Maîtrise des risques pour les logiciels de santé ou des dispositifs médicaux connectés selon NF EN IEC 80001-1

Cyriane Canada, Hippolyte Boucher, Clément Debelle, Jordy Ramos, Jean-Yves Sinnas

Université de Technologie de Compiègne
Master 2 Ingénierie de la Santé
Technologies biomédicales et Territoires de la Santé

Maîtrise des risques pour les logiciels de santé ou des dispositifs médicaux connectés selon NF EN IEC 80001-1

Auteurs :
Cyriane Canada
Hippolyte Boucher
Clément Debelle
Jordy Ramos
Jean-Yves Sinnas

https://doi.org/10.34746/yxb0-qp16

IDCB

Automne 2021

Remerciements :

Nous tenons à remercier toutes les personnes qui ont participé à l'élaboration et au bon déroulement de notre projet concernant la norme NF EN CEI 80001-1.

Tout d'abord, nous remercions les membres de l'équipe pédagogique du Master IDS (Ingénierie de la Santé) pour nous avoir orientés dans nos travaux de recherches.

Nous souhaitons spécialement remercier monsieur Gilbert FARGES, notre porteur de projet à l'UTC, d'avoir suivi l'évolution de notre projet et de nos livrables ainsi que de nous avoir guidé jusqu'à leurs bonnes réalisations.

Un grand merci également à madame Isabelle CLAUDE et monsieur Jean-Matthieu PROT, nos référents du Master, pour leurs soutiens et leurs conseils.

Nous tenons aussi à remercier madame Béatrice KONIG pour ses conseils dans nos recherches documentaires et son aide à la réalisation d'une bibliographie complète.

Finalement nous remercions tous les étudiants du Master IDS pour leur écoute, leur intérêt, et leurs questions quant au fonctionnement de la norme NF EN CEI 80001-1.

Résumé

L'évolution constante de la médecine permet une amélioration des diagnostics et une plus grande variété de traitements et de prise en charge des patients. Cette évolution s'explique en partie par un développement accru des outils de connectiques et informatiques. Grâce à ce développement technologique, les dispositifs médicaux deviennent connectés entraînant donc une transmission des informations ainsi qu'une communication plus rapide et efficace de manière à apporter des réponses à des problèmes complexes non solvables sans cette technologie.

Le développement rapide de l'e-santé, défini dans le milieu médical par les logiciels de santé et les dispositifs médicaux connectés, engendre de potentiels accidents et risques qu'il faut prendre en compte pour éviter tout dysfonctionnement et danger. Ainsi le fabricant et l'exploitant doivent gérer les risques associés à ces systèmes TI (Technologie de l'Information) de santé. La norme NF EN CEI 80001-1 existe ainsi pour aider ces protagonistes à mettre en place une gestion des risques appropriée et ainsi écarter tout risque lié à l'utilisation de tel dispositif et logiciel en rendant leur utilisation optimale.

Pour s'inscrire dans une démarche normative optimale, il est important d'avoir une bonne compréhension de la norme NF EN CEI 80001-1. Pour cette raison, il est intéressant de mettre en place un système de management du risque performant lié à l'exploitation des DMC et logiciels de santé.

L'objectif du travail présenté est de faciliter l'appropriation et l'utilisation de la norme NF EN CEI 80001-1. La première étape d'implantation de la norme dans une organisation est la compréhension de celle-ci, pour cela, une cartographie de la norme résume l'ensemble des objectifs et exigences de celle-ci. Dans un second temps, l'outil de diagnostic et de management des risques proposé permet aux fabricants et exploitants de mesurer leurs validités vis-à-vis de la norme et prévoir les plans managériaux mis en place.

Abstract

The constant evolution in medicine allows an improvement of diagnosis and a larger variety of treatment and caring for the patients. This evolution is explained by an increased development of connectics and informatics tools. Thanks to this technologic development, medical devices have become more and more connected leading to better data transmission along with more efficient and faster communication in order to bring answers to complex problems non solvable without this technology.

The fast e-health development, defined in the medical field as health softwares and connected medical devices, might generate potential accidents and risks which have to be taken into account in order to avoid malfunction or danger. Thus, manufacturers and operators must manage the risks associated with these health IT (Information Technology) systems. Therefore, the NF EN CEI 80001-1 norm helps these protagonists in implementing an appropriate risk management in order to discard any risk associated with the use of these medical devices and softwares, making their use optimal.

To be part of an optimal normative process, having a good understanding of the norm NF EN CEI 80001-1 is important. In that way, implementing a management system of risks related to the exploitation of the connected medical devices and health software can be interesting.

The purpose of the present work is to facilitate the appropriation and use of the NF EN CEI 80001-1 norm. The first step of the norm's implementation in an organization is its comprehension. The cartography tool resuming all the objectives and requirements help to achieve this aim. Secondly, a diagnosis and risk management tool was made to provide producers and managers a simple identification and measurement of their validity regarding the norm, and allows them to create and implement management plans.

Sommaire
Table des matières

Table des abréviations

- ANSM : Agence Nationale de Sécurité du Médicament et des produits de santé
- CEI : Commission Électronique Internationale
- CEE : Conseil des Communautés Européennes
- DGR : Dossier de Gestion des Risques
- DM : Dispositif médical
- DMC : Dispositif Médical Connecté
- DMDIV : Dispositif médical de Diagnostic In Vitro
- DSI : Directeur des Systèmes d'Informations
- EN : Norme Européenne
- HAS : Haute Autorité de Santé
- IFOP : Institut Français d'Opinion Publique
- ISO : International Organization for Standardization
- LFSS : Loi de financement de la Sécurité sociale
- Marquage CE : Marquage Conformité Européenne
- RGPD : Règlement Général sur la Prise en Charge des Données
- RSSI : Responsable de la Sécurité des Systèmes d'Information
- SI : Système d'Information
- SWOT : Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces)
- TI : Technologie de l'Information
- UE : Union Européenne

Table des illustrations

Introduction

La médecine, en constante évolution, s'est améliorée au fur et à mesure du temps sur ses diagnostics, par une plus grande expérience, mais aussi sur les équipements médicaux qui participent à une meilleure élaboration des diagnostics et une plus grande variété de traitements voire une création de traitements. Les développements mondiaux autour des **outils de connectiques et d'informatique** ne cessent d'avancer. L'augmentation des possibilités s'offre aussi au domaine médical qui se doit d'utiliser la pointe de la technologie afin de sensiblement se rapprocher du **meilleur traitement possible**. Aujourd'hui, les dispositifs médicaux sont omniprésents et deviennent de plus en plus connectés afin de transmettre des informations ou de communiquer plus rapidement et efficacement dans l'objectif d'apporter des réponses à des problèmes non résolus sans la technologie ou bien très complexe.

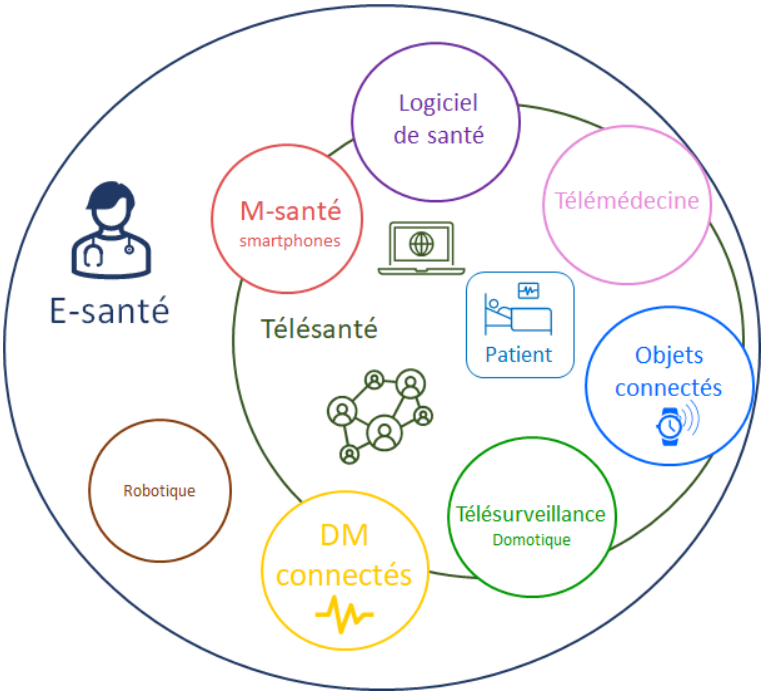

Figure 1 - schéma des différents domaines de l'e-santé

Se développant rapidement, **l'e-santé**, définit par l'ensemble des applications des technologies de l'information et de la télécommunication au service de la santé par l'HAS [1] se répand dans le monde du médical. Deux parties de ce domaine sont particulièrement intéressantes : **les logiciels de santé et les dispositifs médicaux connectés**. Cependant, il convient de différencier un dispositif médical connecté (DMC) d'un objet connecté de santé. La définition ne vient pas du produit en tant que tel, mais de la finalité assignée par le fabricant. Si l'utilisation de son produit de santé est destinée à des fins médicales comme définies dans le règlement européen 2017/745 [23], il sera alors un dispositif médical connecté et devra répondre à certaines exigences spécifiques de sécurité évaluées par des études cliniques afin d'obtenir une certification CE. Au contraire, un objet connecté de santé n'a pas de finalités médicales déclarées, il n'a donc pas de certification CE et correspond généralement plus à un outil du bien-être ou de la prévention.

Lors de l'utilisation de DMC ou de logiciels de santé, la possibilité d'avoir des accidents ou des dysfonctionnements, en rapport avec par exemple de la cybersécurité [27] n'est pas exclue mais le cadre médical dans lequel il est utilisé oblige le fabricant à gérer les risques. Il n'est cependant pas aisé de repérer tous les risques, c'est pourquoi la **norme ISO 80001** existe. Cette norme a pour vocation la **sécurité, l'efficacité et la sûreté** dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connecté par une gestion des risques appropriée. Ainsi, lorsque celle-ci sera bien utilisée, l'utilisation de ces produits de santé apportera un réel apport au monde médical.

Néanmoins, la bonne compréhension de cette norme est importante pour les fabricants s'ils veulent s'inscrire dans une démarche normative. C'est pourquoi il est intéressant de se demander

comment obtenir un **système de management du risque** performant lié à l'exploitation des DMC et des logiciels de santé. Tout d'abord, une ébauche du contexte des DMC permettra de répondre à cette question. Puis, afin de mieux cerner le contexte législatif, une étude des différentes réglementations sur les DMC sera réalisée. Enfin, l'objectif de ce travail étant la création d'un outil facilitant l'exploitation de la norme ISO 80001, les caractéristiques et l'utilisation de cet outil seront détaillés.

I- Les logiciels de santé et DM connectés : apports pour la santé

A - DMC et logiciel de santé : définitions

À l'ère technologique actuelle, les fabricants de dispositifs médicaux disposent de moyens technologiques et connectiques de plus en plus avancés et faciles d'accès. Aussi, bien que certains médecins hésitent à en utiliser, le bénéfice apporté par la connectivité peut devenir essentiel et améliorer la précision ainsi que la rapidité des diagnostics. Il est donc important de définir correctement les dispositifs qui répondent à ces appellations.

D'après le règlement de l'UE 2017/745, un dispositif médical correspond à tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes :

- Diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie,
- Diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci,
- Investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique,
- Communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus [2]

Et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par le métabolisme, mais dont la fonction peut être assistée par de tels moyens.

D'après la Haute Autorité de Santé (HAS), sont définis comme DMC, les dispositifs "utilisés à des fins de télésurveillance médicale ou de téléconsultation" ou "générant une action du patient à des fins d'auto-traitement ou d'autosurveillance". Les DMC devront être "utilisés à des fins médicales", "par le patient lui-même" et disposer d'une "fonction de télécommunication" [3].

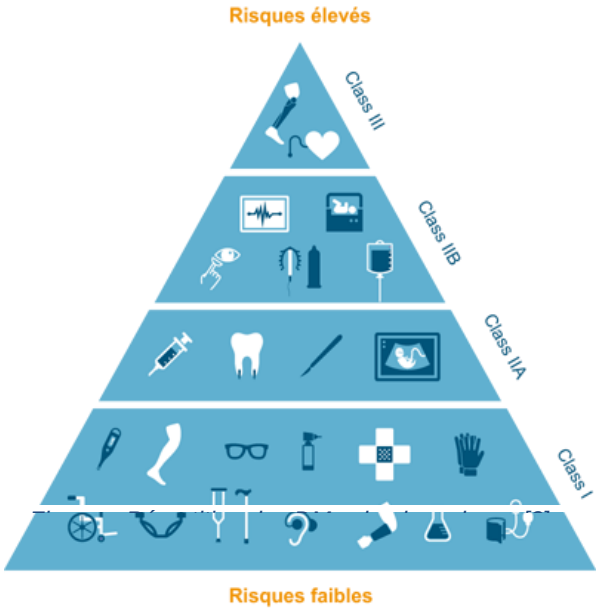

Figure 2 - Répartition des DM selon leur classe [3]

Il convient ensuite de bien différencier les DMC des objets connectés de santé. Les objets connectés de santé, contrairement aux DMC sont utilisés à des fins généralement de bien-être, ils ne sont pas destinés à une finalité médicale déclarée, bien qu'ils puissent participer à avoir une meilleure santé, à titre d'exemple : les montres connectées, les piluliers connectés ou encore les balances connectées [30].

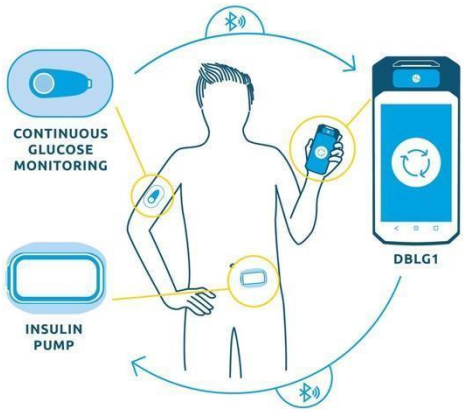

Figure 3 - Exemple de l'utilisation de DMC et logiciels de santé dans le traitement du diabète [5]

En parallèle des DMC, les logiciels de santé apportent aussi énormément d'apports aux patients et aux professionnels de la santé. Le statut de ces logiciels dépend, comme pour les DM, de l'utilisation que le fabricant lui voue. Chaque logiciel de santé demande une analyse fine de la destination d'usage et de l'exploitation des données entrantes. D'après l'ANSM, pour qu'un logiciel de santé soit qualifié de DM ou DMDIV, il doit présenter les trois critères suivants :

- Être destiné à une utilisation à des fins médicales rejoignant la définition du DM ou DMDIV
- 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 [4].
- Si un logiciel de santé cumule ces trois critères, il devient par conséquent un dispositif médical et doit répondre de certaines normes et directives explicites afin d'obtenir le marquage CE

L'illustration ci-dessous explicite les différentes catégories de logiciels de santé selon la norme CEI EN 82304-1 sur les logiciels de santé : exigences générales pour la sécurité des produits [28] ainsi que selon la norme CEI EN 62304 : Logiciels de dispositifs médicaux — Processus du cycle de vie du logiciel [29].

