Pre-print en diffusion libre autorisée
Publication consultable ici : https://doi.org/10.1016/j.irbmnw.2024.100540

Protéger le parc des dispositifs médicaux connectés et l'intégrité physique des patients face aux cyberattaques : des outils pour les équipes biomédicales

Barbier Benoît[a], Robin Thomas[a], Follet Julie[b]

[a] Master Ingénierie de la santé, Département Génie Biologique, Université de Technologie de Compiègne, rue du Docteur Schweitzer, CS 60319, 60203 Compiègne Cedex, France.

[b] Département Génie Biologique, Université de Technologie de Compiègne, rue du Docteur Schweitzer, CS 60319, 60203 Compiègne Cedex, France ; auteur correspondant : julie.follet@utc.fr

Les auteurs déclarent n'avoir aucun lien d'intérêt en relation avec cet article.

Résumé

La numérisation croissante des systèmes d'information des établissements de santé a ouvert de nouvelles voies pour l'amélioration des soins. Cependant, cette avancée technologique s'accompagne d'un défi majeur : garantir la sécurité des soins en contexte de cyberattaques hebdomadaires. A cet effet, la protection des données médicales sensibles, la préservation de l'intégrité des systèmes informatiques, et la garantie du bon fonctionnement des équipements biomédicaux sont des impératifs cruciaux. Face à l'émergence des risques cyber, il est nécessaire d'outiller les ingénieurs biomédicaux dans la prévention des cyberattaques.

En s'appuyant sur les travaux du groupe de travail dédié à la "sécurité numérique des équipements biomédicaux" de l'Association Française des Ingénieurs Biomédicaux publiés en 2021, quatre outils ont été élaborés pour définir les modalités de collaboration entre professionnels biomédicaux et des systèmes informatiques au sein des établissements de santé, sécuriser l'environnement des équipements biomédicaux, favoriser l'intégration de la sécurité numérique dans les procédures d'achat de tels équipements, et évaluer leur criticité.

Les outils proposés ont fait l'objet de tests auprès d'ingénieurs biomédicaux pour vérifier leur adéquation aux besoins de la communauté biomédicale et dégager des perspectives d'évolution.

Mots-clés

AFIB, cybersécurité, prévention, dispositifs médicaux, procédure d'achat.

1. Introduction

En 2023, 581 incidents de cybersécurité ont été déclarés par les établissements de santé français, contre 592 en 2022, et 733 en 2021. Bien que le nombre d'incidents ait diminué, le nombre d'établissements de santé déclarants est en constante augmentation avec 467 structures en 2023, contre 432 en 2022, et 290 en 2021, témoignant d'une menace croissante (1,2). Sur l'ensemble des incidents déclarés en 2023, 27% sont issus d'attaques par *phishing* (envoi d'un mail frauduleux dont les liens hypertextes servent à récupérer les informations personnelles de la victime), et plus de 5% par l'utilisation de rançongiciels ou *ransomwares* (qui chiffrent les données et les fichiers d'un utilisateur ou d'une organisation, et dont la clé de déchiffrement est promise en échange d'une rançon parfois fixée à plusieurs millions d'euros) (1). En 2022, 39% des établissements de santé déclarants ont dû faire fonctionner tout ou partie de leurs services en mode dégradé par la prise d'informations au format papier (comme encore au Centre Hospitalier de Cannes en avril dernier, 3), 42% ont subi une dégradation de leur organisation interne, et 7% reconnaissent un impact direct sur les données du patient, avec 6% des incidents ayant provoqué une mise en danger avérée des patients (2). Certaines de ces attaques ont désorganisé les services ou déstabilisé le parcours de soins au point de causer le décès de patients (4).

