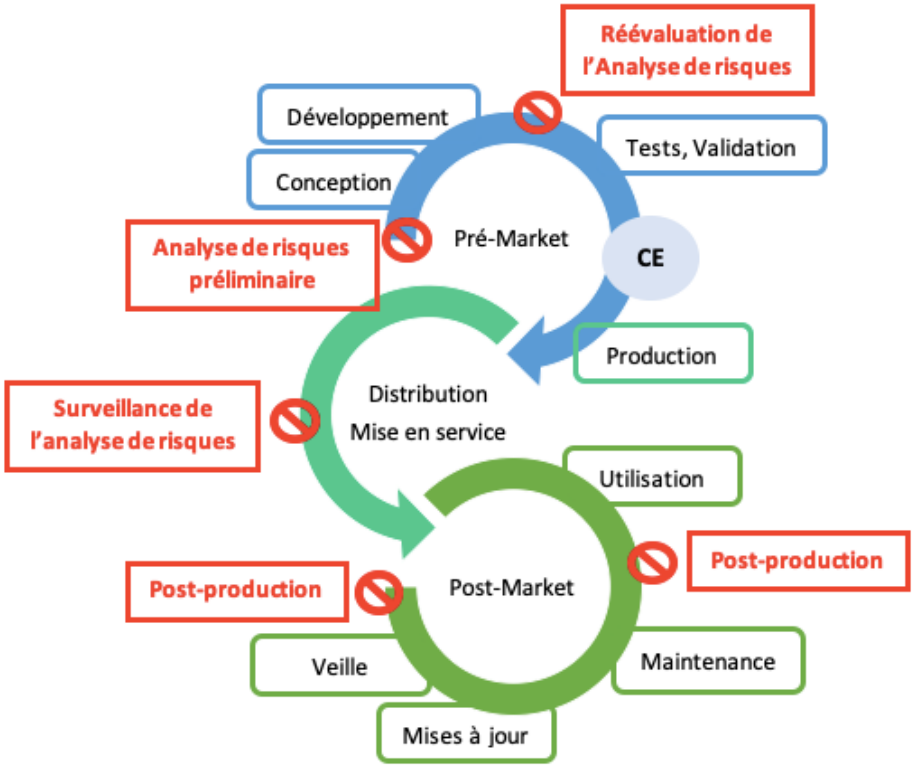

Figure 10 : Analyse de risque au cours du cycle de vie du DM

Selon la norme ISO 14971, les fabricants doivent évaluer, pour un DM donné, dans un contexte d'utilisation défini par le fabricant lui-même, les vulnérabilités qui existent et caractériser l'impact potentiel qui peut en résulter. On parle de vulnérabilité du matériel, du logiciel, de failles dans les procédures et également de problématiques liées à des aspects humains.
Une fois l'événement identifié, ils déterminent le niveau acceptable de risque en définissant le seuil de tolérance au risque.
L'acceptation des risques est évaluée au regard du rapport bénéfice/risque. Un risque est acceptable si :

- Il est maîtrisé autant que possible,
- La réduction du risque n'altère pas le rapport bénéfice/risque global,
- Il présente un rapport bénéfice/risque favorable, et
- Les mesures de surveillance après commercialisation sont planifiées. (4)

Ensuite, ils prévoient les mesures à mettre en place afin de minimiser l'impact potentiel qui en découle. Le déploiement des mesures permet d'assurer la continuité des fonctions à un niveau tolérable. La définition des mesures de réduction du risque est formalisée via l'élaboration d'un plan de gestion des risques et d'un rapport sécurité du logiciel.

- Le plan de Prévention des Risques se construit de la manière suivante :
    - Évaluer les vulnérabilités du logiciel DM tout au long du cycle de vie ;
    - Évaluer les menaces concernant les propriétés Confidentialité/Disponibilité/Intégrité en fonction des vulnérabilités et fonctions critiques évaluées ;
    - Énoncer les exigences de contre-mesures et de sécurité pour toutes les menaces évaluées ;
    - Être en lien avec le Plan de Développement Logiciel et le Plan de Gestion des Risques ;
    - Servir à la réalisation du Rapport de sécurité du Logiciel vérifiant la prise en compte des exigences de sécurité.
- Le rapport de sûreté du logiciel doit :
    - Évaluer les activités liées à la sécurité du logiciel
    - Évaluer la prise en compte des exigences de sécurité émises dans le Plan de Prévention des Menaces
    - Statuer et donner un avis sur la sécurité du logiciel. (4)

Nous allons maintenant nous intéresser à la gestion des risques en matière de technologies de l'information (IT).

2.4.3.2. Gestion des risques en matière de technologies de l'information (IT)

La sécurisation des systèmes d'information (SSI) repose sur un certain nombre de grands principes. Il s'agit d'empêcher l'utilisation non-autorisée, le mésusage, la modification, la copie « silencieuse » ou le détournement du système d'information (Figure 11). (4)

Figure 11 : Grands principes de la SSI

Ces grands principes sont détaillés dans l'Annexe 1.

En France, la protection des systèmes d'information de l'État et la vérification de l'application des mesures dépendent de l'**Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI). L'ANSSI met à disposition un ensemble de guides de bonnes pratiques et de guides de recommandations destinées aux professionnels de la sécurité informatique et au grand public afin de les sensibiliser aux différentes méthodologies de sécurité numérique.

Il existe plusieurs méthodes d'analyse de risque en SSI qui reposent sur l'identification des biens essentiels à protéger. Ces biens sont les éléments qui peuvent, en étant attaqués, avoir des conséquences sur les biens ou les personnes.
La méthode EBIOS est la méthode choisie pour traiter les menaces et risques de sécurité informatique publiée par l'ANSSI (Figure 12). Elle synthétise plusieurs standards. Cette méthode a l'avantage d'être applicable à l'analyse des menaces de cybersécurité qui pèsent sur une organisation ou un produit. (30)

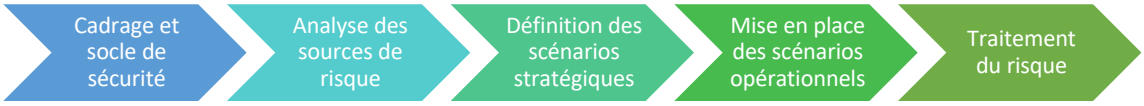

Figure 12 : Différentes étapes de la méthode EBIOS

D'après l'ANSM, les nombreux documents et outils proposés par l'ANSSI peuvent être appliqués aux logiciels de DMDIV. (33) L'ANSSI propose aussi un exemple d'étude des risques réalisée à l'aide de la méthode EBIOS, qui porte à la fois sur la cybersécurité et la protection de la vie privée. (34)

2.4.3.3. Association des deux gestions des risques : convergence des deux mondes

2.4.3.3.1. Principe

Pour appliquer la méthode d'analyse et de gestion du risque des systèmes informatiques aux logiciels de DMDIV, il est nécessaire de trouver un langage commun. En effet, il existe une différence de culture entre le monde du DM et le monde de la sécurité des systèmes d'informatique qu'il faut prendre en compte dans la construction d'une démarche de sécurisation.

- Dans le monde du SSI, le risque est une combinaison d'une menace et des pertes qu'elle peut engendrer. La menace est un scénario envisageable et les pertes sont estimées en termes d'atteinte de besoins essentiels.
- Dans le monde du DM, le fabricant doit apporter les preuves que les risques potentiels liés à l'utilisation du DM sont acceptables au regard du bénéfice apporté au patient.