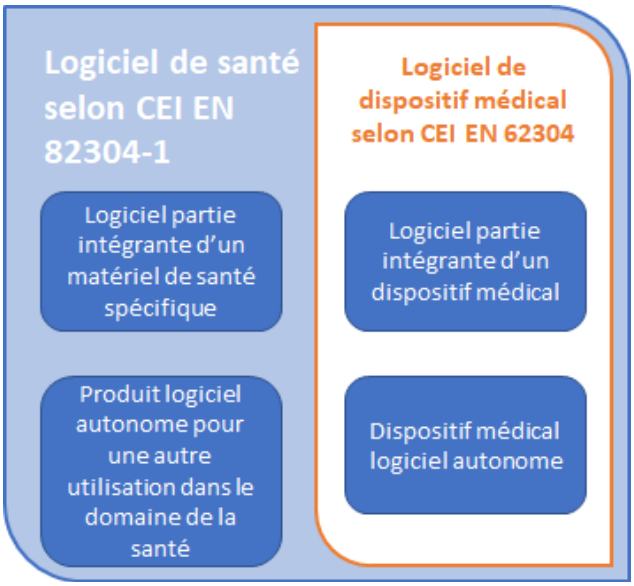

Figure 4 - Critères spécifiques différenciant les logiciels de santé au logiciel de DM (source : auteurs)

Fleurissant, le marché de l'e-santé permettrait de générer, selon une étude du cabinet McKinsey & Company, entre 16.1 et 22.3 milliards d'euros par an [5]. Les solutions innovantes faites pour assurer une plus grande autonomie des patients pourraient représenter entre 3.3 et 4.7 milliards d'euros annuels de valeur créée. Ces chiffres proviennent de plus de 500 recherches internes et études disponibles en France et à l'international. Le marché des dispositifs médicaux s'élevait à 30 milliards d'euros de chiffre d'affaires en 2019 selon une étude du Syndicat national de l'industrie des technologies médicales (Snitem). L'image ci-dessous, issue d'un article de l'Institut de Montaigne, expose la création de valeur en milliards d'euros pour plusieurs catégories d'innovation et d'impact dans le domaine de l'e-santé.

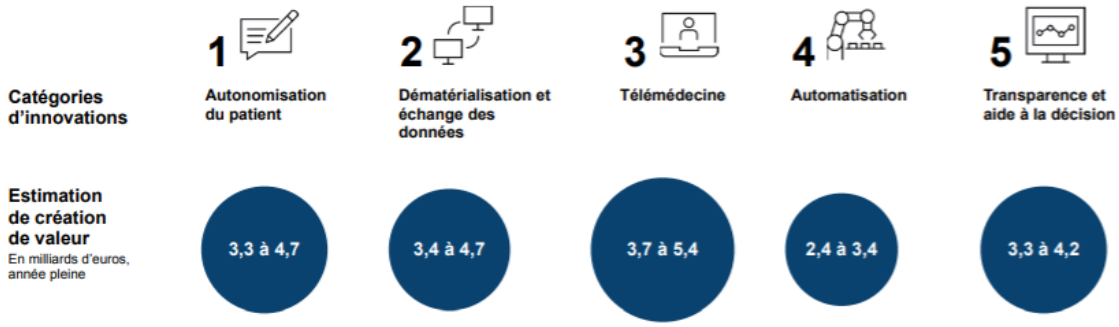

Figure 5 - Catégories d'innovation et impact, entre 16,1 et 22,3 milliards d'euros [7]

Maintenant que les termes sont définis et que le marché est un peu apprécié, les enjeux des dispositifs médicaux connectés et des logiciels de santé seront définis.

B - Les enjeux des DMC et logiciels de santé et de la norme

Étymologiquement parlant, le mot « enjeux » signifie ce qui est mis en jeu, ce qui peut être aussi bien des enjeux matériels (comme l'utilisation d'un dispositif médical connecté) comme des enjeux immatériels (par rapport à la mise en place de la norme 80001-1).

Les enjeux concernent ce que l'on peut gagner mais aussi ce que l'on peut perdre en fonction de l'utilisation de la norme 80001-1 et des objectifs qui sont définis au sein de l'entreprise (fabriquant comme établissement médicaux). Ancré dans un contexte technologique complexe, la norme 80001-1 répond à une montée croissante des DMC et logiciels de santé influant sur plusieurs enjeux tels :

Figure 6 - Les enjeux des DMC, des logiciels de santé et de la norme (source : auteurs)

- **Des enjeux législatifs/réglementaires/juridiques**

Qu'ils prennent la forme d'un implant, d'un équipement ou d'une application mobile, les DMC et logiciels de santé doivent répondre aux exigences spécifiques de sécurité et de bénéfice clinique de la réglementation européenne. L'intérêt de répondre à ces exigences est la limitation des risques pour le patient, l'utilisateur et la sécurité légale du fabricant [21]. C'est-à-dire que le fabricant doit mettre en œuvre les démarches juridiques nécessaires pour que son DMC ou logiciel de santé soit en adéquation avec les législations en vigueur.

Ces enjeux concernant la norme sur la gestion des risques peuvent avoir un impact interne à l'établissement de santé, mais aussi un impact externe avec le fabricant puisqu'il s'agit de mettre en place une norme. La mise en place de la gestion des risques pour les DMC et logiciel de santé implique que les fabricants aient en amont vérifié que leurs produits soient conformes aux normes associées. La norme peut permettre de clarifier certaines responsabilités, autant sur la mise en œuvre du système que sur la gestion des risques tout au long du cycle de vie du DMC ou logiciel de santé.

- **Des enjeux sociaux/ humains**

Les enjeux sociaux impliquent aussi bien le fabricant que le professionnel de santé et le patient. L'apport de ces systèmes TI de santé permet d'éviter les erreurs humaines lors des utilisations ou analyses, sans pour autant limiter les actions et décisions que les humains prendront par la suite. Lors d'échanges avec des professionnels de la santé, ceux-ci rapportent une évolution sur la charge de travail par, entre autres, l'allègement des tâches répétitives et la présence de chaînage, par la dématérialisation des dossiers et par une optimisation du post-traitement des images.

Par exemple, l'entreprise "Azmed" propose un logiciel de santé pour le traitement de l'imagerie médicale qui permettrait de réduire de 20 % les erreurs d'interprétation et un gain de temps de 36 % pour le radiologue [31]. Cela aurait un impact sur le diagnostic des pathologies et donc directement sur la santé du patient.

La norme aura un impact sur la gestion des risques sur le court et le long terme. Par une meilleure gestion des risques, l'exécution de la norme pourra avoir des conséquences bénéfiques directes ou indirectes sur la santé du patient. De plus, une satisfaction client n'est pas à négliger

concernant le fabricant et le professionnel de santé sur la gestion des risques, puisqu'il doit aider les professionnels de santé à appliquer les principes clés de sécurité, efficacité et sûreté des systèmes TI de santé.

- **Des enjeux environnementaux/ organisationnels**

Figure 7 - Appareils de santé connectés dans le monde en 2020 (Sources : [32] + Auteurs)

En 2020, 161 millions d'appareils de santé connectés circulaient dans le monde [32]. Leur présence dans l'environnement médical, bien que réel, n'est pas forcément remarquée. De ce fait, les enjeux matériels auront un impact externe sur l'environnement des professionnels de santé mais aussi des patients et des fabricants. Avec la crise sanitaire encore présente à l'heure actuelle, les systèmes TI de santé prennent une part importante dans tous types d'environnements (fabricants, établissements de santé et patients) avec une analyse de la gestion des risques croissante.

L'environnement de travail est un exemple concret de l'impact que peut avoir la mise en place des outils de la norme. Cela peut à la fois alléger la charge de travail des instances des organismes responsables et des organisations par une rigueur et une amélioration continue, comme l'augmenter sur certains points en fonction de la logistique installée ou de la mauvaise exécution de la norme.

La mise en place des outils en adéquation à la norme dans les établissements de santé permettrait de réduire considérablement la charge de travail. Cela faciliterait l'intégration et le choix des systèmes TI de santé par les établissements médicaux.

- **Des enjeux technologiques**

Les avancées techniques et les recherches médicales accentuent aujourd'hui les spécificités et les possibilités offertes par les DMC et logiciels de santé. Le développement et la diversité des applications technologiques soulignent l'intérêt qu'ils apportent au traitement des patients.

Cependant, il est important de prendre en compte l'accroissement des possibilités de risques, de problèmes voir de dangers que ces progressions technologiques impliquent. En guise d'exemple, l'interopérabilité entre le professionnel de santé et le système TI de santé ainsi que le format des logiciels de santé et la compatibilité, fabricant dépendant, peuvent entraîner des problèmes sur le long terme.

Par exemple, si un logiciel de santé n'est pas compatible avec les technologies informatiques mises en place dans un établissement de santé, sa fonctionnalité sera remise en cause. Néanmoins, dûe aux nouveaux équipements techniques connectés, des formations devront certainement être mises en place afin de permettre aux professionnels de santé de mieux gérer ces outils innovants.

La norme NF EN IEC 80001-1 permettrait ainsi de gérer les nombreuses apparitions technologiques contemporaines. Par exemple, la gestion et l'organisation des données est un point crucial qu'il ne faut surtout pas négliger dans l'appropriation des outils de gestion des risques mais aussi au niveau de la norme. En effet, si les données ne sont pas gérées et organisées de manière optimale, cela peut avoir un impact sur la compréhension et l'utilisation de l'outil. Vu qu'il s'agit d'un

outil numérique en premier lieu, il y a la question de la fiabilité et de la sécurité qui rentre en compte. En effet, l'instauration d'un ou plusieurs outils numériques nécessitent des mises à jour techniques afin que l'outil reste opérationnel.

- **Des enjeux économiques/financiers**

La mise en place dans un premier temps du respect de la norme peut paraître un investissement parfois conséquent. Cependant, des rémunérations directes ou indirectes peuvent apparaître. Par exemple, une bonne prédiction des risques possibles réduit considérablement les maintenances futures lors de l'utilisation d'un DMC.

Également, un autre exemple concerne plus particulièrement les données récoltées pour les DMC et logiciels de santé. En effet, ces données sont dans un premier temps analysées puis utilisées pour aider les patients dans le traitement de leur pathologie (comme la glycémie pour le diabète). Néanmoins, la vente de ces données de façon anonyme à des centres de recherche se fait de plus en plus couramment. Par exemple, d'après une enquête du Consumer Science Analytics (CSA) Research, sur 78% des français interrogés qui sont en accord avec le partage des données médicales, 20% sont prêts à revendre leurs données médicales [33].

Par la soumission du DMC ou du logiciel de santé à la norme 80001-1, et sa conformité aux exigences demandées (Propriétés clés : Sécurité, efficacité et sûreté), le fabricant peut ainsi garantir une sécurité exigée par le marché et l'environnement d'application du système TI de santé pour la transmission des données.

Pour les chargés d'affaires réglementaires au sein de ces structures, un gain de temps est à prévoir par la facilitation de la compréhension de la norme et donc un gain économique. Par exemple, pour un hôpital qui souhaiterait intégrer au sein de ses services un logiciel de santé, la mise en place de la gestion des risques serait facilitée grâce aux outils qui découlent de la norme 80001-1.
Néanmoins, il ne faut pas oublier que la mise en place de la norme 80001 pourrait aussi réduire considérablement la mise en place des DMC et des logiciels de santé car cela pourrait être une contrainte dans leur implantation dans un établissement de santé.

L'état français a financé la numérisation du système de santé à hauteur de 1,5 Milliards d'euros [34].

Tous ces différents enjeux permettent d'appréhender l'environnement autour des systèmes de technologie de l'information de santé et ainsi de définir les principaux risques auxquels les fabricants, les professionnels de santé, les établissements médicaux ou encore les patients pourront rencontrer.

C - Identification des principaux risques

Selon le dictionnaire Larousse, le risque peut être défini comme étant la "Possibilité, probabilité d'un fait, d'un événement considéré comme un mal ou un dommage". Aussi, il est qualifié de "Danger, inconvénient plus ou moins probable auquel on est exposé" [35].
Dans le milieu de la santé, le Centre d'Hygiène et de Sécurité au Travail (CHST) le décrit comme "la probabilité qu'une personne subisse un préjudice ou des effets nocifs pour sa santé en cas d'exposition à un danger." [36]. Il est indispensable d'identifier les risques auxquels sont soumis les DMC et logiciels de santé afin de les maîtriser.
Comme mentionné dans le titre de la norme [21], les risques associés aux DMC et logiciels de santé concernent trois notions : la sûreté, l'efficacité et la sécurité.

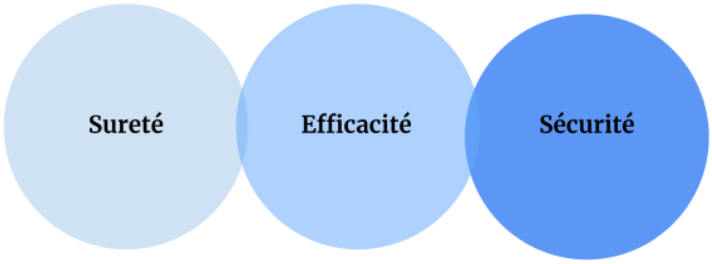

Figure 8 - Les trois notions de risques des DMC et logiciels de santé d'après la norme NF EN IEC 80001-1 [21]

La sûreté "relève d'actes de malveillance envers des personnes, des biens, des bâtiments ou encore des informations, il y a donc une intention de nuire [6]."