En parallèle, les cyberattaques engendrent des coûts de reconstruction du système informatique et des pertes de chiffre d'affaires non seulement liées à la baisse d'activité directement induite par la perturbation voire l'arrêt des services de soins suite à l'attaque, mais encore à la dégradation de l'image de l'établissement (5). Certains cabinets conseil estiment ainsi la perte économique pour les établissements à plus de vingt millions d'euros selon le type d'infrastructures touchées et la durée d'inactivité (6). La direction du Centre Hospitalier d'Albertville-Moutiers avait estimé à 1,5 million d'euros l'impact financier de la cyberattaque subie le 21 décembre 2020 en contexte de forte tension sur les équipes (fin de la 2ème vague de la COVID-19, déconfinement, début de la campagne de vaccination, sous-effectif, 7).

En conséquence, la nouvelle version du référentiel de certification des établissements de santé pour la qualité des soins par la Haute Autorité de Santé (HAS) exige des établissements de santé depuis le 1 janvier 2024 de gérer les risques numériques dans la prestation de soins aux patients (8). Cela en fait le pilier de la nouvelle politique de gestion des risques cyber des établissements de santé français en impliquant le personnel informatique, biomédical et soignant, tout au long du parcours de soins.

Pour lutter au mieux contre ces actes de cyber malveillance, le groupe de travail dédié à la sécurité numérique des équipements biomédicaux de l'Association Française des Ingénieurs Biomédicaux (AFIB) a publié en 2021 une série de recommandations visant à corréler gestion du risque numérique et ingénierie biomédicale (9). Ces recommandations ciblent entre autres la collaboration efficiente entre les différents services d'un établissement de santé concernés par la gestion des risques cyber, l'assurance d'une sécurité optimale de l'environnement des équipements biomédicaux, la prise en compte de la sécurité numérique dans les procédures d'acquisition d'équipements biomédicaux, et la définition de leur niveau de criticité. Pour autant, lors d'entretiens avec des professionnels biomédicaux, il est apparu que les propositions de l'AFIB manquaient de visibilité et que peu collaborateurs avaient investi le temps nécessaire pour se les approprier (10).

2. Renforcer la cybersécurité en établissement de santé : outils pratiques développés par les étudiants biomédicaux de l'Université de Technologie de Compiègne

Dans le cadre d'un projet de Master Ingénierie de la Santé, Parcours Technologies Biomédicales et Territoires de Santé, mené à l'Université de Technologie de Compiègne (UTC), quatre outils d'appropriation des recommandations AFIB précitées ont été conçus pour accompagner les ingénieurs biomédicaux dans la prévention des cyberattaques (10, figure 1).