Pour intégrer les risques liés à la cybersécurité, l'idée est de proposer aux fabricants de réaliser une analyse de risque combinant les 2 approches : analyse de risque en SSI et ISO 14971 (Figure 13). (4)

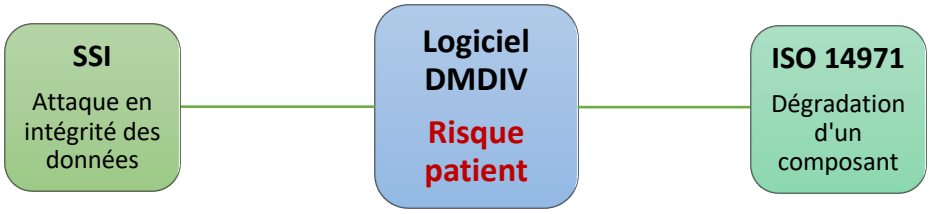

Figure 13 : Combinaison des approches SSI et ISO 14971 pour les logiciels de DMDIV

Il faudra donc concevoir une analyse de risque combinant les deux approches, ce qui consiste à compléter l'analyse de risque « classique » en introduisant les critères de sécurité « cyber » tout au long du cycle de vie du DMDIV. Le but est de décliner les mesures à même de couvrir les menaces identifiées.
Dans son approche, le fabricant devra prendre en compte les différences de risques selon les types de DM concernés et adapter la conception du logiciel de DMDIV en fonction de cela. De même, il devra prendre en compte les spécificités liées à la topologie, l'environnement d'utilisation du logiciel de DMDIV.

Les systèmes étant de plus en plus interconnectés, il apparaît limitant de réaliser uniquement une analyse de risques système par système. Ce schéma d'évaluation apparaît insuffisant pour les architectures complexes, tel que le réseau informatique d'un hôpital.
Or, lorsque le DM est intégré dans un système d'information hospitalier (SIH), il peut être le vecteur de propagation d'une menace. Il faudrait alors suggérer une analyse de risque sur un système complet, ce qui apparaît difficile sachant que l'on ne connaît généralement pas le système informatique global dans lequel le logiciel de DMDIV sera intégré. Il sera donc utile

de proposer au fabricant d'évaluer le risque de propagation des menaces dans le système en cas d'attaque et de le rendre robuste face à une défaillance. (4)

2.4.3.3.2. Méthodologie

La satisfaction des exigences de sécurité s'inscrit dans le cadre général d'un système de management de la qualité « classique » (NF ISO 13483:2016) auquel s'ajoutent les éléments suivants :

1. Identifier les actifs et les biens à protéger, c'est-à-dire établir la liste des biens critiques à protéger et définir les objectifs de sécurité à atteindre sur ces biens.
    i. Dans le cas d'un logiciel de DMDIV en tant que cible de l'attaque, ce sont ceux qui, s'ils sont attaqués, peuvent avoir un impact négatif sur la prise en charge du patient.
    ii. Dans le cas d'un logiciel de DMDIV comme point d'entrée, ce sont ceux qui vont conduire à altérer le fonctionnement de l'infrastructure.

Les biens à protéger sont, *a minima* :

- Le firmware : programme intégré dans un matériel informatique pour qu'il puisse fonctionner
- Le paramétrage médical : par exemple, au niveau du processus de pilotage du capteur à injection, il s'agit de la loi qui mesure la quantité à injecter/calculateur de débit etc.
- Les clés cryptographiques
- Le journal d'évènement/les logs
- Les données relatives aux patients

2. Définir un objectif de sécurité pour chacun des biens en termes d'intégrité, confidentialité, disponibilité et traçabilité et les fonctions de sécurité à implémenter pour atteindre cet objectif de sécurité.

Une fois les biens critiques identifiés, le fabricant doit définir les vulnérabilités potentielles, les dangers et les risques associés (analyse d'impact sur les critères prioritaires). Cette étape permet d'avoir une vision globale de l'ensemble des protections à mettre en place. (4)

La démarche se déroulera de la manière décrite dans la Figure 14.

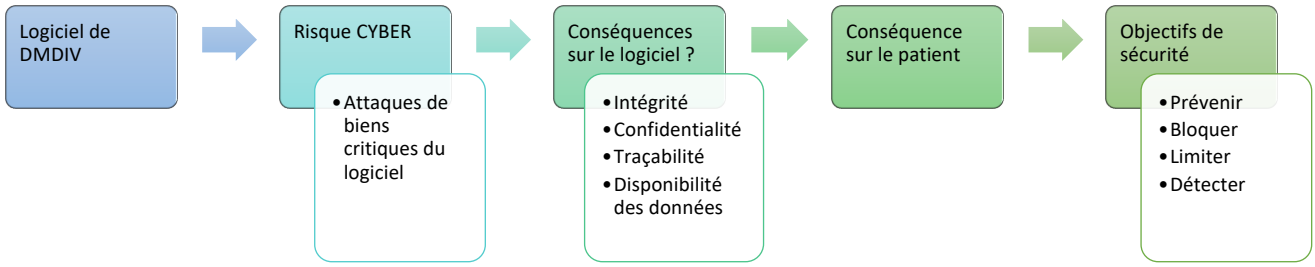

Figure 14 : Démarche à suivre pour avoir une vision globale des risques CYBER sur un logiciel de DMDIV

2.4.4. Mise en place des exigences réglementaires et rédaction de la documentation associée

L'ensemble des enregistrements rédigés dans la documentation associée sont :

- L'analyse des risques de sécurité informatique
- La classification du logiciel de DMDIV en fonction des risques de cybersécurité
- La Software/Cybersecurity Bills of Materials (CBOM/SBOM)
- Les spécifications techniques (Design Secure) basées sur l'analyse des risques
- Les plans de test avec les laboratoires externes
- L'enregistrement de l'organisme au sein de l'ISAO (Information Sharing and Analysis Organizations)

L'ISAO Standards Organisation est une organisation non gouvernementale créée en 2015. Sa mission est d'améliorer la posture de cybersécurité en identifiant des normes et des lignes directrices pour un partage robuste et efficace des informations liées aux risques, aux incidents et aux meilleures pratiques en matière de cybersécurité. Elle a été mise en place par les États-Unis et permet aux fabricants de DM de s'aider mutuellement entre eux en partageant chacun les vulnérabilités et les solutions entreprises pour pallier à ces attaques.

- La surveillance

C'est l'insertion dans le processus de surveillance après commercialisation, d'une procédure de gestion des vulnérabilités et des menaces qui permet d'analyser, d'évaluer et, si nécessaire, de déterminer des mesures de contrôle des risques ou de compensation pour les vulnérabilités identifiées, sur la base du système de surveillance établi dans le SMQ (Système de Management de la Qualité de l'entreprise).

- Le plan périodique sur les activités de cybersécurité

L’entreprise doit rédiger un rapport périodique sur les événements de cybersécurité à l’origine d’un changement (tous les 3 ans) et le fournir aux autorités compétentes, en mentionnant la description de la vulnérabilité ou de la menace à l’origine du changement y compris la manière dont l’entreprise a pris connaissance de la vulnérabilité. Le rapport contient aussi un résumé des conclusions de l’évaluation des risques de l’entreprise, la description de(s) modifications apportées et la justification de(s) changements.