L'efficacité est la "capacité, d'une personne, d'un groupe ou d'un système, à parvenir à ses fins, à ses objectifs (ou à ceux qu'on lui a fixés) [7]."

La sécurité concerne "l'ensemble des risques dont la cause est accidentelle et donc par définition involontaire [6]."

- **Concernant la sûreté :**

Les risques liés à la sécurité lors de l'utilisation des DMC ou logiciels de santé résident dans leur capacité de communication via un réseau sans fil. Ces produits peuvent donc être les cibles d'attaques externes malveillantes lorsque le DM ou logiciel de santé présente un déficit sécuritaire. Les DM standards ne sont pas concernés par le piratage car ils communiquent au sein d'un réseau fermé. De manière simplifiée, les données produites lors de l'utilisation d'un DMC sont transmises vers un logiciel ou application que le patient peut consulter, ou sont transmises vers des serveurs auxquels ont accès les médecins.

Ce type d'attaque externe est plus communément appelé "cyberattaque" et les déficits sécuritaires sont qualifiés de "vulnérabilités". Un leader de la télécommunication a d'ailleurs défini la vulnérabilité en cybersécurité comme étant "une faille de sécurité" provenant "dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel."

L'ANSM a elle définit la cybersécurité comme étant "l'ensemble des mesures techniques ou organisationnelles mises en place pour assurer l'intégrité et la disponibilité d'un dispositif médical (DM) ainsi que la confidentialité des informations contenues ou issues de ce dispositif médical (DM) contre le risque d'attaques dont il pourrait faire l'objet" [8].

Une cyber-veille en santé permet de traquer la moindre vulnérabilité et de publier chaque jour des alertes sur le site du gouvernement français [9]. Certaines vulnérabilités peuvent avoir de réelles conséquences physiques sur le patient, d'autres présentent également un danger même si l'intégrité du patient n'est pas menacée.

Les schémas ci-dessous illustrent la chaîne de transmission des données et leurs acteurs dans le cas d'un système informatique sûr, et dans le cas d'un système informatique présentant des vulnérabilités :

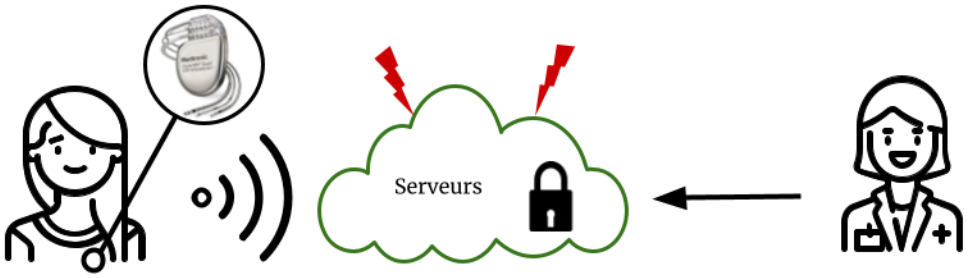

Figure 9 - Cas n° 1 : Les données du défibrillateur automatique implantable (DAI) sont transmises grâce à une fonction de télémédecine sur un serveur sûr résistant aux cyberattaques, accessible par les professionnels de santé (source : auteurs et [44])

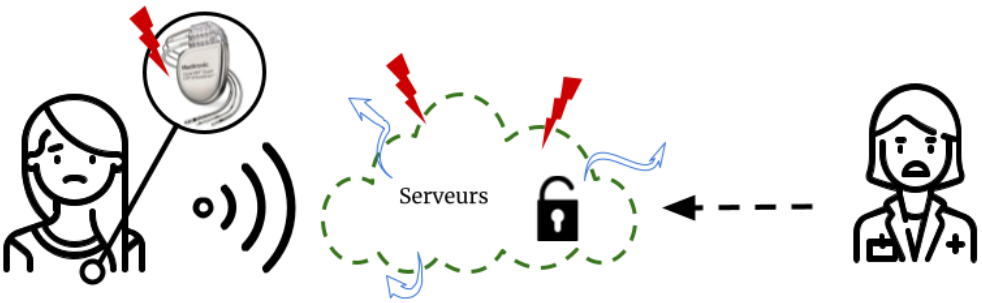

Figure 10 - Cas n°2 : Les données du défibrillateur automatique implantables sont transmises grâce à une fonction de télémédecine sur un serveur présentant des vulnérabilités, victime du potentielles cyberattaques entraînant 2 risques majeurs : l'accès aux donnée

Plus précisément, il existe deux risques majeurs pour les utilisateurs de DMC en cas de cyberattaque :

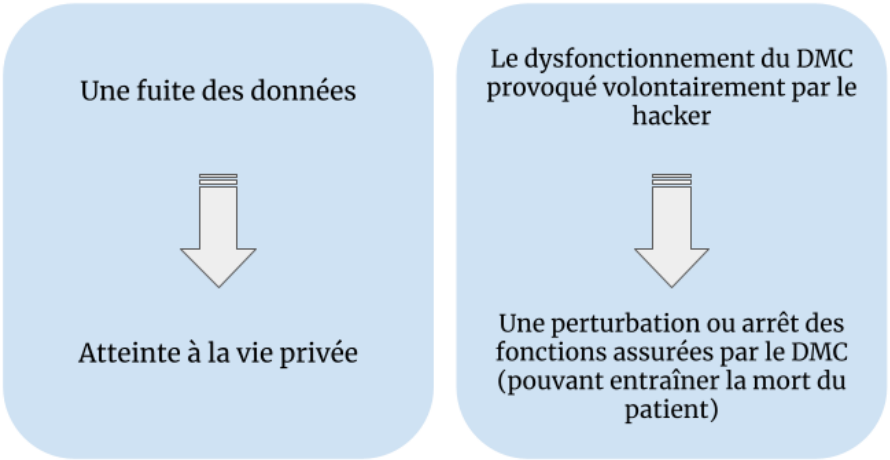

Figure 11 - Deux risques majeurs en cas de cyberattaque et leurs conséquences (source : auteurs)

L'illustration ci-dessous recense quelques exemples de cyberattaques et de vulnérabilités publiées sur le site "cybersurveillance santé" du gouvernement français, mentionnés par l'ANSM ou encore faisant l'objet d'une publication par des chercheurs américains :

- En 2008 : Des chercheurs arrivent à pirater un défibrillateur automatique implantable, à décharger la batterie ou à délivrer un choc à une distance allant jusqu'à 10 mètres du patient [10].
- En 2012 : Un hacker réputé, Jack Barneby pirate en direct un stimulateur cardiaque ainsi qu'une pompe à insuline lors du Congrès national de la sécurité des systèmes d'information de santé, montrant alors son aptitude à décharger totalement la réserve d'insuline dans le patient, pouvant entraîner une dégradation de son état, voire sa mort [11].
- En 2015 : Le piratage du système informatique du service de radiothérapie de Valence, donnant l'accès aux données des patients contenues dans les DM [8].
- En 2016 : Des vulnérabilités déclarées sur une pompe à insuline Johnson & Johnson dotée d'une fonction WIFI [12].
- En 2021 : Déclaration de vulnérabilités au sein de Philips Healthcare Tasy Electronic Medical Record entraînant une atteinte à la confidentialité des données et la violation des politiques de sécurité [9].

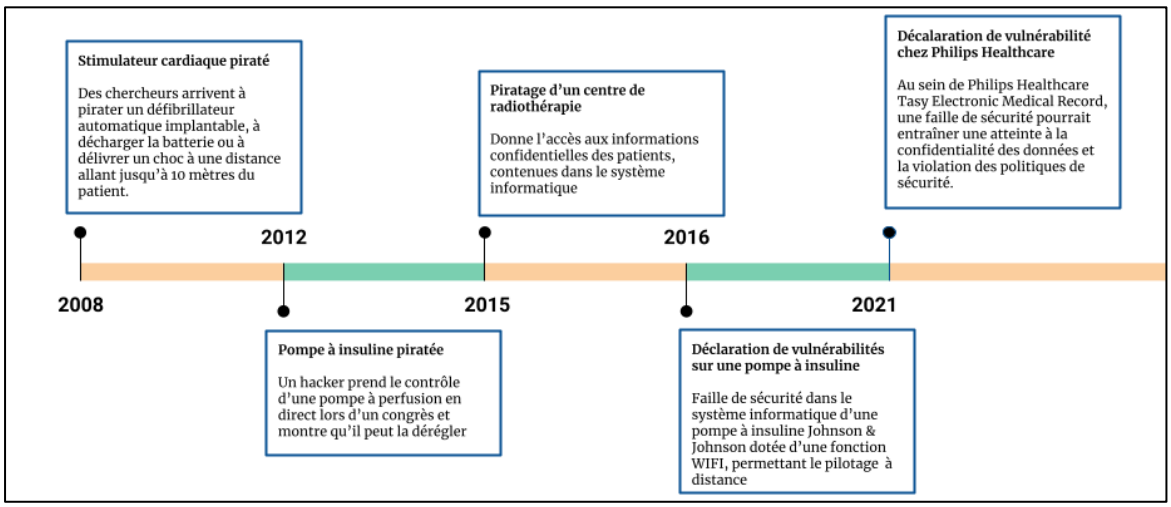

Figure 12 - Quelques exemples de cyberattaques et vulnérabilités (source : auteurs)

Ces exemples de cyberattaques et vulnérabilités montrent à quel point les données de santé peuvent être une cible. Elles sont qualifiées "d'or noir" par les cyberpirates.

- **Concernant la sécurité :**

Comme défini précédemment, la sécurité vise à prévenir les accidents. Sook-Hua Wong (Responsable du segment industriel dans une entreprise qui fournit des équipements de test et de mesure pour la conception électronique) explique que les systèmes TI de santé font l'objet de nombreux tests durant leur phase de conception afin d'assurer leur qualité tout au long du cycle de vie.

Cependant : “certains de ces défauts ne sont pas détectés pendant les tests de fabrication en raison de la couverture insuffisante du système utilisé. Les unités ayant réussi les tests de justesse peuvent être à l’origine de défaillances en cours d’utilisation en raison de leurs performances dégradées.” [37]

Voici donc quelques exemples de défaillances sécuritaires concernant des dispositifs médicaux et logiciels de santé :

- En 2017 : Medtronic annonce que ses modèles de ventilateurs Newport HT70 et Newport HT70 Plus subissent une mise à jour involontaire qui les réinitialise pendant le fonctionnement normal de l’appareil, sans déclenchement de l’alarme. Suite à cette réinitialisation, le ventilateur se met en mode veille jusqu’à ce qu’il soit manuellement reprogrammé. Cet accident peut être mortel pour les patients bénéficiant de ces ventilateurs. [38]

- En 2018 : Le logiciel d‘oncologie et de radiothérapie Aria de Varian Medical Systems attribue les informations d’un patient au dossier d’un autre patient. L’erreur se produit lors du chargement de la page d’un dossier patient. Des erreurs lors du traitement de radiothérapie peuvent survenir. [39]

- **Concernant l’efficacité :**

L’évaluation de l’efficacité des DMC et logiciels de santé est similaire à celle des DM standards bien que les DMC possèdent des spécificités liées à leurs fonctions de connectivité.

C’est la Commission Nationale d’Évaluation des Dispositifs Médicaux et Technologies de Santé (CNEDiMTS) de l’HAS qui est chargée de l’évaluation de ces dispositifs. Plus précisément : “[...] au-delà de la démonstration des performances et de la sécurité, elle s’attache à évaluer l’intérêt du DM pour le patient et pour la santé publique (service attendu), ainsi que sa place dans l’arsenal disponible en France (amélioration du service attendu) [40]“.

Pour éclaircir la procédure d’évaluation des DMC, l’HAS publie en janvier 2019 le “Guide sur les spécificités d’évaluation clinique d’un dispositif médical connecté (DMC) en vue de son accès au remboursement [41]”.

Voici quelques exemples de dispositifs médicaux connectés dont le service attendu a été jugé comme insuffisant par la CNEDiMTS :

- En 2020 : Abbott demande l’inscription sur la LPPR d’un système de stimulation cérébrale pour les patients atteints de la maladie de Parkinson. Ce stimulateur implantable est accompagné d’une télécommande pour la gestion de la douleur par le patient. Les données cliniques ont été jugées impertinentes, la CNEDiMTS a conclu que le service attendu était insuffisant et que ce système répondait à un besoin thérapeutique déjà couvert par d’autres dispositifs [45].

- En 2021 : Abbott demande l’inscription sur la LPPR d’un capteur de pression pulmonaire Cardiomems. Ce capteur est doté d’une fonction de télécommunication pour transmettre les données aux médecins. La CNEDiMTS conclut que les données cliniques ne permettent pas de prouver l’intérêt de ce dispositif dans l’indication revendiquée. [42]

En conclusion, la nécessité de protéger l'accès aux DMC et logiciels de santé tout au long de leur cycle de vie est démontrée. La norme NF EN IEC 80001-1 propose des actions à mettre en place afin de s'assurer de la sécurité, de l'efficacité et de la sûreté d'un système TI lors de sa mise en œuvre et son utilisation. D'autres exigences sécuritaires existent et influencent de plus ou moins près l'utilisation des DMC et logiciels de santé.

II- Etat de l'art autour des exigences sécuritaires sur les DMC et logiciels de santé

A - Obligations réglementaires et normatives sur les services biomédicaux en termes de DMC et logiciels de santé

Juridiquement, le terme connecté renvoie uniquement à l'ajout d'une fonction de communication pour le DM. Cependant les DMC doivent conserver une sécurité et une performance sur tout leur cycle de vie. Pour cette raison, il est nécessaire d'inclure des mises à jour régulières ainsi que des activités de maintenance. Cela peut se faire via l'application d'obligations réglementaires dans les services biomédicaux mais aussi avec des normes facultatives.

Il existe des obligations réglementaires pour les DMs tel que le décret n°2001-1154(5 décembre 2001). Celui-ci met sous la responsabilité des services biomédicaux la maintenance et les contrôles qualité interne et externe des dispositifs médicaux. La difficulté de cibler les familles de dispositifs ainsi que de préciser les contrôles qualité de chaque DM était présente avec ce décret. Pour cette raison, il a été publié l'arrêté du 3 mars 2003 pour résoudre les problématiques précédentes et ainsi proposer un listing des DM concernés par le décret n°2001-1154 [13].