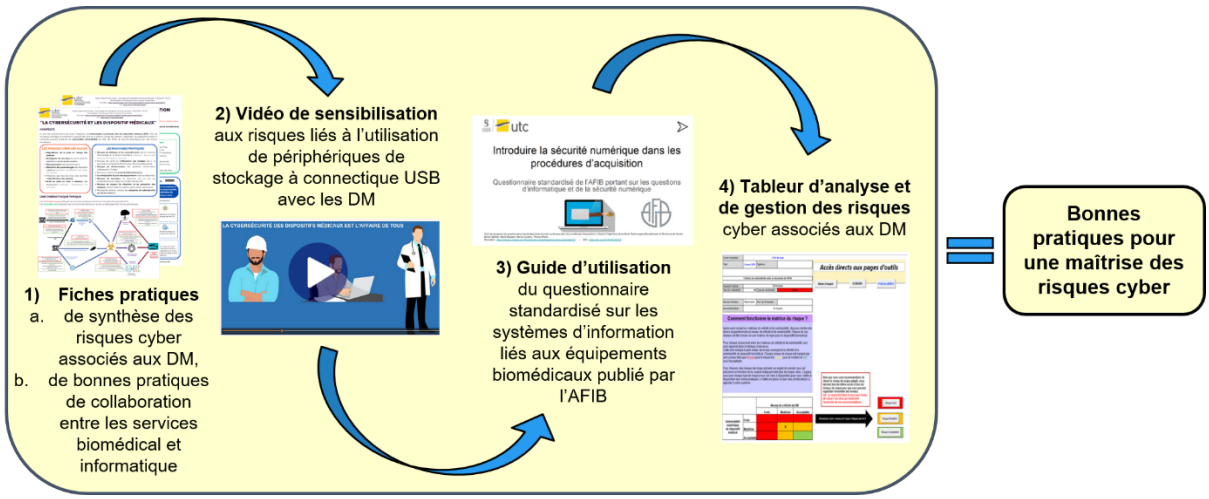


Figure 1. Outils pour une bonne maîtrise des risques cyber par l'ingénieur biomédical – Panorama et séquence d'utilisation type (DM : Dispositifs Médicaux ; lien d'accès aux outils : https://doi.org/10.34746/ids213/).

Un tutoriel vidéo de 2 min 20 s a également été élaboré pour exposer de façon synthétique la finalité et la complémentarité de ces quatre outils (10, vidéo libre d'utilisation également disponible sur https://travaux.master.utc.fr/wp-content/uploads/sites/16/2023/07/ids213-outils05-fichier.mp4).

Leur construction a intégré les retours d'expériences de professionnels biomédicaux pour confronter nos propositions à la réalité du terrain et les améliorer en conséquence (10).

2.1. La collaboration entre les services biomédical et informatique

Le premier outil s'intéresse à la collaboration entre le service biomédical et le service informatique d'un établissement de santé. Il a pour objectif de proposer une répartition des tâches entre ces services, en fonction de leurs propres missions, budgets et contraintes, au travers d'une fiche recto-verso (10, libre d'utilisation et disponible également sur : https://travaux.master.utc.fr/wp-content/uploads/sites/16/2023/07/ids213-outils03-fichier.pdf).

De façon pédagogique, le recto rappelle les risques cyber associés aux dispositifs médicaux (DM), illustre les mauvaises pratiques interservices qui favorisent ces risques, et schématise une cyberattaque type en listant les actions qui entravent la progression de l'attaque, afin de permettre aux ingénieurs biomédicaux d'identifier les failles potentielles et contribuer à y remédier (figure 2).