Nous venons de voir la nécessité d’inclure la notion de cybersécurité tout au long du développement des logiciels de DMDIV. Nous allons à présent regrouper tous ces éléments dans une discussion afin de soulever des perspectives intéressantes sur le sujet.

PARTIE III : DISCUSSION ET PERSPECTIVES

3.1. Discussion

Tout au long de ce travail, nous avons pu apprécier l'importance de l'intégration de la cybersécurité au développement des logiciels de DMDIV d'aide à la décision clinique, face à la problématique de leur sécurité informatique .

Les avantages de la cybersanté, toute activité dans laquelle un moyen électronique est utilisé pour fournir des informations, des ressources et des services d'ordre sanitaire (35), sont nombreux comme le montre l'exemple ici des logiciels de DMDIV d'aide à la décision clinique. D'abord, la cybersanté permet un meilleur accès aux informations requises pour améliorer les services de santé et les soins des patients. Ensuite, ces options novatrices en matière de soins de santé permettent à chacun de suivre en continu ses données personnelles pour ainsi devenir acteur de sa santé, en relation ou non avec un professionnel, comme nous l'illustre bien l'exemple des logiciels qui permettent de calculer la dose d'insuline que le patient doit s'injecter en fonction des données de sa glycémie journalière.
De plus, ces technologies de l'information constituent une aide précieuse aux professionnels de santé qui peuvent à présent s'appuyer sur ces logiciels à des fins d'aide à la décision clinique. C'est le cas, par exemple, pour les logiciels permettant d'évaluer le niveau de fibrose hépatique du patient, ce qui permettra une estimation précise du stade de la fibrose et ainsi constituera une aide à la prise de décision clinique et thérapeutique du patient. Un autre exemple, illustrant parfaitement cet atout des logiciels de diagnostic *in vitro* d'aide à la décision clinique, est les dispositifs de dépistage utilisés pour détecter la présence ou la prédisposition à la trisomie 21 fœtale. Ces logiciels permettent de fournir aux cliniciens un score de facteur de risque pour la probabilité que le fœtus présente des mutations génétiques et, ainsi, aider à la décision clinique finale.

Cependant, cette tendance à l'amélioration de la communication et de la connectivité, tout en créant un potentiel d'avantages énormes pour la santé, a également créé la possibilité de résultats négatifs. Il s'agit notamment de la perte de la vie privée, du vol d'identité et d'informations, et de problèmes de sécurité majeurs pour le patient. (26) Ainsi, la potentialité de cyberattaques des logiciels de DMDIV est un sujet particulièrement important, qui

engendre un risque majeur pour les établissements de santé, les professionnels de santé et les patients utilisateurs de ces dispositifs. Ces risques sont d'autant plus graves dans le secteur de la santé, qu'ils ont un impact direct sur la vie des patients. Selon la HAS, « un logiciel qui va être utilisé par un praticien, dont la fonction est basée sur les données algorithmes ayant pour objectif un diagnostic ou le choix d'un traitement thérapeutique aura un impact plus important qu'un logiciel de dispensation pharmaceutique, par exemple ». Cet argument montre que, par la dangerosité possible de ces produits envers les patients, ils devraient être parfaitement évalués. (36) En effet, les risques étant portés sur les fonctionnalités de ces dispositifs à partager des informations à travers des liaisons sans fil (Bluetooth, wifi…) ou par connexion physique à un réseau internet, ces risques concernent principalement l'échange de données (imagerie médicale, résultats de biologie), le pilotage du dispositif (programmation de pompes à perfusion ou de dispositifs implantables actifs), le suivi du patient à distance (surveillance de signes vitaux) ou la maintenance des produits.
Cette question n'est pas nouvelle, mais elle commence à prendre néanmoins de l'ampleur tant la préoccupation est grandissante sur la sécurité de ces produits. Aux États-Unis, l'un des principaux acteurs du secteur des DM sur le marché américain a été au centre d'une polémique sur la potentielle vulnérabilité aux cyberattaques de ces pacemakers et défibrillateurs implantables. (37)

Face à ces risques, il est donc indispensable de préciser quel est l'encadrement juridique qui permet de protéger la sécurité des logiciels de DMDIV. Comme nous l'avons vu tout le long de cette thèse, ces dispositifs sont soumis à un corps de règles qui nécessite pour le fabricant la mise en œuvre de textes complexes. La question pour le fabricant de logiciels de DMDIV est de mettre en œuvre le dispositif le plus sécurisé pour limiter les conséquences de toute attaque malveillante. (37)

En effet, les logiciels de santé qualifiés de DMDIV sont soumis à la fois au nouveau Règlement (UE) 2017/746, l'IVDR, et au nouveau règlement sur la protection des données (RGPD). Ces textes visent à assurer la confidentialité, l'intégrité et la disponibilité des informations contenues ou issues d'un DM connecté ou d'un logiciel. Ils visent à assurer la protection contre les attaques intentionnelles et malveillantes. Mais, il conviendrait d'ajouter à ces textes la notion de manipulation non intentionnelle, de mésusage ou d'erreur d'utilisation, *a fortiori* lorsque ces logiciels de DMDIV sont utilisés ou « mis à disposition » de personnes

fragiles, de personnes âgées, dépendantes, malades, ou encore présentant des altérations de leurs facultés de discernement.

En outre, en Europe, l'IVDR ne couvre pas toutes les problématiques transversales liées à la cybersécurité, et les fabricants ne disposent que d'un guide de référence élaboré par le MDCG (MDCG 2019-16) portant sur la cybersécurité des DM. (37)

Au niveau français, l'ANSM s'est saisie de cette question, et a mis en place en 2019 un Comité (CSST) composé d'experts externes, choisis en raison de leurs compétences et expériences diverses sur le sujet de l'informatique et de la cybersécurité. Ce comité est chargé de proposer au directeur général de l'ANSM, des recommandations à l'attention des fabricants de logiciels de DM et DMDIV de manière à ce qu'ils puissent prendre les mesures nécessaires pour prévenir toute attaque malveillante à l'encontre des dispositifs qu'ils commercialisent et ainsi empêcher la compromission des données et l'utilisation détournée de ces logiciels de DM. (37) Ainsi, l'ANSM a rédigé un projet de recommandations à destination des fabricants de DM intégrant du logiciel pour que la cybersécurité soit prise en compte lors du développement des produits et ainsi réduire au maximum le risque d'attaque informatique. Ce projet reprend les mesures nécessaires pour prévenir toute attaque malveillante à l'encontre de leurs DM et ainsi empêcher la compromission des données et l'utilisation détournée des DM qu'ils mettent sur le marché. C'est la première fois, en Europe, que des recommandations dans ce domaine sont élaborées et l'ANSM a partagé ses travaux avec la Commission Européenne afin que la réglementation évolue pour l'intégrer. (6) Actuellement, en l'absence de réglementation spécifique aux technologies numériques en santé et à leur cybersécurité, les fabricants de logiciels de DMDIV pratiquent une veille réglementaire internationale, et plus précisément américaine où le sujet a été particulièrement développé ces dernières années, afin d'inclure un maximum de notions dans leur analyse de risque.