La Haute Autorité de Santé a également élaboré une classification pour les solutions numériques utilisées dans le cadre de soins médicaux. La classification se fait selon 11 catégories de solutions numériques classées en 4 niveaux selon leur finalité d'utilisation. Ce qui aura pour impact de définir qui est responsable des DM connectés et des logiciels de santé. De plus, le DMC devra répondre aux attentes du nouveau règlement européen 2017/745/EU [23]. D'autres règlements pourront intervenir par rapport à la nature du dispositif. Par exemple la directive 2011/65/UE qui s'applique aux équipements électroniques et électriques qui a pour objectif la limitation de substances dangereuses. Il y a également les directives 2014/53/EU et 2006/66/EC qui traitent, respectivement, des équipements radioélectriques et des batteries. La caractéristique première des DMC et logiciels de santé est l'utilisation de données personnelles, il est donc primordial de prendre cette caractéristique en compte, pour cela il est nécessaire de considérer le règlement 2016/679 dit RGPD [54] (Règlement Général sur la Prise en Charge des Données) [14] [15] [16].

Le schéma ci-dessous illustre les réglementations à appliquer dans un service biomédical, avec les réglementations spécifiques aux DM en gris et les réglementations liées aux DMC et logiciels de santé en vert pour les acteurs concernés (DSI et ingénieur biomédical).

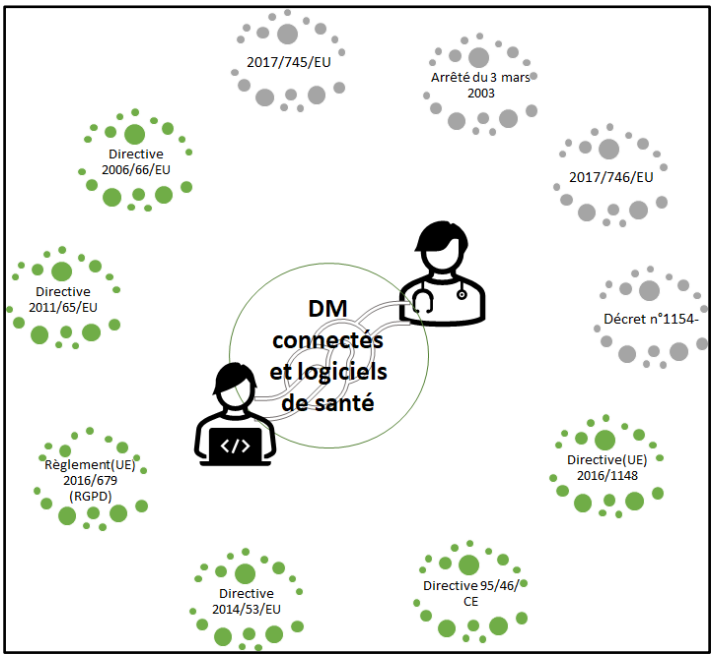

Figure 13 - Réglementation pour les DMC à appliquer dans un service biomédical en coopération avec la DSI (source : auteurs)

En plus de ces obligations réglementaires, il existe également des normes dites volontaires pouvant être appliquées dans un service biomédical et apportant un bénéfice certain aux activités réalisées [17] [18] [19].

- La norme ISO 9001 :2015, système de management de la qualité [46].
- La norme NF S99-170 système de management de la qualité de la maintenance et des risques associés [47].
- La norme NF S99-172, gestion des risques liés à l'exploitation des DM dans les établissements de santé [48].
- Le Guide de Bonnes Pratiques Biomédicales en Établissement de Santé
- La norme ISO 13485, traite des exigences spécifiques aux dispositifs médicaux. Version 2016 adaptée aux services biomédicaux sur les rôles de maintenance et de contrôle qualité [49]
- La norme EN 62304 traite du développement ainsi que de de la maintenance des logiciels DM [50].
- La norme CEI EN 82304-1, assure la sécurité et la sûreté des produits logiciels de santé autonomes [51].
- La norme EN 60601 pour les systèmes électromédicaux basés sur leurs exigences de sécurité et de performance [52]
- La norme ISO 27000 qui se caractérise par la sécurité de l'information.
- La norme ISO/IEC 15408 dont le but est la protection des données en vue de contrôler les divulgations non autorisées d'informations ou encore leurs modifications [53].

Le schéma ci-dessous illustre les normes pouvant être appliquées dans un service biomédical, avec les normes spécifiques aux DM (en bleu) et les normes liées aux DMC (en vert) et logiciels de santé pour les acteurs concernés (DSI et ingénieur biomédical).

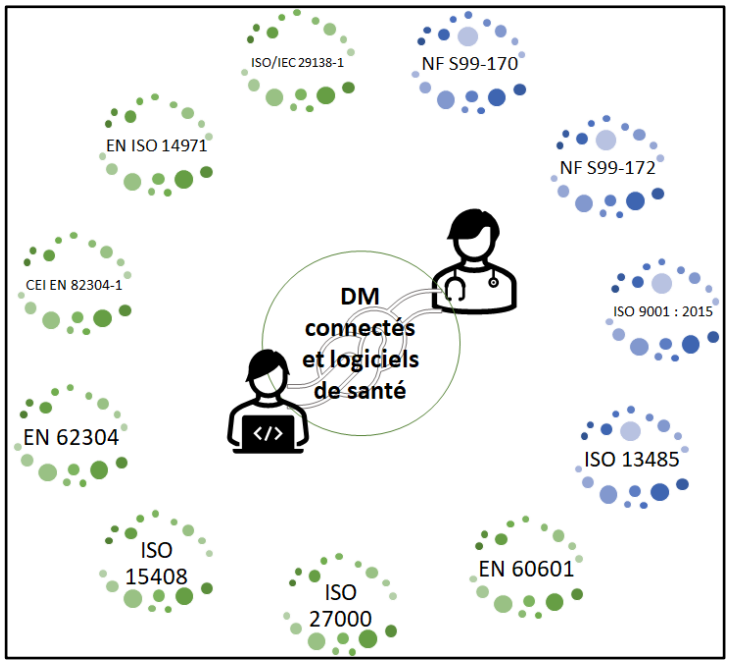

Figure 14 - Normes facultatives pour les DMC pouvant être appliquées dans un service biomédical en coopération avec la DSI (source : auteurs)

Il faudra prendre en compte la nouvelle classification HAS [20] pour les solutions numériques médicales, ce qui aura pour effet de redéfinir les obligations et responsabilités liées au DMC et logiciels de santé. La norme NF EN 80001-1 s'inspire des autres normes sur les DM (par exemple ISO 14971), ce qui aura pour effet de définir les responsabilités au sein des établissements de santé mais aussi de garantir la sécurité, l'efficacité et la sûreté des DMC et logiciels de santé.

B - Généralités sur le management des risques

La norme NF EN 80001-1 reposant sur la sécurité, l'efficacité et la sûreté des DMC et logiciels de santé, il est primordial de s'intéresser au management et à la gestion des risques [21]. En qualité, le risque représente l'effet de l'incertitude sur un résultat escompté [22]. Il peut être de catégories variables en fonction du secteur de l'entreprise : risques d'accident industriel, risque de pollution, risque éthique, risque lié à la santé et la sécurité au travail, risques de non-conformité... Il est dans l'intérêt de tous de les minimiser voire de les éliminer. Afin de les identifier, certains outils de management peuvent être employés comme le SWOT, par exemple. À la suite de l'identification, il est nécessaire de les évaluer puis d'agir dessus.

Ainsi de manière à éviter un risque, des exigences réglementaires peuvent être imposées (règlements) ou suivies volontairement (normes).

Dans un souci de simplification et de manière à renforcer une coordination entre les pays de l'Union Européenne, des Règlements Européens (2017/745 & 2017/746) sont entrés en vigueur en 2017 dans le but de remplacer la directive 90/385/CEE (relative aux dispositifs médicaux implantables actifs) et la directive 93/42/CEE (relative aux autre dispositifs médicaux). Ces nouveaux règlements proposent des renforcements des textes à suivre, avec une augmentation des exigences de sécurité pour les DM les plus à risque, des exigences cliniques, mais aussi une amélioration du suivi et de la surveillance des DM après leur mise sur le marché [23].

Il existe aussi des normes qui donnent et expliquent les ressources nécessaires afin de bien maîtriser les risques. Premièrement la norme ISO 31000 qui affiche les principes et lignes directrices du management du risque est présentée, et qui est utilisable par tout type d'organisme, peu importe la taille et le domaine d'activités [24]. Mais il y a également d'autres normes plus spécifiques comme la norme NF EN ISO 14971 :2019 qui concerne la maîtrise des risques autour des DM à destination du fabricant, ou encore la norme NF S99-172 qui permet de mettre en place un système de management du risque autour des DM à usage de l'exploitant (service biomédical).

Dans le secteur médical, le risque doit être écarté du mieux possible, car la santé du patient en dépend, le cas le plus grave pouvant entraîner la mort de ce dernier. Or, aucun risque sur la santé d'un patient ne peut être pris. Ainsi, le management du risque pour les DMC et logiciels de santé est une activité essentielle qui doit impérativement être adoptée par les organismes concernés.

- **NF EN ISO 14971 :2019 (fabricants)**

Selon cette norme qui s'adresse principalement aux fabricants de l'industrie biomédicale, le risque est défini comme la combinaison de l'occurrence du dommage et de la gravité. Ainsi grâce à une notation sur une échelle préalablement établie, il est possible de créer une matrice d'évaluation du risque. Celle-ci permet alors de classer le risque en le catégorisant d'acceptable à inacceptable. Dans cette gestion des risques, le risque est considéré comme un événement entravant les des tâches spécifiques du processus et non comme est donc considéré comme un risque global empêchant la finalité du processus.

L'objectif final pour un fabricant étant d'atteindre la sécurité à tous les niveaux du processus de fabrication, se caractérisant par l'absence de risque inacceptable.

Cette norme aide donc à la gestion des risques avec tout d'abord une analyse du risque, suivie d'une évaluation du risque, d'un contrôle du risque, et enfin d'un des activités de production et de postproduction [25].

- **NF S99-172 (exploitant)**

La norme NF S99-172, apporte des outils (activités à réaliser, paramètres à contrôler et plans d'actions à instaurer) aux établissements exploitant les DMC afin de les aider à mettre en place un système de management du risque s'améliorant en continue.

Dans les grandes lignes, cette norme permet d'estimer, évaluer et anticiper les risques et potentiels risques mais aussi les opportunités associées au contexte et aux objectifs de l'exploitant, pour ensuite les maîtriser grâce à un système de management du risque puis de vérifier l'efficacité de ce système mis en place.

La finalité globale pour l'exploitant est d'assurer la sécurité du patient en proposant un environnement et une aptitude à fournir des DM, conformes aux exigences du patient et à la réglementation [26].

C - Contexte de la norme 80001

Cette norme est destinée à remplacer la norme homologuée NF EN 80001-1, d'août 2011.

Dans le cadre de cette norme, il est nécessaire de différencier "fabricant" et "exploitant" de dispositifs médicaux connectés (DMC). Le fabricant conçoit et commercialise le DMC qui sera soit directement utilisé par le patient, soit utilisé par l'exploitant, au service des patients.

Selon l'article R5211-5 du Code de la Santé Publique, les exploitants sont toutes les personnes physiques ou morales assurant la responsabilité juridique de l'activité requérant l'utilisation d'un dispositif. "La notion d'exploitation comprend la commercialisation ou la cession à titre gratuit du produit sur le marché français" d'après la LFSS dans l'article L165-1-1-1 du Code de la sécurité sociale.

Les exploitants diffèrent selon l'utilisation du DMC. Dans le cas de notre projet, l'utilisation est exclusive aux établissements de santé. Les exploitants sont donc les services biomédicaux des établissements concernés. En effet, ils sont responsables de l'achat, de l'utilisation dans le respect des conditions définies par le fabricant, et de la maintenance des dispositifs médicaux connectés. Ils font le lien entre le fabricant des DMC et les patients présents en établissement de santé en mettant les DMC à disposition des professionnels de santé.

La norme NF EN 80001-1 recommande qu'avant l'installation d'un DM une gestion des risques soit faite de manière à incorporer celui-ci au mieux dans un réseau TI. Ceci permettrait d'éviter les risques comme ceux pouvant affecter la vie des patients. Pour cela, il faut prendre en compte la suppression, le changement ou la maintenance d'un DMC dans un réseau TI. Les fabricants des DMC devront fournir des informations relatives à l'incorporation d'un DMC dans un réseau TI. Ces informations seront nécessaires à l'organisme responsable pour pouvoir contrôler les risques édictés dans cette norme. Ces documents incluront des données d'accompagnement ainsi que des instructions spécifiques pour la personne responsable. Ce qui permettra de savoir comment le DMC transfère les données sur le réseau TI et la capacité que doit avoir celui-ci pour inclure ce nouveau DM. Les fonctions explicitées dans la norme devront être affectées aux personnes concernées dans les services de santé. Ainsi le service biomédical devra planifier l'incorporation de DM ainsi que gérer les modifications apportées à la suite de leur incorporation. Mais il faudra également prendre en charge la mise en service du réseau TI, son utilisation ainsi que les modifications qui peuvent y être apportées [21].

III - La norme NF EN IEC 80001

A - Le contenu de la norme

La norme NF EN IEC 80001-1 est construite sur deux types d'articles et deux annexes (figure suivante). Les quatre premiers articles sont informatifs, ils permettent de poser les bases de l'application de la norme. Les articles 5 et 6 sont, eux, des articles normatifs, ils explicitent les demandes et exigences de la norme. Enfin, les deux annexes informatives donnent d'autres types d'informations qui pourraient intéresser le lecteur.