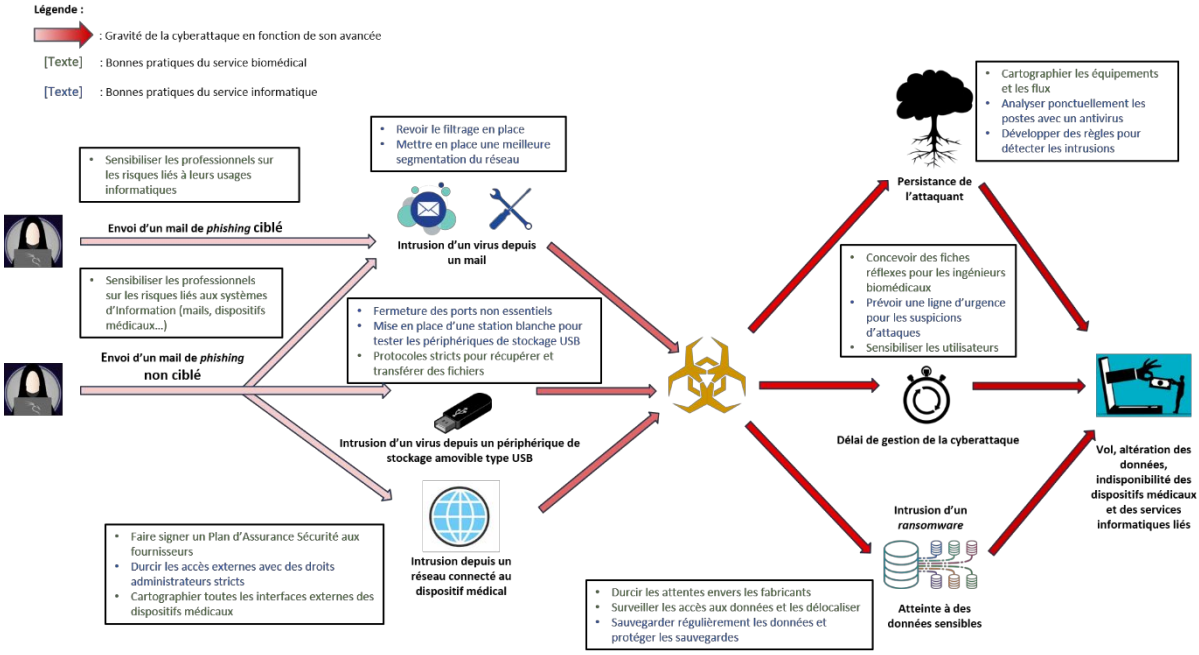


Figure 2. Arbre des pratiques d'entrave de la progression des cyberattaques par les services biomédicaux et informatiques, issu de la fiche de collaboration interservices élaborée par les étudiants de Master Ingénierie de la Santé de l'UTC (10).

Le verso de la fiche porte sur la mise en place d'un mode fonctionnement et d'une ligne de partage des responsabilités entre le service biomédical et le service informatique grâce aux retours d'expérience de différents établissements de santé. Cette mise en place comprend la définition des modalités de la collaboration entre les services, l'identification et le suivi des logiciels utilisés, et la définition du périmètre des logiciels, systèmes d'informations, infrastructures et terminaux dont le service biomédical est responsable.

2.2. La sécurité de l'environnement des équipements biomédicaux

Le deuxième outil est une vidéo de sensibilisation qui résume en près de 3 min 30 s la problématique des périphériques de stockage à connectique USB (pour *Universal Serial Bus*), fréquemment connectés directement aux DM pour des mises à jour et des transferts de données, ce qui constitue une porte d'entrée pour les cyberattaques. Le contenu de la vidéo se veut le plus accessible possible avec de nombreuses illustrations schématiques, des explications brèves et des exemples métier spécifiques au milieu hospitalier pour favoriser une diffusion et un visionnage par l'ensemble des personnels soignants avec lesquels les équipes biomédicales sont en contact (10, vidéo libre d'utilisation également disponible sur : https://drive.google.com/file/d/1V1Z7_6GNkzLGNfjadRd_xigOzC_lY0VU/view?usp=drive_link).

2.3. La cybersécurité comme critère d'achats des dispositifs médicaux

Pour aider l'ingénieur biomédical à se représenter l'environnement numérique dans lequel se situera le DM dont il projette de faire l'acquisition, une troisième outil a été proposé (10). Il s'agit d'un guide d'utilisation interactif qui permet de progresser étape par étape dans le questionnaire standardisé élaboré par l'AFIB traitant des « systèmes d'information liés aux équipements biomédicaux » (9). Cet outil a pour objectif de faciliter la lecture du questionnaire et de guider sa complétude grâce à des logigrammes synthétiques (figure 3, version intégrale de l'outil libre d'utilisation également disponible sur https://travaux.master.utc.fr/wp-content/uploads/sites/16/2024/01/ids213-outils01-fichier-vf.pdf).