De plus, la plupart des orientations en matière de cybersécurité des dispositifs médicaux au sens large sont récentes et évolueront au fur et à mesure que la nature des cyber-attaques évolue et que les propriétés émergentes, c'est-à-dire les « vulnérabilités », des DM existants et nouveaux seront connues. Les différentes parties prenantes reconnaissent désormais que la mise en place de la cybersécurité doit être un effort de collaboration tout au long du cycle de développement du produit. Auparavant, la gestion des risques liés aux DM était axée sur la sécurité fonctionnelle, les risques liés à la sécurité (à l'exclusion de la cybersécurité) ou la

protection des données. Aujourd'hui, de multiples approches abordent activement les risques liés au cycle de vie et les dommages potentiels des incidents de cybersécurité. (28)

Cette problématique du renforcement de la sécurité ne touche pas seulement les fabricants, mais elle concerne tous les professionnels de santé, et établissements qui sont utilisateurs de ces DM connectés et logiciels : ils doivent, dans leurs pratiques au quotidien, intégrer les mesures de sécurité nécessairement adaptés aux profils des usagers et patients, afin de ne pas ouvrir les portes aux piratages informatiques. Cela devrait très rapidement induire des actions coordonnées entre tous les acteurs, de formation, information, élaboration de procédures, protocoles, contrôles, dans un encadrement juridique, réglementaire et contractuel sécurisé. (37)

Tout comme la gestion globale des risques du dispositif, la gestion des risques de cybersécurité est un processus vivant, itératif et en constante évolution. Elle doit également s'appuyer sur les composantes essentielles suivantes :

- La cybersécurité évolue avec le temps dans un environnement qui lui aussi change rapidement. L'évolution des technologies et des opportunités et menaces associées, doit être constamment surveillée, anticipée et prise en compte par tous les acteurs.
- Elle est en interface avec un grand nombre de processus du SMQ : post-market surveillance, vigilance, gestion des changements, maîtrise des risques, etc. La bonne définition et mise en œuvre des interfaces avec ces processus est décisive pour établir une maîtrise des risques de cybersécurité efficace dans le temps. (38)

Par exemple, la FDA réinvente son approche et adapte ses processus, notamment concernant les logiciels médicaux, car, selon elle, son approche traditionnelle concernant les DM à risque modéré et élevé n'est pas bien adaptée à la conception, au développement plus rapide et au type de validation utilisé pour les logiciels. Elle concentre sa surveillance sur les applications médicales mobiles présentant un risque plus élevé pour les patients, a adopté un schéma de classification des risques, et des principes de gestion de la qualité adaptés aux logiciels, et plus récemment, la rédaction d'un guide sur l'application de l'évaluation clinique pour les logiciels qui sont des dispositifs médicaux. (39)

Ainsi, chaque acteur est responsable de la sécurité des logiciels de DMDIV et cela commence par le recensement des différents cas de réactovigilance, relatif à la surveillance des incidents et risques d'incidents résultant de l'utilisation d'un DMDIV (40). En effet, pour apprécier la

fréquence et la gravité des incidents, il est nécessaire d'avoir une remontée des informations. Nous pouvons prendre l'exemple de la base de données MAUDE (Manufacturer and User Facility Device Experience) de la Food and Drug Administration (FDA) aux États-Unis, qui permet un accès libre aux différents cas de matériovigilance[8] et réactovigilance recensés, relative à la surveillance des incidents et risques d'incidents des dispositifs médicaux en général. Il est donc nécessaire d'être attentif aux cas de matériovigilance liés à la cybersécurité qui peuvent plus facilement passer inaperçus et de les signaler. (27)

3.2. Perspectives

C'est lors de mon stage de fin d'étude au sein de la société HalioDx, entreprise spécialisée dans le diagnostic immuno-oncologique, que cette problématique de thèse m'est apparue. Dans un monde où la digitalisation est de plus en plus présente, il est indéniable, de mon point de vue, que la santé numérique constitue une des évolutions majeures des systèmes de soins. Comme en témoigne la stratégie « Ma santé 2022 », présenté par le Président de la République en 2018, qui vise à renforcer considérablement le poids de la e-santé dans l'organisation des soins. (41)

L'évolution de l'évaluation de ces produits doit passer par des réflexions considérant toutes les spécificités inhérentes à cette nouvelle technologie en termes de produit, de développement, de preuve clinique et de transposabilité en vie réelle. (36)

Ainsi, à l'échelle européenne, une première proposition serait de créer une agence européenne de cybersanté autonome, indépendante de l'administration gouvernementale, tout en permettant son influence et sa surveillance. Cette dernière serait donc organisée et dirigée par des experts médicaux, industriels, universitaires et autres experts indépendants, mais sans contrôle centralisé de l'un de ces groupes. Cette agence adopterait une politique d'amélioration continue, reconnaissant le fait que les recommandations en matière de cybersécurité sont en constante évolution et sont directement liées à l'innovation dans le domaine de la e-santé. La création d'un tel organisme contribuerait grandement à établir et à conforter la confiance des consommateurs et des utilisateurs finaux, à limiter les cyberattaques, et à favoriser l'innovation sans crainte. De par la complexité et l'évolution

[8] La matériovigilance a pour objet la surveillance des incidents et risques d'incidents résultant de l'utilisation des DM mis sur le marché afin de prendre les mesures préventives ou correctives appropriées.

constante du sujet, il apparait difficile pour une agence comme l'ANSM de traiter des différentes problématiques de la cybersanté.
Dans cette optique, il pourrait être envisagé de faire évoluer les règlements européens actuels (MDR et IVDR), afin d'intégrer une partie spécifique adapté au développement des dispositifs médicaux logiciels et systèmes IT de santé. Un des sujets principaux de ce règlement pourrait être la gestion des risques de tels produits, en insistant sur le processus de *Cybersecurity by Design*, qui est primordial à leur développement. En conséquence, les fabricants devront construire un processus de *Cybersecurity By Design* efficace et adapté à leur organisation, ainsi qu'aux produits qu'ils commercialisent. (38) Ceci pourrait être fait à l'image de la FDA qui a ainsi adopté un schéma de classification des risques pour les patients et des principes de gestion de la qualité adaptés aux logiciels et plus récemment la rédaction d'un guide sur l'évaluation clinique des logiciels qui sont des DM. En outre, au vu de la complexité du sujet concernant la rapidité de l'évolution de ces nouvelles technologies, il semble important qu'une seule entité soit en charge de la veille et de l'adaptation des réglementations en vigueur.

Afin d'avoir un socle harmonisé pour la vérification et la validation de ses logiciels et système IT de santé, une deuxième proposition pourrait être, à l'échelle internationale, la création d'un organisme de certification indépendant, qui soit consacré à l'élaboration de STC, de normes d'exigences et de programmes d'essais pour la cybersécurité de ces produits. Celui-ci pourrait alors établir une harmonisation internationale entre les différentes réglementations déjà existantes. Bien que l'accent sur l'indépendance de cette organisme de certification soit fort, il est néanmoins indispensable qu'il ait une liaison et une relation forte et efficace avec les gouvernements, permettant des efforts synergiques, tout en maintenant sa valeur en tant qu'organisme indépendant. Il devra s'efforcer de faire preuve d'ouverture et de transparence en divulguant publiquement ses opérations, ses spécifications ainsi que ses méthodes et résultats d'évaluation. Ainsi, les fabricants pourraient recevoir, en gage de conformité à ces normes pour une sécurité significative des systèmes électroniques, un « label de qualité » indépendant. Au même titre que les objectifs du marquage CE sont de garantir la performance revendiquée par le fabricant au sein de l'UE, les objectifs d'une telle certification, seraient de cibler des exigences spécifiques en matière de cybersécurité dans le but d'améliorer la sécurité informatique afin d'optimiser le développement de ces produits et ainsi favoriser l'innovation en santé, à l'échelle mondiale.