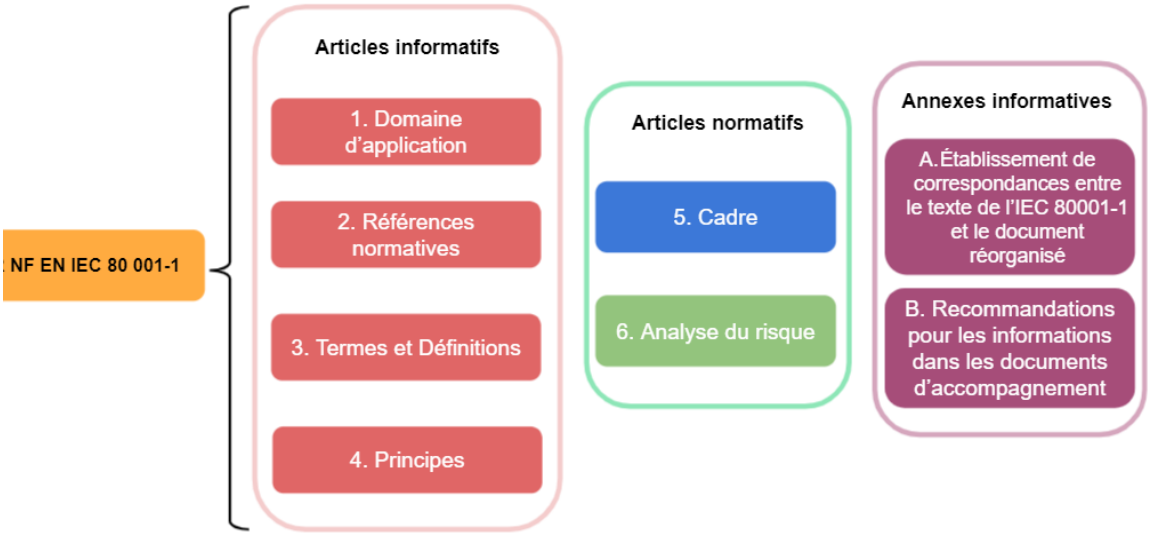

Figure 15 - Organisation de la norme NF EN IEC 80 001-1 (source : auteurs)

Dans les articles 1 à 4, plusieurs éléments sont définis. Tout d'abord, le domaine d'application de la norme, qui correspond à "la gestion des risques avant, pendant et après la connexion d'un système TI de santé au sein d'une infrastructure TI de santé" [21] ainsi que la référence de la norme. Puis, le troisième article explicite les définitions qui semblent essentielles à la bonne compréhension du texte telles que : conséquence, soins de santé, risque initial, vraisemblance, processus, gestionnaire des risques et plan de gestion des risques.

Le quatrième article décerne un certain nombre de principes intrinsèques à la gestion des risques. Ces principes attribuent la valeur, l'objectif et la finalité de la gestion des risques lors de son utilisation dans des systèmes TI de santé au sein d'une infrastructure TI de santé. Le bon respect de ces principes garantit à l'infrastructure la sauvegarde et/ou l'amélioration vérifiables de la sécurité, de l'efficacité et de la sûreté dans la mise en œuvre et l'utilisation des systèmes TI de santé connectés.

Dans les deux articles normatifs seront tout d'abord explicités le cadre puis les exigences pour l'analyse du risque. L'article 5 a donc pour vocation de faciliter l'intégration de la gestion des risques au sein de l'organisation. Cela passe par différents biais :

- ➔ Une sensibilisation de la direction au leadership
- ➔ L'intégration de la gestion des risques à l'ensemble des niveaux de l'organisation
- ➔ La planification de cette gestion des risques au long du cycle de vie du système TI de santé
- ➔ La constitution et le maintien d'un dossier de gestion des risques
- ➔ L'importance du niveau d'allocation de ressource
- ➔ L'utilisation de la communication et de la consultation

- ➔ L'évaluation périodique de la conformité du plan de gestion des risques
- ➔ L'amélioration continue des processus de gestion des risques

Tous ces éléments mettent en place le cadre qui contribue à l'optimisation du respect des exigences de l'analyse des risques de l'article 6. Au sein de cet article, le processus d'analyse des risques est explicité par une série d'éléments :

- ➢ Des exigences générales par :
    - La définition de l'objet et du domaine d'application du processus
    - L'identification et la documentation des dangers par la description d'événements ou conditions susceptibles d'entraîner un dommage.
    - L'estimation du risque par l'utilisation de critères spécifiés dans le plan de gestion des risques pour chaque danger identifié
    - L'évaluation du risque selon leur gravité et leur vraisemblance
    - La maîtrise du risque pour réduire la vraisemblance d'un risque et la gravité d'un danger
    - Une analyse bénéfices-risques pour évaluer l'acceptabilité des risques résiduels associés à un danger
    - La vérification des mesures de maîtrise du risque
    - L'évaluation et le compte-rendu du risque résiduel

- ➢ Les exigences spécifiques au cycle de vie par :
    - Une acquisition des risques
    - Une examination des informations
    - Une analyse des activités et acteurs impliqués
    - Une vérification des activités de gestion des risques
    - Une documentation du processus de gestion des incidents pour évaluer la performance du système TI de santé au long de son utilisation
    - Les conditions de mises hors service d'un système TI de santé

Ainsi, ces deux articles sont le réel contenu exécutif de la norme.

Les annexes, quant à elles, sont à titre informatif. L'annexe A est un tableau mettant en avant l'ensemble des exigences de l'IEC 80001-1 selon chaque article. L'annexe B est un document d'orientation destiné aux organisations souhaitant collaborer avec leurs fournisseurs de systèmes TI de santé pour gérer les risques liés à la mise en œuvre et à l'exploitation des systèmes TI de santé en réseau. "Il vise à donner une vue d'ensemble du système [...] et à fournir des caractéristiques cliniques et opérationnelles [21]."

La norme NF EN IEC 80001-1 concerne une norme d'exigence. Elle contient, seulement dans les articles, un total de 46 fois le mot "doit". Il y a 65 missions/exigences pour l'organisation, 8 pour la direction de l'organisation, 2 pour le gestionnaire des risques du système TI de santé et 32 pour l'organisme responsable.

Cependant, dans cette norme, certains points peuvent être sujet à des problèmes de compréhension s'ils sont mal définis, c'est le cas notamment des acteurs inclus et des documents utilisés.

B - Les acteurs et documents autour de la norme

Pour aider à la compréhension et à la mise en place de la norme 80001-1, il est nécessaire de bien définir les acteurs concernés et les responsabilités qui leur incombent. En effet, cette norme s'adresse aux intervenants impliqués dans l'application de la gestion des risques durant les différentes phases du cycle de vie du système TI de santé, de sa mise en œuvre à son utilisation clinique dans des systèmes ou infrastructures TI de santé. Ces infrastructures sont pourvues de réseaux câblés ou

sans fil avec des échanges et stockage de données qui impliquent une gestion des risques liés à leur utilisation. La norme 80001-1 permet ainsi, de définir les responsabilités de chaque intervenant au cours des différentes phases du cycle de vie du DMC pour en garantir sa sécurité, sa sûreté et son efficacité [21].

Le logigramme suivant permet de suivre le rôle des différents acteurs et les responsabilités qui leurs sont attribuées dans la gestion des risques.

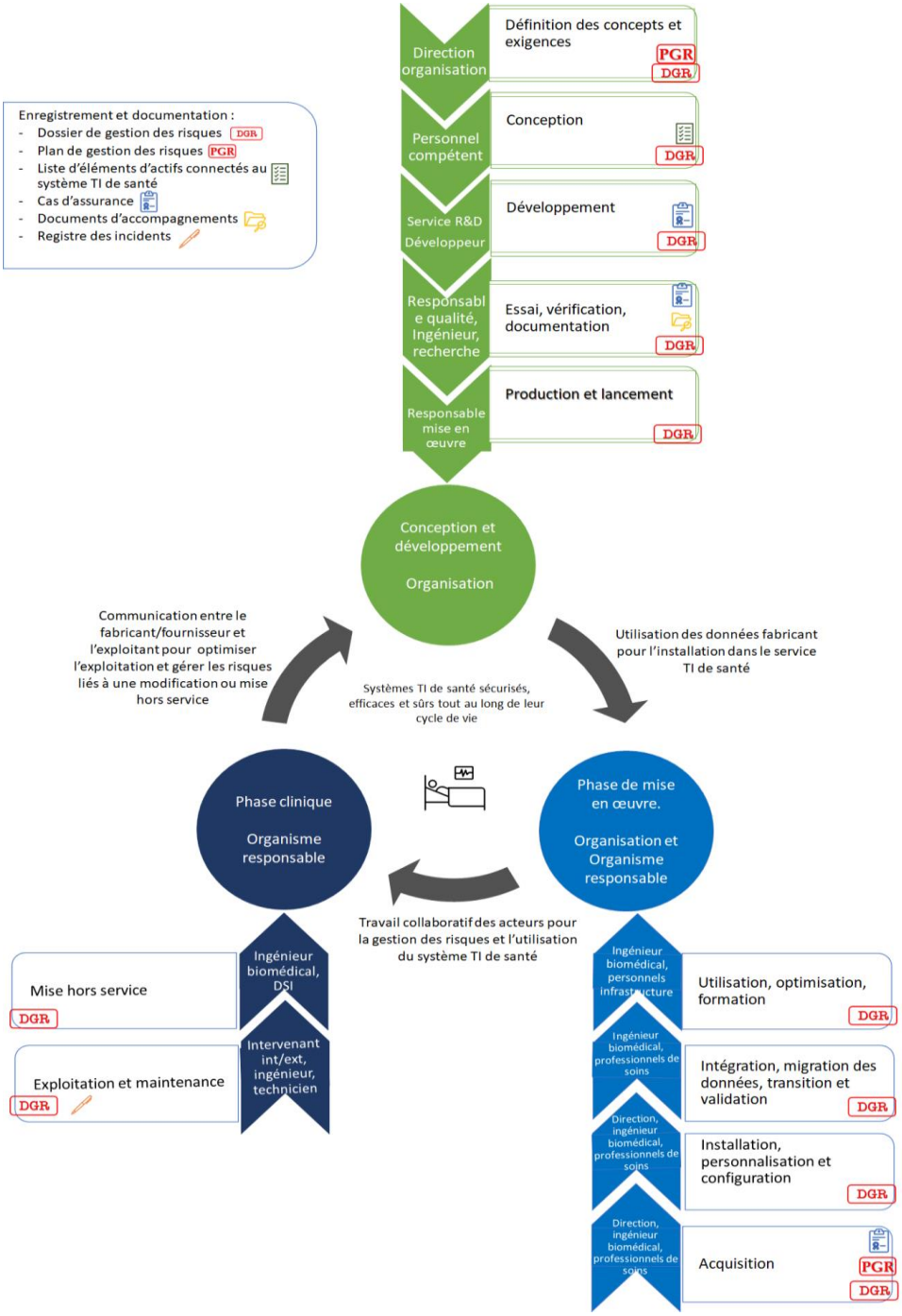

Figure 16 - Acteurs et documents impliqués dans la gestion des risques, tout au long du cycle de vie d'un système TI de santé, selon la norme NF EN 80001-1 (source : auteurs)

Dans un premier temps, il est important de définir ce qu'est l'organisation. Celle-ci représente, dans la norme, les fournisseurs ou encore les fabricants de système TI de santé. Il est important de

relever ce qu'elle doit faire pour améliorer la gestion des risques dans l'utilisation de ses dispositifs. En effet, il incombe aux organisations de maintenir une qualité des dispositifs ainsi que leur amélioration, en prenant en compte les risques relevés au cours de l'utilisation de tels dispositifs chez leurs utilisateurs [21]. En effet, le marquage CE a introduit une conduite de dossier d'acquisition, d'installation, de gestion de maintenance et de gestion de fin de vie que le fabricant doit prendre en compte [43].

Il est également nécessaire de définir le second « intervenant » cité dans la norme, qu'est l'organisme responsable. Celui-ci représente la totalité des acteurs d'une infrastructure (exploitant), de la direction jusqu'à l'utilisateur du dispositif (personnel de l'infrastructure). Cet organisme se décompose ainsi en plusieurs échelons, comme vu dans le logigramme, avec en haut le propriétaire et la direction de l'infrastructure qui attribuent certaines responsabilités à son personnel et le forme à l'utilisation de tels dispositifs ; du responsable de la mise en service et de la gestion des risques (ingénieur biomédical, DSI…) à l'utilisateur (professionnels soignants, intervenants internes…). En effet, le personnel de santé doit prendre conscience des risques et de l'importance de la sécurité numérique dans l'établissement de santé [43].

Par ailleurs, au sein de ces organismes responsables, sont définis pour assurer la qualité, la maintenance et l'amélioration du système TI de santé certains intervenants. Depuis 20 ans, la numérisation s'est développée dans tous les secteurs, il est donc nécessaire d'avoir une vision globale des activités. Ainsi des responsables métiers sont répertoriés, tel que la RSSI qui va définir une sécurité des systèmes informatiques, la direction informatique qui a un rôle d'architecte de la solution informatique pour l'ensemble de l'infrastructure. Ou encore l'ingénieur biomédical qui reste garant de la sécurité du DM et bien d'autres intervenants tels que le responsable médical et du personnel infirmier et le responsable qualité qui joueront un rôle important dans la gestion des risques. [43]

Il est également possible de retrouver des intervenants extérieurs tels que des sociétés externes qui peuvent gérer les contrats de maintenance et les contrôles qualités suivants les réglementations nationales en vigueur. Ou encore des auditeurs externes relevant les risques pouvant survenir lors de l'utilisation de tels dispositifs. Dans ce cas, il est important de consigner les risques liés à ces interventions.

Afin de définir un plan de gestion des risques d'un système TI de santé sûr, efficace et sécurisé, il est nécessaire d'enregistrer et de documenter certaines informations sur l'utilisation de ce système. L'organisation et l'organisme responsable devront ainsi mettre en place des processus de gestion des risques dont les résultats seront consignés dans le DGR en suivant un plan de gestion des risques [21]. Le DGR rassemble donc les informations nécessaires à la gestion des risques. Il sert également à prouver que les activités mises en place respectent les exigences de la norme. Le PGR sert, quant à lui, à la planification de la gestion des risques en y précisant les responsabilités, le domaine d'application et les critères d'acceptabilité des risques.

Par ailleurs, au sein du DGR, se trouve le dossier du cas d'assurance. Ce dernier regroupe les éléments de preuve démontrant que le système TI de santé déployé répond aux critères de sûreté et de sécurité. Il est composé de 3 éléments distincts :

- Un argumentaire structuré
- Un ensemble de preuve
- Une affirmation convaincante et compréhensible

Cependant le cas d'assurance peut également être représenté sous la forme de graphique ou même de tableau. Le tout étant que les informations importantes puissent être repérées et comprises facilement. Les fabricants peuvent passer à travers le dossier du cas d'assurance afin de gérer et communiquer les risques associés à leurs produits au sein de leur entreprise, mais aussi lorsque ces produits sont utilisés par l'exploitant.