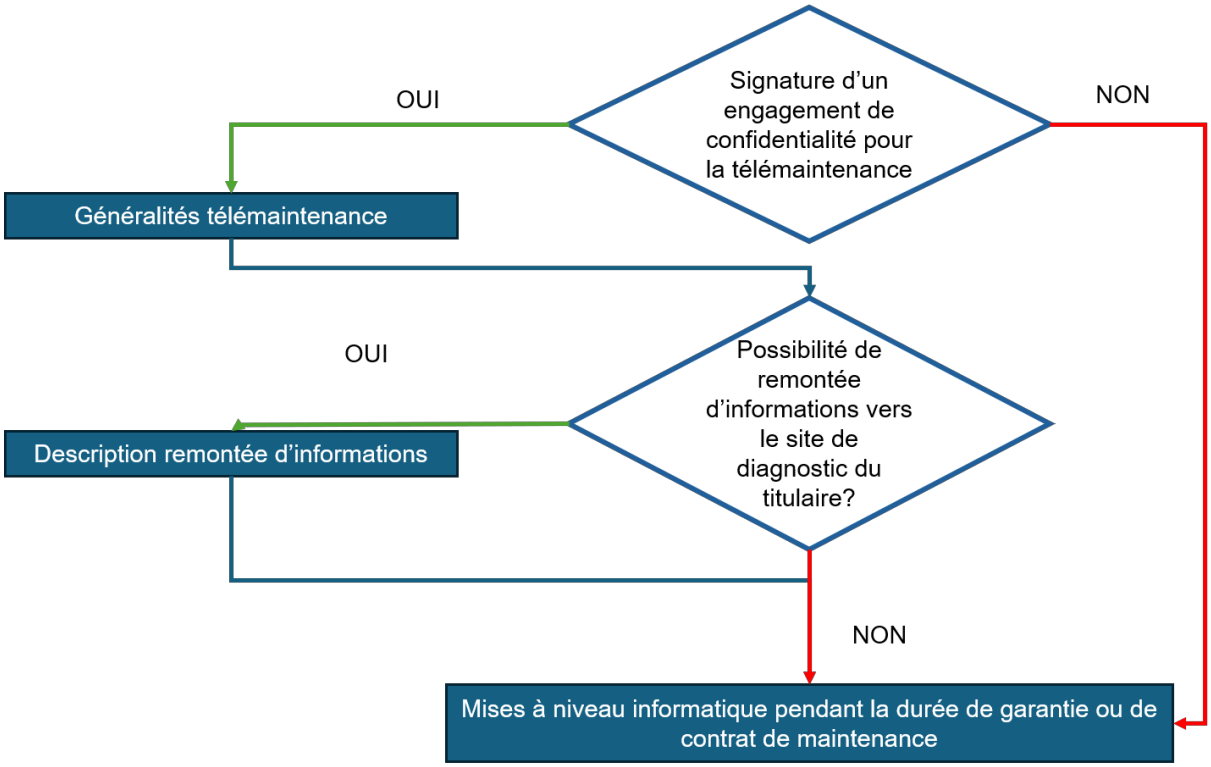


Figure 3. Extrait du guide d'utilisation interactif du questionnaire standardisé sur les « systèmes d'information liés aux équipements biomédicaux » publié par l'AFIB en 2021 (9).

Pour ce faire, le questionnaire standardisé a été scindé en 4 parties : 1- Dispositif, 2- Serveurs et architecture logicielle, 3- Logiciels, 4- Maintenance et sécurité. La figure 3 représente les premières étapes du logigramme dédié à la partie « Maintenance et sécurité ». Chaque case bleue regroupe une série de questions propres à l'item auquel elle se rapporte. Les losanges blanc entourés de bleu correspondent à des choix de situations ou d'options permettant de ne faire apparaitre à l'utilisateur que les questions pertinentes, c'est-à-dire correspondantes à ses choix plutôt que de balayer l'intégralité du questionnaire. Par exemple, si le dispositif

évalué ne peut pas envoyer de données dans le dossier patient, les questions concernant cette interaction ne seront pas affichées.

2.4. L'analyse et la gestion des risques cyber associés aux dispositifs médicaux

Le quatrième et dernier outil produit est un tableur au format Excel® qui intègre un outil d'analyse des risques cyber associés au DM considéré mais également une synthèse de plans d'actions adaptés à mettre en œuvre pour réduire ces risques (10, libre d'utilisation et disponible également sur https://travaux.master.utc.fr/?sdm_process_download=1&download_id=33963).

L'outil d'analyse des risques cyber associés au DM permet de classer les DM d'un parc selon les dommages qu'ils sont susceptibles d'engendrer sur le service de soin et directement sur les patients en cas de cyberattaque.