Une troisième piste à suivre serait d'intégrer cette dimension aux études cliniques des logiciels de DMDIV. En effet, ce nouvel environnement appelle un modèle d'évaluation différent de celui connu jusqu'à présent. (42) Par exemple, la cybersécurité pourrait être vu comme une performance à part entière dans l'évaluation des performances du dispositif, au même titre que la performance clinique, la performance analytique et la validité scientifique. Il s'agit d'instaurer la confiance auprès de l'ensemble des acteurs de santé, impliqués directement ou indirectement, par l'usage de la solution numérique.

Enfin, les patients sont de plus en plus mobiles, informés et connectés et l'utilisation de ces objets/applications connectés s'accélère, conférant au pharmacien un nouveau rôle, essentiel, dans le parcours santé du patient, à tous les points clé de la chaîne de soins, depuis la qualification de ces logiciels pour les pharmaciens d'industrie, jusqu'à leur délivrance et leur utilisation, pour les pharmaciens d'officine. Mais, au-delà de son atout de proximité et de la reconnaissance de ses compétences, le pharmacien doit adapter sa pratique et sa formation à ce nouveau contexte de conseil et d'accompagnement d'un usager-patient qui ne compte pas descendre du train à grande vitesse de la révolution digitale. (42) Il pourrait être intéressant de proposer, lors de la formation universitaire des futurs pharmaciens, des cours abordant la notion de cybersanté au sens large.

Le rôle du corps médical sur le sujet est primordial. Il sera nécessaire de faire participer les professionnels de santé à la sensibilisation des patients à la cybersécurité. Par exemple, les informer que certains comportements apparemment anodins peuvent avoir des répercussions sur la cybersécurité. Parmi ceux-ci, le problème des mots de passe. Ils sont souvent très simples, de façon à s'en souvenir facilement, ou partagés sur des fichiers informatiques. Cette situation facilite grandement l'accès aux DM, ou à leur logiciel, par une personne extérieure et éventuellement mal intentionnée. Ainsi, choisir des mots de passe sécurisés et les garder secret diminue déjà grandement les risques d'introduction d'un pirate dans le système. Un autre exemple pertinent serait l'importance de tenir à jour les logiciels utilisés par les dispositifs et également les systèmes d'exploitation des ordinateurs, ceux-ci corrigent en général des failles de sécurité connues. (27)

D'une façon générale, il est important que le corps médical soit mieux sensibilisé aux aspects de cybersécurité, que ce soit par les deux points précédents (mots de passe sécurisés, mises à jour de logiciels), mais aussi dans le choix des DM utilisés. Des organismes accrédités existent pour donner une certification de sécurité, il peut donc être intéressant, lors d'un achat,

de demander si cette certification a été faire. Cela montre que le corps médical est sensibilisé à cet aspect. (27)

Dans un registre autre que celui de la cybersécurité, ces logiciels d'aide à la décision clinique constituent une réelle opportunité pour la médecine de demain. Cependant, il est nécessaire d'associer à cet avantage, la notion de risque clinique d'utilisation qu'ils soulèvent. En effet, tout le monde s'accorde à dire que les logiciels destinés à fournir aux professionnels des informations utilisées pour prendre des décisions à des fins thérapeutiques ou diagnostiques, présentent des niveaux de risques variables, selon leurs fonctionnalités et les algorithmes qui les supportent, et les données sur lesquelles sont fondés leurs algorithmes. Ces dernières années, la littérature scientifique a vu littéralement « exploser » les évaluations associées à ces solutions numériques comme en témoigne, par exemple, l'évaluation exponentielle du nombre de publications académiques en relation avec les évaluations cliniques de ces logiciels. La requête réalisée le 13/11/2021 sur la ressource PubMed via l'expression « clinical evaluation » et « software » l'illustre parfaitement sur ces 20 dernières années : 119 publications rapportées en 2000 vs 294, 438, 713 et 1276 respectivement les années 2005, 2010, 2015 et 2020 (1). Dans son rapport pour le numérique (39), la HAS indique qu'il faut clarifier les objectifs de l'évaluation des produits du numérique afin « de mieux les mobiliser ou de les adapter aux spécificités du numérique » et notamment en « priorisant en particulier les logiciels représentant un risque médical majeur pour les patients. ». Elle ajoute qu'il faut « définir sans délai un cadre pour une évaluation clinique graduée du rapport bénéfice/risque et de l'efficacité des fonctionnalités logicielles d'aide aux décisions diagnostiques ou thérapeutiques. » (36)

Il est donc urgent que les professionnels puissent s'assurer de la qualité clinique des décisions suggérées par les logiciels, surtout pour celles qui sont le plus à risque pour leurs patients. L'échelle des risques pour ces logiciels, en fonction des conséquences qu'ils peuvent entraîner pour les patients, permet de fonder une approche graduée de leur évaluation. Ceux les plus à risque, dont les fonctionnalités sont susceptibles de causer la mort ou une détérioration grave ou irréversible de l'état de santé d'une personne, devraient faire l'objet d'une évaluation robuste au préalable, complémentaire à celle du marquage CE.

En particulier, la possibilité d'une évaluation clinique nationale et graduée de ces logiciels (ou de leurs fonctionnalités diagnostiques ou thérapeutiques dans le cas où ils en auraient d'autres) devrait être envisagée, afin de confirmer leur rapport bénéfice/risque et leur efficacité dans les conditions nationales prévues de leur utilisation. (39)

Pour une institution comme la HAS, la possibilité d'intégrer des arbres de décision issus de recommandations dans les logiciels professionnels (aide au diagnostic, à la décision thérapeutique, à la prise en charge) constitue une opportunité majeure pour assurer l'intégration de ces recommandations dans les pratiques professionnelles. (39)
Ainsi, après avoir fait l'objet d'une expérimentation entre 2014 et 2021, la HAS a publié, le 18 janvier 2022, un référentiel pour les solutions de télésurveillance pour 4 des 5 pathologies visées par le programme d'expérimentation : à savoir, le diabète, l'insuffisance cardiaque chronique, l'insuffisance rénale chronique et l'insuffisance respiratoire chronique. Le 5ème référentiel, relatif à la télésurveillance des patients porteurs de prothèses cardiaques implantables à visée thérapeutique, sera publié ultérieurement. Ces référentiels permettront aux industriels et aux professionnels de santé de se préparer au cadre pérenne en ayant connaissance des exigences – techniques et organisationnelles, retenues par la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS), (43) commission de la HAS qui examine toute question relative à l'évaluation en vue de leur remboursement par l'assurance maladie et au bon usage des DM et des technologies de santé. (44)

Ainsi, avec leur intégration dans les recommandations professionnelles, il est indéniable que ces logiciels d'aide à la décision clinique représente une réelle opportunité dans le système de soins. Cependant, il est nécessaire que tous les acteurs du développement de ces logiciels relèvent le défi d'associer les compétences du domaine informatique, médical et pharmaceutique, afin de développer des systèmes et logiciels sécurisés, fiables et utiles.