L'organisation devra établir dès le début de la conception et maintenir à jour le DGR. Elle y consignera les preuves de l'évaluation de son système TI de santé mais également les résultats d'activité des gestions des risques. Il faudra également y faire figurer un plan de gestion des risques détaillant les activités d'analyse, d'évaluation et de maîtrise de la gestion des risques. Les utilisateurs

et l'utilisation du système en fonction du milieu clinique du déploiement devront également y être inscrits, et seul le personnel formé sera autorisé à utiliser ce matériel après déploiement [43]. Les dangers connus dû au déploiement avec une évaluation du risque initial et résiduel devront également y être consignés. Une liste des éléments actifs connectable au dispositif sera également rédigée par l'organisation pour aider les exploitants, dans l'installation de DMC avec leur système TI de santé déjà en place. L'organisation devra contrôler de manière proactive les propriétés clés de son système après déploiement. Pour cela il devra mettre en place une surveillance de son système lors de son exploitation et devra maintenir une maintenance de son système jusqu'à sa fin de vie, et consigner les incidents éventuels dans le DGR.

Quant à lui, l'organisme responsable définit une échelle de complexité du déploiement et de l'intégration d'un tel DMC. Il pourra recueillir les informations appropriées à l'installation dans sa structure du système, via les documents d'accompagnement des fabricants, de manière à gérer au mieux les risques liés à la personnalisation de son écosystème socio technologique. Il devra également consigner dans le DGR les résultats identifiés et analysés d'activités liées à la gestion des risques. Une analyse bénéfice/risque lié au danger d'utilisation du système sera faite et incorporée au DGR. Les activités et intervenants nécessaire d'impliquer seront identifiés dans un plan global, lui aussi incorporé dans le DGR.

En cas de modification d'un dispositif avec ou sans consentement du fabricant, il devra être confirmé que les modifications sont conformes aux instructions du fabricants ou alors suivre les étapes réglementaires. L'organisme responsable ainsi que l'organisation devront incorporer les résultats de gestion des risques dans le DGR.

Pour faciliter la compréhension des responsabilités des protagonistes et des interactions nécessaires à la bonne conduite de cette norme, la création d'outils est primordiale. En effet, ceux-ci permettront aux utilisateurs de mieux appréhender les rôles et "obligations" de chacun.

C - Les outils d'appropriation de la norme et les méthodes choisies

Analyse normative opérationnelle & cartographie

De manière à faciliter la prise en main de la norme NF EN IEC 80001-1 par ses utilisateurs et afin d'éviter une lecture pesante, plusieurs outils de compréhension et d'utilisation seront déployés.

Tout d'abord, une analyse normative opérationnelle (ANO) sera réalisée de manière à faire ressortir les éléments importants de chaque article. Le processus suivant a été utilisé :

1. Sélectionner une partie du texte normatif
2. Identifier les éléments clefs de l'article normatif
3. Expliciter un objectif synthétique
4. Identifier les documents, leurs types et leur gestion

Pour ce faire, un code couleur permet de catégoriser ces éléments :

- Rouge : Identification d'une exigence avec l'apparition du verbe "devoir"
- Bleu : Identification d'un élément principalement concerné par l'exigence
- Vert : Identification d'une action devant être réalisée
- Violet : Identification d'un élément concerné au conditionnel (ex : Lorsque qu'un, dans le cas où…)
- Orange : Identification d'un acteur principal

A partir de ces éléments, chaque article peut être résumé en une phrase concise, qui sera appelée "objectif". Grâce à cette phrase, le lecteur pourra identifier rapidement le message général de l'article.

L'ANO permet aussi de synthétiser les actions devant être entreprises par les acteurs, mais également de regrouper la documentation intervenant dans l'article.

Grâce à cette ANO il sera possible d'en tirer une cartographie intéractive de la norme. Cette cartographie sera un support facilitant la lecture de la norme en proposant une interface permettant de naviguer entre les différents articles. En voici un exemple :

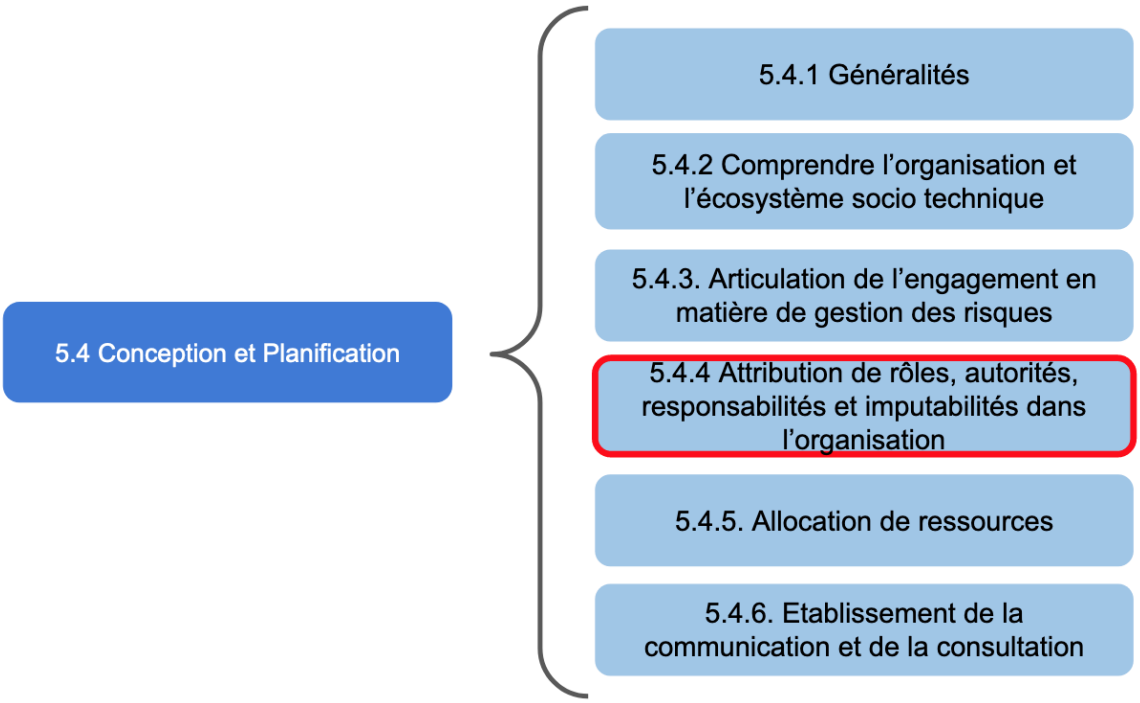

Figure 17 - Plan détaillé du sous article 5.4 "Conception est Planification" (source : auteurs)

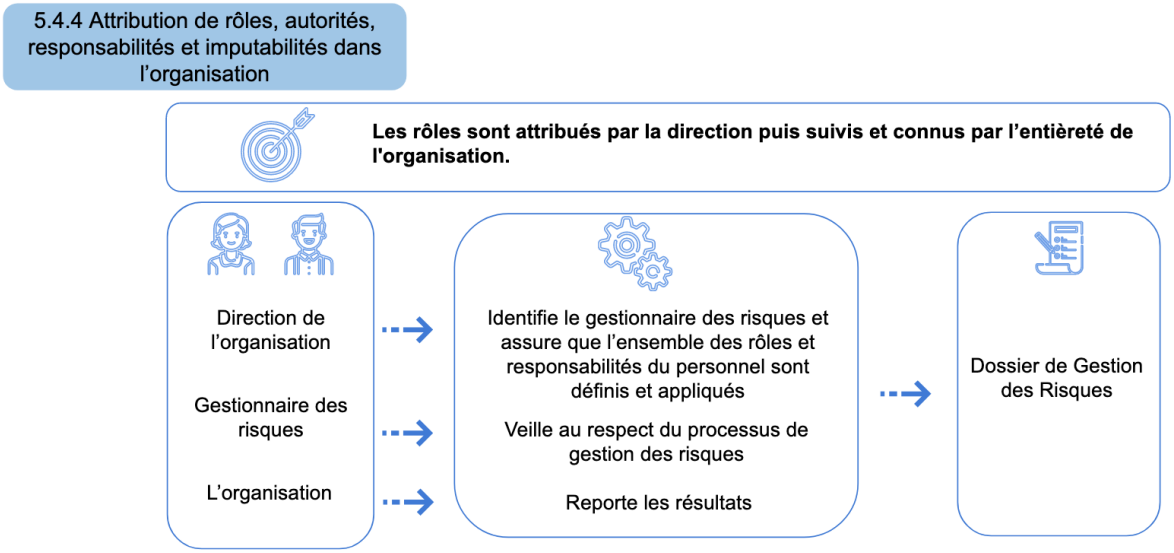

Figure 18 - Détail de l'article 5.4.4 "Attribution des rôles, autorités, responsabilités et imputabilités dans l'organisation" comprenant l'objectif, les acteurs, les actions à réaliser et les documents utilisés (source : auteurs)

Outil d'autodiagnostic et de management

Un outil d'autodiagnostic et de management a également été instauré. Ce dernier est un chaînon fondamental qui va permettre aux établissements de santé comme au fabricant d'évaluer sa conformité à la norme 80001-1 et par conséquent définir les axes d'amélioration à privilégier.

Cet outil d'autodiagnostic et de management se compose de plusieurs parties qui se divisent en plusieurs étapes. Dans un premier temps, un mode d'emploi est proposé où les seules cases modifiables par l'utilisateur sont celles avec un fond blanc et une police bleu vif (dans l'objectif de capter l'attention de l'utilisateur sur les cases modifiables).
Ensuite, il y a la première partie qui consiste à faire une évaluation de la gestion des risques des systèmes TI de santé (DMC et logiciels de santé) en corrélation avec les différents critères de la norme 80001-1.
Comme vue sur la figure X, l'évaluateur doit choisir entre les différents niveaux de véracité conseillés :

- Vrai (Le critère est satisfait)
- Plutôt Vrai (le critère est satisfait, mais des améliorations sont possibles)
- Plutôt Faux (le critère n'est satisfait que partiellement)
- Faux (le critère n'est pas satisfait du tout)
- Non-Applicable (non comptabilisé mais à justifier)

Autodiagnostic selon la norme NF EN IEC 80001-1

Attention : Seules les cases blanches écrites en bleu peuvent être modifiées par l'utilisateur. Cela concerne toutes les parties de l'outil

Etablissement :	**Nom de l'établissement**	
Date de l'autodiagnostic :	Date de l'autodiagnostic	Signature.s animateur.s de l'autodiagnostic
Animation de l'autodiagnostic :	NUMS et Prenom.s animateur.s de l'autodiagnostic	
Email :	Email.s animateur.s	
Tél :	Tél animateur.s	
L'équipe d'autodiagnostic :	NOMS et Prénoms des participants à l'autodiagnostic	

Réf.	Critères d'exigence des articles de la norme	Evaluations	%	Libellés des évaluations	Références des documents, modes de preuve et commentaires
Tous les Articles de la norme :					
Art. 5	**Cadre**		**62%**	Conformité de niveau 3 : Des améliorations peuvent encore être apportées.	**Probant**
5.1	**Généralités**	**Probant**	**57%**	**Conformité de niveau 3 : Des améliorations peuvent encore**	
cr 1	Tous les intervenants et la direction prennent en compte le cadre de la gestion des risques et l'intègrent à d'autres activités et fonctions importantes.	Plutôt Vrai	57%	Niveau 4 : Le critère est formalisé et réalisé de manière assez convaincante	
5.2	**Leadership et engagement**	**Maîtrisé**	**77%**	**Conformité de niveau 4 : Tracez vos activités et prouvez vos résultats pour mieux progresser.**	
cr 2	La gestion des risques est assurée et évaluée tout au long du cycle de vie du système des technologies de l'information (TI) de santé.	Vrai	77%	Niveau 5 : Le critère est suivi et amélioré dans sa mise en œuvre	...
5.3	**Intégration de la gestion des risques**	**Insuffisant**	**12%**	**Conformité de niveau 1 : Revoyez le fonctionnement de vos activités.**	
cr 3	La gestion des risques concerne tous les niveaux et tous les membres d'une organisation(fabricants).	Faux	12%	Niveau 2 : Le critère n'est pas réalisé ou alors de manière très aléatoire	...

Figure 19 - Outil d'autodiagnostic : Evaluation (source : auteurs)

Ainsi, cette étape d'évaluation va permettre d'obtenir des **résultats globaux** qui vont déterminer des axes d'amélioration. Cette partie est composée de 2 sous-parties, l'une qui détermine les niveaux de conformité et la véracité selon la norme 80001-1 (voir figure X ci-dessous).

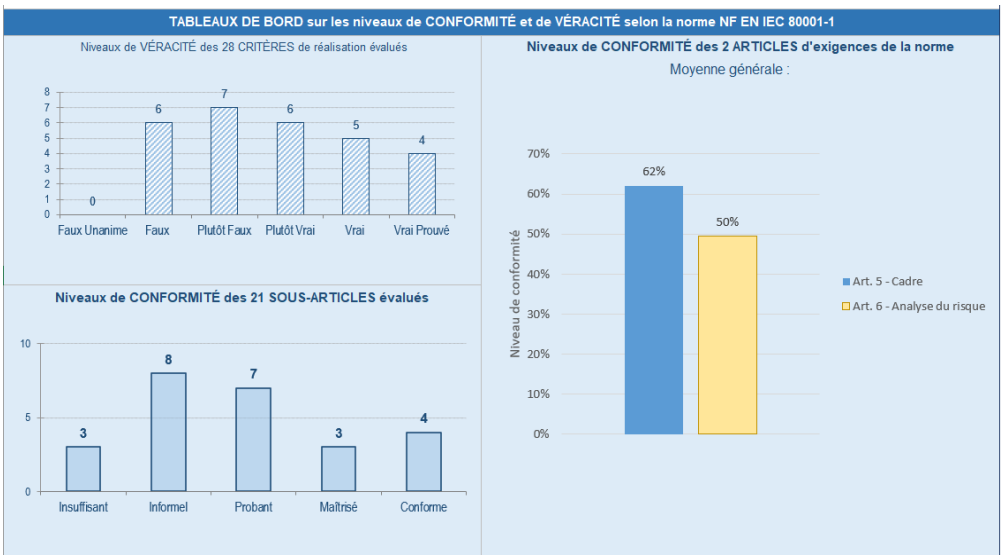

Figure 20 - Résultats globaux : Tableaux de bord (source : auteurs)

L'autre qui détermine un bilan global avec des commentaires sur les résultats obtenus et des plans d'actions prioritaires (Quoi/Qui/Quand et où) (Voir figure X ci-dessous).