Pour définir de telles classes de risques cyber, deux critères sont tout d'abord évalués, la criticité du DM et sa vulnérabilité numérique (respectivement en onglets 1 et 2 du tableur), puis agrégés par le biais d'une matrice de risques (onglet 3) qui attribue un niveau de risque acceptable, modéré ou fort au DM considéré, dont découlera un plan d'action spécifique pour réduire les risques cyber associés (onglet 4 pour le plan d'actions dédié à un DM de niveau de risque cyber acceptable, onglet 5 pour un niveau de risque modéré, onglet 6 pour un niveau de risque fort).

Concrètement, la criticité du DM est évaluée grâce à la Méthode d'Analyse de la Criticité des DM en Exploitation (ou MACE). Cette méthode est efficace pour définir le niveau de criticité d'un DM car elle se base sur l'évaluation de la criticité du DM à la fois par le service de soins qui l'utilise au quotidien et à la fois par le service biomédical expert du sujet, à défaut de l'Analyse des Modes de Défaillances de leurs Effets et de leurs Criticités (ou méthode AMDEC) qui est plus généraliste (11). La vulnérabilité numérique du DM est évaluée grâce à un questionnaire créé par l'AFIB qui porte sur les caractéristiques d'un DM liées au système informatique de l'établissement, potentielles portes d'entrée pour accéder aux données personnelles des patients (9).

L'utilisation de l'outil d'analyse des risques cyber proposé est simple puisqu'il suffit de répondre à 19 questions réparties en 2 volets :

- Le premier volet dédié à l'analyse de la criticité du DM en 9 questions dont les réponses permettent de calculer automatiquement un score sur 36 points. Selon le score obtenu, un niveau de criticité acceptable (< 19 points), modéré, ou fort (> 26 points) sera affecté au DM étudié.

- Le second volet dédié à l'analyse de la vulnérabilité du DM en 10 questions dont les réponses permettent de calculer automatiquement un score sur 10 points. Selon le score obtenu, le niveau de vulnérabilité du DM est considéré comme acceptable (< 3 points), modéré, ou fort (> 6 points).

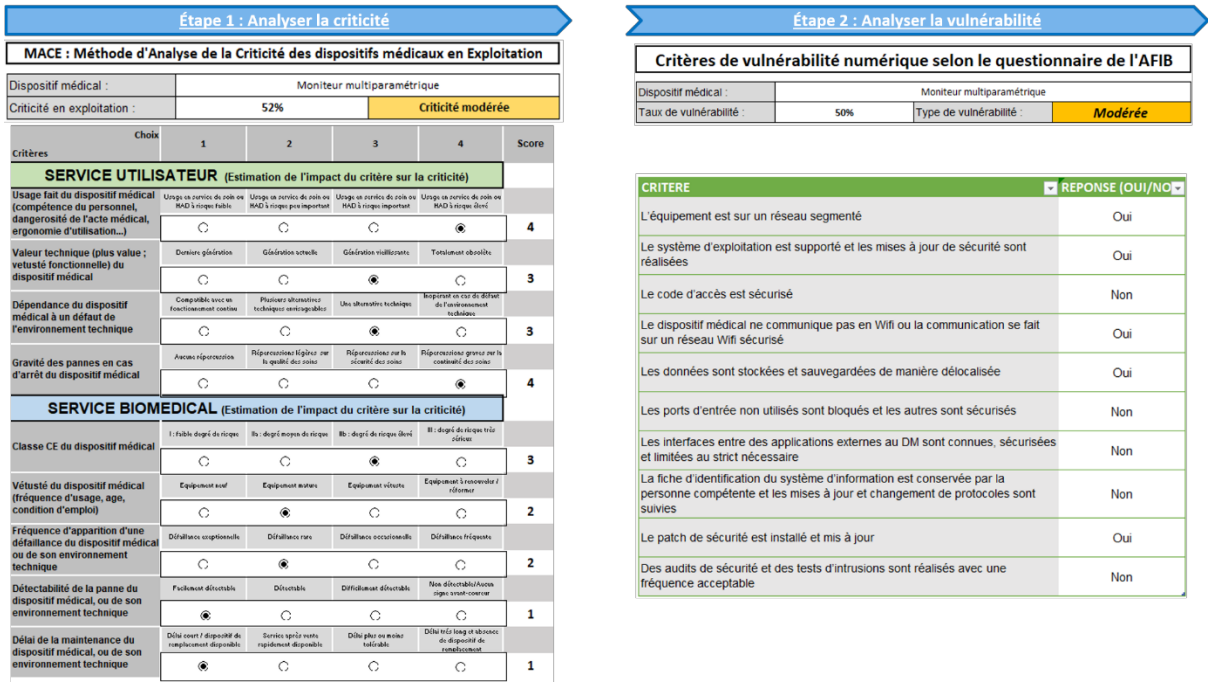
Enfin, la matrice des risques définit automatiquement des niveaux de risque cyber selon les scores de criticité et de vulnérabilité numérique obtenus (figure 4).