Conclusion

La croissance rapide des technologies numériques a fait progresser la médecine et la société, mais a également introduit de nouveaux risques. La compromission de la sécurité des dispositifs médicaux et le risque associé pour les fonctions vitales, la propriété intellectuelle et la vie privée sont des préoccupations émergentes.

Plusieurs projets ont été menés concluant de l'intérêt de cette nouvelle approche de la médecine : prévention accrue, meilleur suivi du patient, meilleure qualité de vie grâce au maintien à domicile, communication facilitée. Cependant, le cadre légal de ces solutions numériques reste complexe, dans l'attente de réglementations plus poussées dans le domaine. (3)

Certains de ces produits, de par leur finalité médicale, entrent dans le champ d'application des règlements DM et DMDIV. La finalité de ces textes est d'améliorer le système d'accès au marché des dispositifs médicaux afin de garantir leur efficacité et leur sécurité. Actuellement, lors de la conception d'un logiciel de DMDIV, un travail de qualification doit être réalisé afin de déterminer si le produit entre dans le champ des règlements DM ou non. Si c'est le cas, la classe du DM ou DMDIV doit alors être définie car elle détermine les exigences essentielles auxquelles devra se conformer le produit de santé. (3)

Néanmoins, on a pu voir que la sécurité des patients peut dépendre de la cybersécurité de ces logiciels de DMDIV d'aide à la décision clinique. En effet, ces logiciels étant de plus en plus reliés à un réseau, ils peuvent être la cible d'attaques extérieures, fréquemment dans le but de récupérer des données personnelles, mais il n'est pas exclu d'avoir à affronter un jour une exploitation des fonctions de celui-ci à l'encontre des patients. (27)

Il parait donc indispensable d'intégrer cette notion de cybersécurité au développement de ces logiciels de DMDIV afin de garantir une protection maximum aux patients et aux utilisateurs. Récemment, de nombreuses guidelines sur le sujet ont vu le jour mais au vue de l'explosion de l'utilisation de ces solutions numériques ces dernières années, il serait intéressant d'envisager la mise en place d'une réglementation spécifique à ces technologies. Cette dernière pourrait avoir un impact favorable sur le développement sécuritaire de ces produits, en permettant par exemple leur intégration dans les recommandations des pratiques

professionnelles, comme ça a été le cas récemment avec l'inclusion des solutions de télésurveillance pour certaines pathologies chroniques par la HAS.

Ainsi, même si la conception est irréprochable d'un point de vue sécuritaire, il faut ensuite une utilisation responsable de la part de tous les acteurs, ce qui inclut le corps médical mais aussi les patients. Il est donc nécessaire d'intégrer cet aspect de cybersécurité dans l'activité quotidienne. Or, actuellement, les mesures prises concernent essentiellement la protection des données personnelles stockées, oubliant le piratage direct des logiciels de DMDIV. Nous devons dorénavant commencer à réfléchir à ce risque qui porte déjà un nom : le *medjacking (medical device hijacking)*. (27)

Reste à souhaiter que les différentes législations aient la capacité de s'adapter à cette nouvelle approche de la santé afin de garantir l'efficacité et la sécurité des produits disponibles sur le marché, de protéger les données personnelles de santé, de favoriser le bon usage de ces nouveaux outils de santé, tout en favorisant le développement rapide des technologies de santé. (3)

Bibliographie

1. Charle-Maachi C, Moreau-Gaudry A, Sainati D, Camus D, Adenot I, Barthelemy C-E, et al. Les solutions numériques en santé, quelles valeurs apportées, quels mécanismes de financement et quelles évaluations ? Therapie. 6 déc 2021;

2. La téléconsultation connaîtra-t-elle le même essor que lors de la 1re vague de la covid-19 ? [Internet]. Maiia. 2020 [cité 19 févr 2022]. Disponible sur: https://news.maiia.com/essor-teleconsultation-vague2-covid/actualites/

3. RIEU S. Applications et objets connectés : statut réglementaire (en France) et impact des nouveaux règlements européens DM/DMDIV. Université Toulouse III Paul Sabatier; 2021.

4. Rapport ANSM Juillet 2019 - Rapport sur la cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie [Internet]. [cité 7 févr 2022]. Disponible sur: http://www.specialitesmedicales.org/offres/doc_inline_src/666/ANSM%2B-%2BCybersecurite_Recommandations-Fr.pdf

5. MDCG 2019-11 : Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 - MDR and Regulation (EU) 2017/746 - IVDR - October 2019 [Internet]. [cité 7 févr 2022]. Disponible sur: https://ec.europa.eu/health/system/files/2020-09/md_mdcg_2019_11_guidance_en_0.pdf

6. ANSM. L'ANSM lance une consultation publique sur un projet de recommandations pour la cybersécurité des dispositifs médicaux - ANSM [Internet]. 2019 [cité 7 févr 2022]. Disponible sur: https://ansm.sante.fr/actualites/lansm-lance-une-consultation-publique-sur-un-projet-de-recommandations-pour-la-cybersecurite-des-dispositifs-medicaux

7. Lobach DF, Kawamoto K, Anstrom KJ, Russell ML, Woods P, Smith D. Development, Deployment and Usability of a Point-of-Care Decision Support System for Chronic Disease Management Using the Recently-Approved HL7 Decision Support Service Standard. MEDINFO 2007. 2007;861-5.

8. Etude des systèmes d'aide à la décision médicale [Internet]. [cité 15 févr 2022]. Disponible sur: https://www.has-sante.fr/upload/docs/application/pdf/2011-01/etude_sadm_etat_des_lieux_1.pdf

9. SNITEM. Dossier de presse - Réglementation Dispositif Médical [Internet]. calameo.com. 2020 [cité 7 févr 2022]. Disponible sur: https://www.calameo.com/snitem/read/0006105420ba3ae2d56be

10. Commission Européenne. Nouveaux règlements [Internet]. Commission Européenne. 2020 [cité 7 févr 2022]. Disponible sur: https://ec.europa.eu/health/medical-devices-sector/new-regulations_fr

11. ANSM. Mise sur le marché des dispositifs médicaux et des dispositifs médicaux de diagnostic in vitro [Internet]. ANSM.fr. 2021 [cité 7 févr 2022]. Disponible sur: https://ansm.sante.fr/page/mise-sur-le-marche-des-dispositifs-medicaux-et-des-dispositifs-medicaux-de-diagnostic-in-vitro

12. JOUE. RÈGLEMENT (UE) 2017/746 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission. 117176. 5 mai 2017;157.

13. ANSM. Logiciels et applications mobiles en santé [Internet]. ANSM.fr. 2021 [cité 7 févr 2022]. Disponible sur: https://ansm.sante.fr/documents/reference/reglementation-relative-aux-dispositifs-medicaux-dm-et-aux-dispositifs-medicaux-de-diagnostic-in-vitro-dmdiv/logiciels-et-applications-mobiles-en-sante

14. Levelut V. Classification des DMDIV sous le Règlement : une refonte complète [Internet]. Nexialist - votre partenaire pour la conformité des dispositifs médicaux. 2017 [cité 7 févr 2022]. Disponible sur: https://nexialist.fr/classification-des-dm-div-sous-le-reglement-une-refonte-complete/