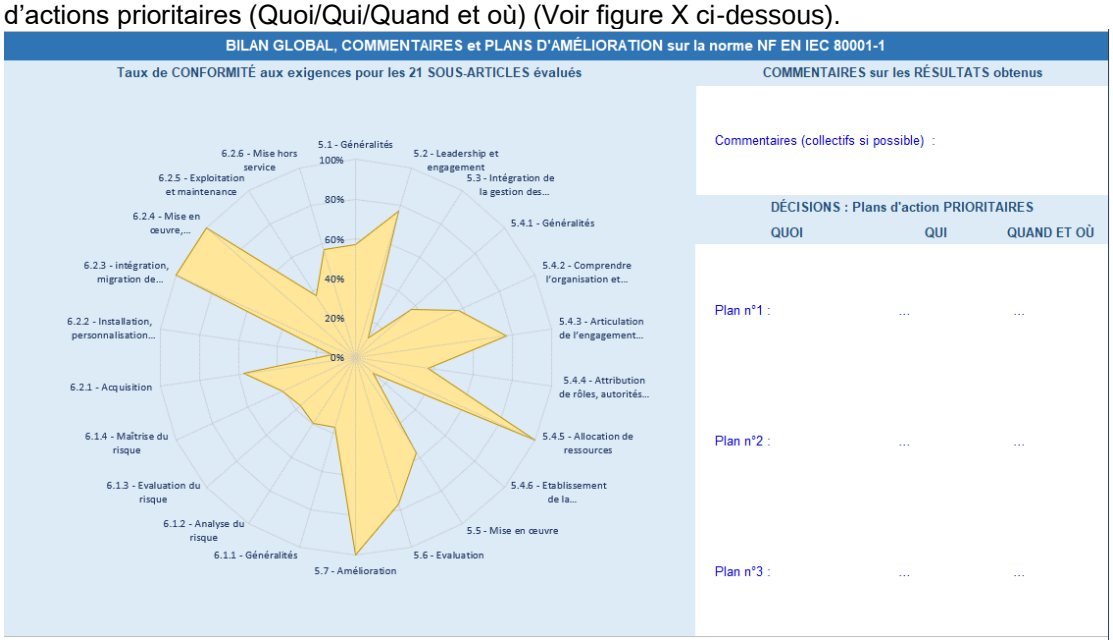

Figure 21 - Résultats globaux : Bilan global, commentaires et plans d'amélioration (source : auteurs)

Ils seront plus détaillés dans les **résultats par article** pour avoir une vue plus précise des actions qui peuvent être mises en place.

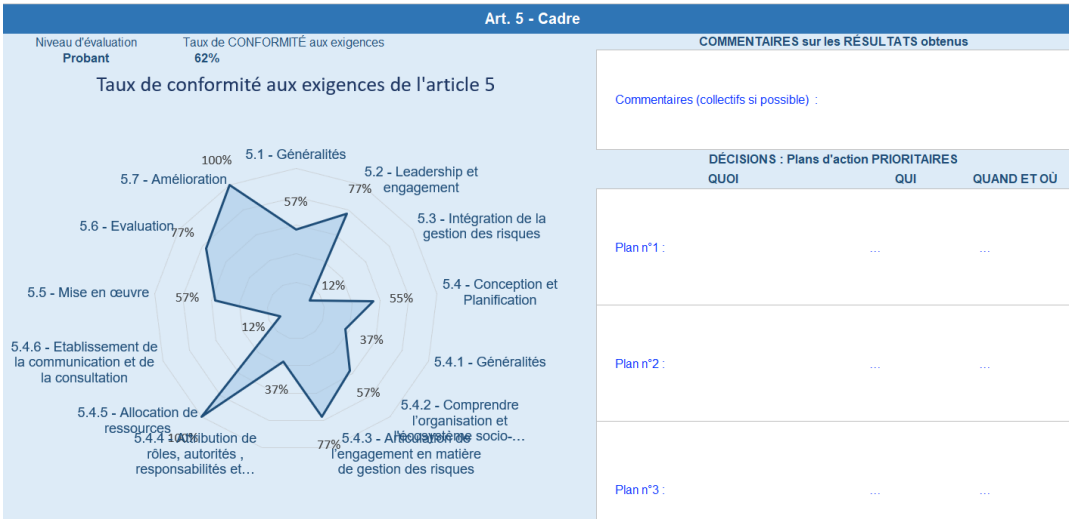

Figure 22 - Résultats par article (exemple de l'article 5 de la norme 80001-1)(source : auteurs)

Rattaché à ces résultats globaux et par article, une **maîtrise documentaire** est proposée aux utilisateurs (Organisation et organisme responsable) de l'outil pour permettre de faire un point sur les documents nécessaires et manquants lors de cette analyse de la gestion des risques.

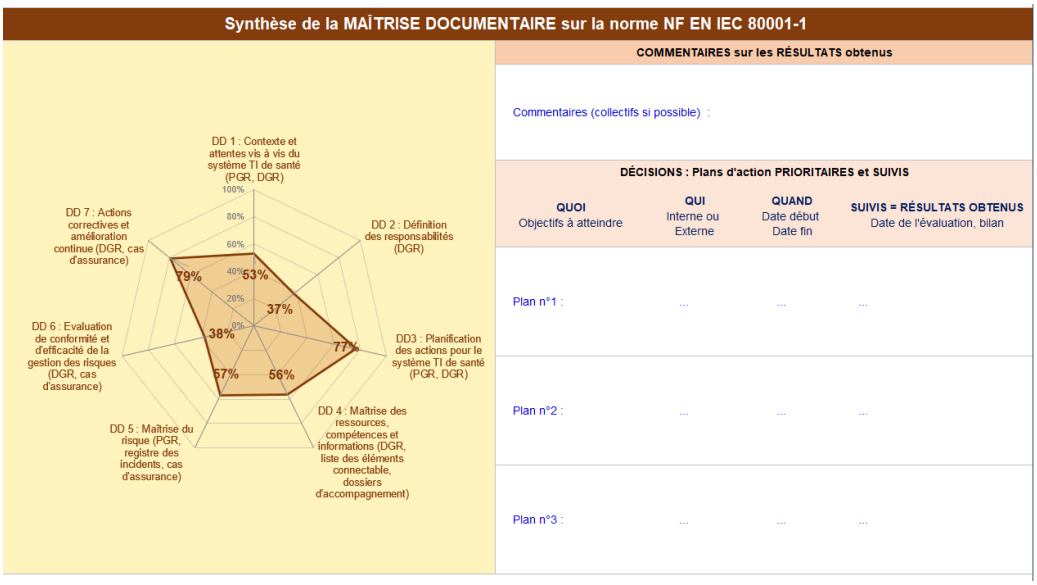

Figure 23 - Synthèse de la maîtrise documentaire (source : auteurs)

MAÎTRISE DOCUMENTAIRE sur la norme NF EN IEC 80001-1 : détail des dossiers et des critères associés						
Maîtrise estimée des Dossiers documentaires (DD)				Critères utilisés pour chaque dossier		
Dossiers documentaires (DD)	Libellé interne au Service Biomédical	Evaluation sur la docuentation		Moyenne des évaluations	Critères associés	Articles associés
DD 1 : Contexte et attentes vis à vis du système TI de santé (PGR, DGR)		Incomplet	Consolider la rédaction : des éléments sont manquants	53%	1, 2, 3, 4, 5, 6	5.1, 5.2, 5.3, 5.4
DD 2 : Définition des responsabilités (DGR)		Très incomplet	Améliorer la rédaction : revoyez le contenu du document	37%	7	5.4
DD3 : Planification des actions pour le système TI de santé (PGR, DGR)		Presque Complet	Finaliser la rédaction : des améliorations peuvent être apportées	77%	6	5.4
DD 4 : Maîtrise des ressources, compétences et informations (DGR, liste des éléments connectable, dossiers d'accompagnement)		Incomplet	Consolider la rédaction : des éléments sont manquants	56%	8, 9, 10, 15, 23, 26	5.4, 5.5, 6.1, 6.2
DD 5 : Maîtrise du risque (PGR, registre des incidents, cas d'assurance)		Incomplet	Consolider la rédaction : des éléments sont manquants	57%	10, 13, 14, 16, 18, 25, 26, 28	5.5, 6.1, 6.2
DD 6 : Evaluation de conformité et d'efficacité de la gestion des risques (DGR, cas d'assurance)		Très incomplet	Améliorer la rédaction : revoyez le contenu du document	38%	11, 15, 19, 20, 21, 22, 24, 27	5.6, 6.1, 6.2
DD 7 : Actions correctives et amélioration continue (DGR, cas d'assurance)		Presque Complet	Finaliser la rédaction : des améliorations peuvent être apportées	79%	12, 18, 28	5.7, 6.1, 6. 2

Figure 24 - Maîtrise documentaire : détails des dossiers et des critères associés (source : auteurs)

Pour organiser au mieux cet outil de diagnostic, une **cartographie des processus** est présente dans l'outil pour pouvoir se repérer (voir figure ci-dessous).

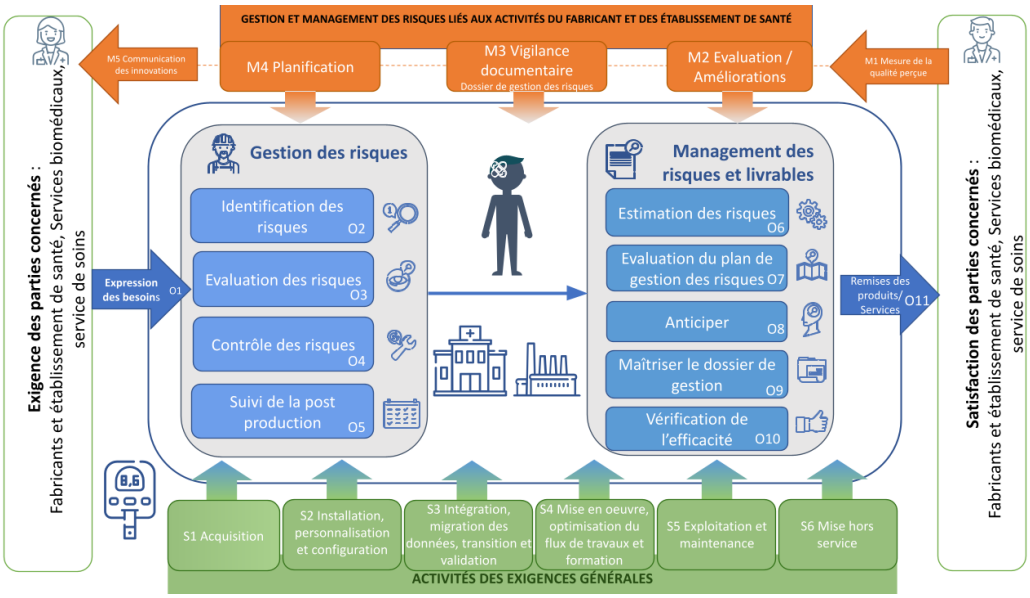

Figure 25 - Cartographie des processus de la gestion des risques selon la norme 80001-1 (source : auteurs)

Cet outil de diagnostic et de management a pour objectif d'évaluer le taux de conformité des nouvelles mesures mises en place par un organisme, et ainsi donner des indications sur les secteurs maîtrisés et moins maîtrisés. Un tel rapport permettra de revoir la stratégie mise en place dans cet organisme.

Conclusion

Dans un environnement relativement complexe, les DMC et les logiciels de santé sont donc d'un apport considérable à la médecine contemporaine. Les nombreux projets et applications nous poussent à considérer ces entités comme de plus en plus présentes dans le milieu professionnel et peuvent apporter leurs lots d'espoir pour une plus grande efficacité de traitement voir même la découverte de nouveaux types de traitements.

Néanmoins, comme explicité lors de ce mémoire, il est important de garder une certaine prudence vis-à-vis de leurs utilisations et de leurs créations. En effet, la gestion et le management des risques sont de rigueur si l'on se réfère aux enjeux exposés plus tôt et aux problèmes qui ont pu advenir dans le passé. Le bien-être du patient demande aux fabricants et aux exploitants un maximum d'attention et de prévention.

Bien au courant de ces enjeux, les administrations, les dirigeants ainsi que d'autres acteurs ont pris certaines mesures et continuent de s'adapter progressivement à un monde technologique qui avance vite. Les normes, directives et règlements s'attachant à la sécurité des DMC et des logiciels de santé ont ainsi pu être répertoriées.

Lors de notre deuxième partie de mémoire, les termes et définitions de la norme étant définis, il a été nécessaire de comprendre et d'appréhender la norme point par point. C'est pourquoi, la mise en œuvre de l'ANO puis d'une cartographie a vu le jour sous le soleil du jalon 2. En se basant sur les données récoltées puis analysées, d'autres outils (autodiagnostic et questionnaire) ont été spécifiés en tout état de cause pour concevoir et intégrer la norme NF EN IEC 80001-1 chez les organisations et les organismes responsables (fabricants, établissements de santé, etc…).

Par ailleurs, la place du patient au sein de ce projet a pu être redéfinie à plusieurs reprises, de manière à garder le cap sur l'objectif principal de la norme, concernant la gestion des risques des DMC et logiciel de santé pour la santé du patient.

Dans ce dernier jalon, les différentes compétences de chacun mises en œuvre ont permis de mettre en place un outil d'autodiagnostic adapté à la norme NF EN IEC 80001-1. Un travail d'équipe constant et sans faille a permis de proposer un outil utile (pour les établissements de santé mais aussi pour les fabricants), utilisé (pour les dispositifs médicaux connectés et logiciels de santé) et utilisable (grâce à l'outil d'autodiagnostic).

La pérennisation de ce projet dans le temps est une perspective intéressante, c'est pourquoi un questionnaire a été créé, initialement dédiée à la création des outils, mais qui a été remanié pour prendre en compte les axes d'améliorations.

Bibliographie

[1] HAS, « E-santé », *Haute Autorité de Santé*, nov. 07, 2016. https://www.has- sante.fr/jcms/c_2056029/en/e-sante (consulté le oct. 11, 2021).

[2] G. Morisse & al., « Dispositifs médicaux connectés : des opportunités florissantes pour de meilleurs soins de santé (2ème partie) », *Quantmetry*, mars 23, 2021. https://www.quantmetry.com/blog/dispositifs-medicaux-connectes-soins-sante-2/ (consulté le oct. 11, 2021).