15. Navarro M. Classification des logiciels (de) dispositifs médicaux (A, B, C, D) [Internet]. mauricenavarro.com. 2019 [cité 7 févr 2022]. Disponible sur: https://www.mauricenavarro.com/articles/classification-des-logiciels-de-dispositifs-medicaux-A-B-C/

16. ISO. IEC 62304:2006 : Logiciels de dispositifs médicaux - Processus du cycle de vie du logiciel [Internet]. ISO. 2006 [cité 7 févr 2022]. Disponible sur: https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/03/84/38421.html

17. CVO-Europe LSC. Documentation technique des Dispositifs Médicaux et DM DIV (Europe) - Règlements 2017/745 et 746 [Internet]. CVO-EUROPE. [cité 7 févr 2022]. Disponible sur: https://www.cvo-europe.com/formation-cvo-europe/documentation-technique-dispositifs-medicaux-dm-div-europe-reglements-2017745-746

18. Graham B. Designing Security into Medical Device Software [Internet]. 2016 [cité 7 févr 2022]. Disponible sur: https://blogs.grammatech.com/designing-security-into-medical-device-software

19. Nexialist. La minute règlementaire - Choisir la procédure d'évaluation de la conformité de son DM : no stress ! [Internet]. Nexialist - votre partenaire pour la conformité des dispositifs médicaux. 2020 [cité 15 févr 2022]. Disponible sur: https://nexialist.fr/la-minute-reglementaire-choisir-la-procedure-devaluation-de-la-conformite-de-son-dm-no-stress/

20. GMED - Le marquage CE des dispositifs médicaux de diagnostic in vitro [Internet]. [cité 7 févr 2022]. Disponible sur: https://lne-gmed.com/wp-content/uploads/2020/10/GMED-Guide-Marquage-CE-DMDIV-FR.pdf

21. Nexialist. Synthèse MDCG 2020-1 [Internet]. Nexialist - votre partenaire pour la conformité des dispositifs médicaux. 2020 [cité 7 févr 2022]. Disponible sur:

https://nexialist.fr/mdcg-2020-1-guidance-on-clinical-evaluation-mdr-performance-evaluation-ivdr-of-medical-device-software-march-2020/

22. LACINA D. Evaluation du lecteur de glycémie assure 4 de numéro de série 56000 (Arkray) chez les personnes vivant avec le VIH/SIDA en zone rurale : cas de l'Hôpital Baptiste de Ferkessedougou. UFR de la République de Côte d'Ivoire; 2013.

23. MDCG 2020-1 : Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software - March 2020 [Internet]. [cité 7 févr 2022]. Disponible sur: https://ec.europa.eu/health/system/files/2020-09/md_mdcg_2020_1_guidance_clinic_eva_md_software_en_0.pdf

24. Navarro M. Exigences de la norme EN ISO 13485 [Internet]. mauricenavarro.com. [cité 7 févr 2022]. Disponible sur: https://www.mauricenavarro.com/ressources/exigences-de-la-norme-en-iso-13485/

25. IMDRF - Software as a Medical Device (SaMD) : Application of Quality Management System [Internet]. [cité 7 févr 2022]. Disponible sur: https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-151002-samd-qms.pdf

26. Yuan S, Fernando A, Klonoff DC. Standards for Medical Device Cybersecurity in 2018. J Diabetes Sci Technol. 24 mars 2018;12(4):743-6.

27. Joannis P-ED, Rochereau A, Serrano C, Pineau J. Cybersécurité des dispositifs médicaux : point sur la menace réelle et rôle du corps médical. Rev Med Suisse 121773-5. 2016;3.

28. Jones RW, Katzis K. Cybersecurity and the Medical Device Product Development Lifecycle. Stud Health Technol Inform. 2017;238:76-9.

29. Risques cyber [Internet]. Gouvernement.fr. [cité 7 févr 2022]. Disponible sur: https://www.gouvernement.fr/risques/risques-cyber

30. Cybersécurité des dispositifs médicaux : environnement règlementaire [Internet]. [cité 7 févr 2022]. Disponible sur: https://travaux.master.utc.fr/wp-content/uploads/sites/16/2021/07/ids101-mim.pdf

31. TGA HSR. Medical device cyber security guidance for industry. mars 2021;55.

32. Underwriters Laboratories. In: Wikipédia [Internet]. 2021 [cité 16 févr 2022]. Disponible sur: https://fr.wikipedia.org/w/index.php?title=Underwriters_Laboratories&oldid=187124759

33. ANSSI. La méthode EBIOS Risk Manager – Le guide [Internet]. ANSSI. 2021 [cité 19 févr 2022]. Disponible sur: https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

34. ClubEBIOS. Étude de cas [Internet]. Club EBIOS. 2021 [cité 19 févr 2022]. Disponible sur: https://club-ebios.org/site/category/type/typeetudedecas/

35. FEULIEN C. La cybersanté en pleine évolution [Internet]. Education Santé. 2017 [cité 19 févr 2022]. Disponible sur: https://educationsante.be/la-cybersante-en-pleine-evolution

36. LE GAT J. Logiciels d'aide à la décision: quel enjeux pour l'accès au marché. Université de Rouen Normandie; 2019.

37. Béatrice Espesson-Vergeat, Pezzali G. Cyberattaque des objets connectés dans le secteur de la santé : quelle protection des fabricants et des utilisateurs ? [Internet]. Fidal. 2017 [cité 7 févr 2022]. Disponible sur: https://www.fidal.com/fr/actualites/cyberattaque-des-objets-connectes-dans-le-secteur-de-la-sante-quelle-protection-des

38. RENARD P. DM connectés et cybersécurité : points d'attention et benchmarking [Internet]. DeviceMed.fr. 2021 [cité 7 févr 2022]. Disponible sur: https://www.devicemed.fr/dossiers/reglementation/dm-connectes-et-cybersecurite-points-dattention-et-benchmarking/27025

39. Rapport d'analyse prospective 2019 - Numérique : quelle (R)évoluation ? [Internet]. [cité 7 févr 2022]. Disponible sur: https://www.has-sante.fr/upload/docs/application/pdf/2019-07/rapport_analyse_prospective_20191.pdf

40. ANSM. La réactovigilance [Internet]. ANSM.fr. [cité 19 févr 2022]. Disponible sur: http://dev4-afssaps-marche2017.integra.fr/Declarer-un-effet-indesirable/Reactovigilance/Reactovigilance/(offset)/0

41. BUTHION A. e-santé : quoi de neuf docteur? Comment le numérique révolutionne la santé et les soins [Internet]. Caisse des Dépôts. 2021 [cité 19 févr 2022]. Disponible sur: https://www.caissedesdepots.fr/blog/article/e-sante-quoi-de-neuf-docteur

42. Rafidison P. Cybersanté, un nouveau défi pour les pharmaciens [Internet]. Académie Nationale de Pharmacie. 2018 [cité 7 févr 2022]. Disponible sur: https://www.acadpharm.org/divers/page.php?rb1=80&id_doc=5084

43. HAS. Télésurveillance médicale : référentiels des fonctions et organisations des soins [Internet]. Haute Autorité de Santé. 2022 [cité 7 févr 2022]. Disponible sur: https://www.has-sante.fr/jcms/p_3311071/fr/telesurveillance-medicale-referentiels-des-fonctions-et-organisations-des-soins

44. HAS. Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé [Internet]. Haute Autorité de Santé. 2021 [cité 21 févr 2022]. Disponible sur: https://www.has-sante.fr/jcms/c_419486/fr/commission-nationale-d-evaluation-des-dispositifs-medicaux-et-des-technologies-de-sante

45. Maîtriser la SSI pour les systèmes industriels [Internet]. [cité 19 févr 2022]. Disponible sur: https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale.pdf

Annexe 1

Les grands principes de la SSI	Définitions
Sensibilisation des personnels	Une partie importante des incidents est liée à une méconnaissance par les intervenants des risques sur l'installation. Leur sensibilisation aux règles « d'hygiène informatique » contribue à réduire les vulnérabilités et les opportunités d'attaques. La sensibilisation doit être régulière car les risques évoluent en permanence.
Cartographie des installations et analyse de risque	Il est important de déterminer : - Les objectifs métier (production, distribution, protection des biens et des personnes…) et les services assurés ; - Les impacts en cas d'interruption de service ; - Les fonctions indispensables à l'atteinte des objectifs, et en particulier : • Leurs niveaux d'implication et de criticité dans la réalisation des services, • Systèmes qui les portent, • Si ces systèmes sont centralisés, distribués, accessibles à distance, etc. ; Un inventaire des installations matérielles, des systèmes et des applications critiques est un pré-requis incontournable à la mise en place de la sécurité des SI. Cet inventaire est la première étape de l'analyse des risques, qui permettra de définir les différents niveaux de criticité, de sûreté, de disponibilité ou d'intégrité attendus pour les éléments cartographiés. Tout projet doit en effet comprendre une analyse de risque afin d'identifier les éléments sensibles du système, leurs besoins et les objectifs de sécurité face aux menaces retenues.
Prévention : concept de la défense en profondeur	La défense en profondeur consiste à protéger les installations en les entourant de plusieurs barrières de protection autonomes et successives. Elles peuvent être technologiques, liées à des procédures organisationnelles ou humaines. Adopter une démarche de défense en profondeur permet de se protéger contre des menaces qui ne sont pas encore connues, de diminuer le périmètre sur lequel une menace est exercée ou d'en atténuer l'impact. Cette stratégie doit intégrer non seulement une démarche de protection préventive, mais aussi des mesures de surveillance, de détections et de réaction.
Surveillance des installations et détection des incidents	Ces mesures n'empêcheront pas un incident mais permettront de le détecter et d'en limiter autant que possible les effets. Plus un incident sera détecté tôt, plus il sera possible de mettre en place des mesures pour en réduire et confiner les effets comme par exemple : - Isoler physiquement les installations en cas d'attaque virale pour limiter les risques de propagation ; - Arrêter une installation avant sa dégradation si ces données de configuration ne sont plus intègres, suite à des erreurs ou des

	modifications intentionnelles.
Traitement des incidents, chaîne d'alerte	Un dispositif de détection n'a de sens qu'associé à la mise en place d'une organisation et de procédures pour traiter les incidents. Il convient de déterminer : - Que faire lors de la détection d'un incident ; - Qui alerter ; - Quelles sont les premières mesures à appliquer. Un processus d'escalade doit être défini pour gérer les incidents au bon niveau de responsabilité, et décider en conséquence : - S'il faut déclencher un Plan de Reprise d'Activité (PRA) ; - Si une action judiciaire est nécessaire.
Veille sur les menaces et les vulnérabilités	Se tenir informé de l'évolution des menaces, des vulnérabilités en identifiant les incidents qu'elles favorisent, ainsi que leurs effets potentiels constitue une mesure fondamentale de défense. Par exemple, le site internet du centre opérationnel de l'ANSSI est une source d'information importantes sur les vulnérabilités identifiées, les éventuels correctifs existants ou les contre-mesures qu'il est possible de mettre en place.
Les plans de reprise et de continuité d'activité (PRA / PCA / DRP)	Se préparer à faire face à des événements exceptionnels pour lesquels toutes les mesures précédentes auraient échoué minimisera les impacts et permettra de redémarrer l'activité le plus rapidement possible. Les Plans de Continuité d'Activité métier de l'entreprise (PCA) doivent donc intégrer les systèmes d'informations industriels. Ils incluent la définition des Plan de Reprise d'Activité (PRA), ou Disaster Recovery Plan (DRP), qui identifient les moyens et procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas de sinistre ou d'événements exceptionnels. Ils devraient décrire comment reconstruire le système suite à une attaque virale, un incendie, une inondation ou une perte de données. (45)

SERMENT DE GALIEN

Je jure, en présence de mes maîtres de la Faculté, des conseillers de l'Ordre des pharmaciens et de mes condisciples :

- **D'honorer ceux qui m'ont instruit dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle à leur enseignement.**
- **D'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de l'honneur, de la probité et du désintéressement.**
- **De ne jamais oublier ma responsabilité et mes devoirs envers le malade et sa dignité humaine, de respecter le secret professionnel.**
- **En aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels.**

Que les hommes m'accordent leur estime si je suis fidèle à mes promesses.

Que je sois couvert d'opprobre, méprisé de mes confrères, si j'y manque.

Mathilde VOUILLOT 2022

LOGICIELS D'AIDE À LA DÉCISION CLINIQUE DANS LE DIAGNOSTIC *IN VITRO* : DÉVELOPPEMENT ET CYBERSÉCURITÉ

RÉSUMÉ

Au sein du large domaine que représente la e-santé, les logiciels d'aide à la décision clinique connaissent actuellement un essor important. En effet, grâce à la combinaison de bases de données médicales et d'algorithmes avec des données spécifiques au patient, ces outils informatiques sont de plus en plus proposés comme solutions médicales afin de fournir aux professionnels de santé et/ou aux utilisateurs, des recommandations pour le diagnostic, le pronostic, la surveillance et le suivi des patients de façon individuelle.

La finalité médicale des données ainsi obtenues représente un enjeu réglementaire majeur. Ainsi, les logiciels spécifiquement destinés par le fabricant à une ou plusieurs des fins médicales visées dans la définition d'un dispositif médical de diagnostic *in vitro* (DMDIV) répondront du Règlement (UE) 2017/746, afin d'obtenir le marquage CE en vue de leur mise sur le marché européen.

Cependant, ces logiciels de DMDIV ont rapidement été intégrées dans la pratique médicale quotidienne sans que les risques associés soient parfaitement maîtrisés. En effet, la connectivité de ces dispositifs les exposent à des cybermenaces qui peuvent potentiellement conduire à un risque accru de préjudice pour les patients. Il devient donc essentiel que les fabricants de ce type de logiciels soient en capacité d'intégrer, tout au long du développement et du cycle de vie de leurs produits, une sécurité informatique face à ces menaces. C'est ce qu'on appelle la cybersécurité.

MOTS-CLÉS : logiciels, dispositifs médicaux de diagnostic in vitro, DMDIV, aide à la décision clinique, règlementation, Règlement (UE) 2017/746, IVDR, cybersécurité, RGPD, software, SaMD, cyber-attaque, MDSW, IVD MDSW, cybersanté

PRÉSIDENT DU JURY : Pr. Pascal RATHELOT
DIRECTEUR DE THÈSE : Pr. Romaric LACROIX
AUTRES MEMBRES DU JURY : Dr. Pierre LEMERCIER