[3] HAS, « Travaux sur les spécificités méthodologiques d'évaluation clinique des Dispositifs Médicaux Connectés », *HAS*, avr. 2018, [En ligne]. Disponible sur: https://www.has-sante.fr/upload/docs/application/pdf/2018-04/travaux_sur_les_specificites_methodologiques_devaluation_clinique_des_dispositifs_medicaux_connectes_feuille_de_route.pdf

[4] ANSM, « Logiciels et applications mobiles en santé - ANSM », mai 25, 2021. 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 (consulté le oct. 11, 2021).

[5] institut Montaigne, « E-santé : augmentons la dose ! », juin 2020, Consulté le: oct. 10, 2021. [En ligne]. Disponible sur: https://www.institutmontaigne.org/ressources/pdfs/publications/e-sante-augmentons-la-dose-annexe-chiffrage.pdf

[6] Iremos, « Qu'est-ce que la sûreté ? » https://www.iremos.fr/blog/qu-est-ce-que-la-surete-acte- malveillance (consulté le oct. 12, 2021).

[7] « Efficacité », *Wikipédia*. mai 19, 2021. Consulté le: oct. 12, 2021. [En ligne]. Disponible sur: https://fr.wikipedia.org/w/index.php?title=Efficacit%C3%A9&oldid=183048589

[8] ANSM, « Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie », Recommandations ANSM, juill. 2019. [En ligne]. Disponible sur: http://www.specialitesmedicales.org/offres/doc_inline_src/666/ANSM%2B-%2BCybersecurite_Recommandations-Fr.pdf

[9] « Cyberveille Santé | Accompagnement Cybersécurité des Structures de Santé », 2021. https://www.cyberveille-sante.gouv.fr/cyberveille-sante (consulté le oct. 11, 2021).

[10] K. Wellington, « Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions », *Santa Clara High Technology Law Journal*, vol. 30, n° 2, Art. n° 2, janv. 2013.

[11] M. Ward, « Warning over medical implant attacks - BBC News », avr. 10, 2012. https://www.bbc.co.uk/news/technology-17623948 (consulté le oct. 11, 2021).

[12] Danny Bradbury, « 4 Ways Johnson & Johnson Is Leading the Fight Against Cyberattackers », *Content Lab U.S.*, oct. 08, 2017. https://www.jnj.com/innovation/johnson-and-johnson-leading-fight-to-prevent-cyberattacks (consulté le oct. 11, 2021).

[13] « Maintenance et contrôle qualité des dispositifs médicaux - ANSM », oct. 02, 2021. https://ansm.sante.fr/documents/reference/maintenance-et-controle-qualite-des-dispositifs-medicaux (consulté le oct. 02, 2021).

[14] Parlement européen et du Conseil, « Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux », 2017/745, 2017. [En ligne]. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017R0745

[15] M. Navarro, « Classification des logiciels (de) dispositifs médicaux (A, B, C…) », *mauricenavarro.com*, déc. 28, 2019. https://www.mauricenavarro.com/articles/classification-des-logiciels-de-dispositifs-medicaux-A-B-C/ (consulté le oct. 11, 2021).

[16] M. Navarro, « Réglementation et normes applicables aux logiciels de santé », *mauricenavarro.com*, avr. 30, 2021. https://www.mauricenavarro.com/articles/reglementation-et-normes-applicables-aux-logiciels-de-sante/ (consulté le oct. 06, 2021).

[17] M. Navarro, « Normes applicables aux logiciels (de) dispositifs médicaux », *mauricenavarro.com*, juill. 02, 2018. https://www.mauricenavarro.com/articles/normes-applicables-aux-logiciels-de-dispositifs-medicaux/ (consulté le oct. 10, 2021).

[18] G. P. F. de Q. • E. dispositifs médicaux et gestion des risques • A. norme X. S99-223, « Les normes applicables aux Dispositifs Médicaux », *Qualitiso*, sept. 04, 2014. https://www.qualitiso.com/normes-dispositif-medical/ (consulté le oct. 11, 2021).

[19] M. Navarro, « Norme CEI EN 82304-1 pour logiciel dispositif médical (DM ou DMDIV) », *mauricenavarro.com*, sept. 19, 2019. https://www.mauricenavarro.com/articles/norme-cei-en-82304-1-pour-logiciel-dispositif-medical-dm-ou-dmdiv/ (consulté le oct. 06, 2021).

[20] Morgane Morey et Béatrice Espesson-Vergeat, « Dispositifs médicaux connectés – nouveau guide de la HAS », *Fidal*, févr. 27, 2019. https://www.fidal.com/fr/actualites/dispositifs-medicaux-connectes-nouveau-guide-de-la-has (consulté le oct. 02, 2021).

[21] AFNOR, « NF EN IEC 80001-1 : Maîtrise des risques des logiciels de santé et DM connectés ». sept. 16, 2021. [En ligne]. Disponible sur: https://www.iso.org/fr/standard/72026.html

[22] « Définition Risque qualité - Qualité ISO 9001 », *Certification QSE*, janv. 05, 2017. https://www.certification-qse.com/definition-risque-qualite-qualite-iso-9001/ (consulté le oct. 11, 2021).

[23] « RÈGLEMENT (UE) 2017/ 745 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux, modifiant la directive 2001/ 83/ CE, le règlement (CE) no 178/ 2002 et le règlement (CE) no 1223/ 2009 et abrogeant les directives du Conseil 90/ 385/ CEE et 93/ 42/ CEE », p. 175.

[24] « ISO - ISO 31000 — Management du risque », *ISO*, oct. 11, 2021. https://www.iso.org/fr/iso-31000-risk-management.html (consulté le oct. 11, 2021).

[25] Carolina MACEDO & al., « IDS072 - Le management du risque des dispositifs médicaux selon la norme NF S99-172 :2017 », *Bibliothèque des travaux Master*, 2021 2020. https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids072/ (consulté le oct. 11, 2021).

[26] « NF S99-172 (février 2017) Exploitation et maintenance des dispositifs médicaux – Système de management du risque lié à l'exploitation des dispositifs médicaux - Bivi - Qualite », févr. 2017. https://bivimetrologie.afnor.org/notice-details/nf-s99-172-fevrier-2017-exploitation-et-maintenance-des-dispositifs-medicaux-systeme-de-management-du-risque/1305754 (consulté le oct. 11, 2021).

[27] Pierre-Emmanuel De Joannis et al., « Cybersécurité des dispositifs médicaux : point sur la menace réelle et role du corps médical », *Revue Medicale Suisse*, oct. 19, 2016. https://www.revmed.ch/revue-medicale-suisse/2016/revue-medicale-suisse-535/cybersecurite-des-dispositifs-medicaux-point-sur-la-menace-reelle-et-role-du-corps-medical (consulté le oct. 05, 2021).

[28] ISO/TC 215, « IEC 82304-1:2016 : Logiciels de santé - Partie 1 : Exigences générales pour la sécurité des produits ». oct. 2016. [En ligne]. Disponible sur: https://www.iso.org/fr/standard/59543.html

[29] « IEC 62304:2006 Logiciels de dispositifs médicaux — Processus du cycle de vie du logiciel ». Organisation Internationale de normalisation, revue en 2015 2006. [En ligne]. Disponible sur: https://www.iso.org/fr/standard/38421.html

[30] L. Cambon, « Objets connectés, mobiles, communicants en prévention : dépasser l'outil, penser l'intervention… », *Sante Publique*, vol. Vol. 28, nº 1, Art. nº 1, avr. 2016.

[31] « AZMed ». https://azmed.co/ (consulté le nov. 04, 2021).

[32] « Santé connectée : les 4 chiffres qu'il faut connaître », *Microsoft experiences*, juill. 19, 2017. https://experiences.microsoft.fr/business/intelligence-artificielle-ia-business/sante-connectee-chiffres/ (consulté le nov. 04, 2021).

[33] P. F. Soyez @FabienSoyez et M. à jour le mardi 03 décembre 2019 à 17:00, « Vendre ses données de santé, ça coûte combien ? », *CNET France*. https://www.cnetfrance.fr/news/vendre-ses-donnees-de-sante-ca-coute-combien-39895205.htm (consulté le nov. 04, 2021).

[34] xerfi, « E-santé : perspectives pour le marché des systèmes d'information de santé ». https://www.xerfi.com/presentationetude/E-sante-perspectives-pour-le-marche-des-systemes-d-information-de-sante_20CHE49 (consulté le nov. 04, 2021).

[35] Larousse, « Définitions : risque - Dictionnaire de français Larousse », nov. 04, 2021. https://www.larousse.fr/dictionnaires/francais/risque/69557 (consulté le nov. 04, 2021).

[36] C. canadien d'hygiène et de sécurité au travail Gouvernement du Canada, « Danger et risque : Réponses SST », oct. 27, 2021. https://www.cchst.ca/oshanswers/hsprograms/hazard_risk.html (consulté le nov. 04, 2021).

[37] RENARD Patrick, « Stratégies de test de fabrication pour les dispositifs médicaux connectés », *DeviceMed.fr*, oct. 29, 2021. https://www.devicemed.fr/dossiers/equipements-de-production-et-techniques-de-fabrication/metrologie_controle/strategies-de-test-de-fabrication-pour-les-dispositifs-medicaux-connectes/28878 (consulté le nov. 04, 2021).

[38] Affairs et Office of Regulatory, « Medtronic Announces Worldwide Voluntary Field Corrective Action for Newport™ HT70 and Newport™ HT70 Plus Ventilators », *U.S. Food and Drug Administration*, juill. 20, 2020. https://www.fda.gov/safety/recalls-market-withdrawals-safety-alerts/medtronic-announces-worldwide-voluntary-field-corrective-action-newporttm-ht70-and-newporttm-ht70 (consulté le nov. 04, 2021).

[39] « Risque d'erreur dans l'attribution d'un dossier patient sur le logiciel ARIA® Oncology Information System v 15.5 | Accompagnement Cybersécurité des Structures de Santé », nov. 04, 2021. https://www.cyberveille-sante.gouv.fr/alertes/1129-risque-derreur-dans-lattribution-dun-dossier-patient-sur-le-logiciel-ariar-oncology (consulté le nov. 04, 2021).

[40] Haute Autorité de Santé, « Consultation publique sur le projet de grille d'analyse destinée à être utilisée par la CNEDiMTS pour contribuer à son évaluation de dispositifs médicaux embarquant des systèmes décisionnels s'appuyant sur des procédés d'apprentissage automatique (« Intelligence artificielle ») ». nov. 20, 2019. [En ligne]. Disponible sur: https://www.has-sante.fr/upload/docs/application/pdf/2019-11/notice_consultation_algorithmes.pdf

[41] Haute Autorité de Santé, « Guide sur les spécificités d'évaluation clinique d'un dispositif médical connecté (DMC) en vue de son accès au remboursement ». janv. 2019. [En ligne]. Disponible sur: https://www.has-sante.fr/upload/docs/application/pdf/2019-02/guide_sur_les_specificites_devaluation_clinique_dun_dmc_en_vue_de_son_acces_au_remboursement.pdf

[42] HAS, « Avis de la CNEDiMTS sur le capteur de pression Cardiomems ». avr. 27, 2021. [En ligne]. Disponible sur: https://www.has-sante.fr/upload/docs/evamed/CNEDIMTS-6376_CARDIOMEMS_27_avril_2021_(6376)_avis.pdf

[43] « AFIB, Association Française des Ingénieurs Biomédicaux ». https://www.afib.asso.fr/ (consulté le sept. 11, 2020).

[44] « Claria MRI™ - CRT-D by Medtronic | MedicalExpo », nov. 04, 2021. https://www.medicalexpo.fr/prod/medtronic/product-70691-791458.html (consulté le nov. 04, 2021).

[45] Haute Autorité de Santé, « Avis de la CNEDiMTS sur le stimulateur Brio ». déc. 01, 2020. [En ligne]. Disponible sur: https://www.has-sante.fr/upload/docs/evamed/CNEDIMTS-6087_BRIO_1er_d%C3%A9cembre_2020_(6087)_avis.pdf

[46] « ISO 9001 :2015 », *ISO*. https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/06/20/62085.html (consulté le nov. 03, 2021).

[47] « Certification AFAQ Maintenance des dispositifs médicaux ». https://certification.afnor.org/divers/certification-nf-s99-170-maintenance-des-dispositifs-medicaux (consulté le nov. 03, 2021).

[48] « norme NF S99-172 Exploitation des dispositifs médicaux - Gestion des risques liés à l'exploitation des dispositifs médicaux dans les établissements de santé (annulée en février 2017) », Ed. Afnor, Paris, www.afnor.org, sept. 01, 2003. [En ligne]. Disponible sur: https://sagaweb-afnor-org.ezproxy.utc.fr/fr-FR/sw/Consultation/Notice/1273927/

[49] L. Beuzelin et al., « Accompagnement à la certification ISO 13485 : 2016 », *IRBM News*, vol. 39, nº 2, p. 57-61, avr. 2018, doi: https://doi.org/10.1016/j.irbmnw.2018.02.002.

[50] « IEC 62304:2006 Logiciels de dispositifs médicaux — Processus du cycle de vie du logiciel ». Organisation Internationale de normalisation, revue en 2015 2006. [En ligne]. Disponible sur: https://www.iso.org/fr/standard/38421.html

[51] ISO/TC 215, « IEC 82304-1:2016 : Logiciels de santé - Partie 1 : Exigences générales pour la sécurité des produits ». oct. 2016. [En ligne]. Disponible sur: https://www.iso.org/fr/standard/59543.html

[52] « norme NF EN 60601-1 Appareils électromédicaux - Partie 1 : exigences générales pour la sécurité de base et les performances essentielles (Tirage 5 (2014-09-01)) », Ed. Afnor, Paris, www.afnor.org, janv. 01, 2007. [En ligne]. Disponible sur: https://sagaweb-afnor-org.ezproxy.utc.fr/fr-FR/sw/consultation/notice/1274667?recordfromsearch=True

[53] « ISO/IEC-15408-1:2009 », *ISO*. https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/05/03/50341.html (consulté le nov. 03, 2021).

[54] « RÈGLEMENT (UE) 2016/ 679 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 27 avril 2016 - relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/ 46/ CE (règlement général sur la protection des données) », p. 88.