		Niveau de criticité du DM		
		Forte	**Modérée**	**Acceptable**
Vulnérabilité numérique du dispositif médical	**Forte**			
	Modérée			
	Acceptable			

Figure 4. Matrice des risques cyber associés aux dispositifs médicaux proposée en fonction de la criticité du dispositif médical considéré évaluée selon la méthode MACE et sa vulnérabilité numérique évaluée selon les critères retenus par l'AFIB (9).

Pour chaque niveau de risque cyber (acceptable, modéré ou fort), l'utilisateur accède par un simple bouton cliquable au plan d'actions recommandées correspondant.

La figure 5 fournit un exemple d'utilisation de l'outil d'analyse des risques cyber proposé, avec un moniteur multiparamétrique.



Étape 1 : Analyser la criticité

MACE : Méthode d'Analyse de la Criticité des dispositifs médicaux en Exploitation

Dispositif médical :	Moniteur multiparamétrique	
Criticité en exploitation :	52%	Criticité modérée

Critères / Choix	1	2	3	4	Score
SERVICE UTILISATEUR (Estimation de l'impact du critère sur la criticité)					
Usage fait du dispositif médical (compétence du personnel, dangerosité de l'acte médical, ergonomie d'utilisation...)	Usage en service de soin ou HAD à risque faible	Usage en service de soin ou HAD à risque peu important	Usage en service de soin ou HAD à risque important	Usage en service de soin ou HAD à risque élevé	
	○	○	○	◉	4
Valeur technique (plus value ; vetusté fonctionnelle) du dispositif médical	Dernière génération	Génération actuelle	Génération vieillissante	Totalement obsolète	
	○	○	◉	○	3
Dépendance du dispositif médical à un défaut de l'environnement technique	Compatible avec un fonctionnement continu	Plusieurs alternatives techniques envisageables	Une alternative technique	Inoperant en cas de défaut de l'environnement technique	
	○	○	◉	○	3
Gravité des pannes en cas d'arrêt du dispositif médical	Aucune répercussion	Répercussions légères sur la qualité des soins	Répercussions sur la sécurité des soins	Répercussions graves sur la continuité des soins	
	○	○	○	◉	4
SERVICE BIOMEDICAL (Estimation de l'impact du critère sur la criticité)					
Classe CE du dispositif médical	I : Faible degré de risque	IIa : degré moyen de risque	IIb : degré de risque élevé	III : degré de risque très sévère	
	○	○	◉	○	3
Vétusté du dispositif médical (fréquence d'usage, age, condition d'emploi)	Equipement neuf	Equipement mature	Equipement vétuste	Equipement à renouveler / réformer	
	○	◉	○	○	2
Fréquence d'apparition d'une défaillance du dispositif médical ou de son environnement technique	Défaillances exceptionnelle	Défaillance rare	Défaillances occasionnelle	Défaillance fréquente	
	○	◉	○	○	2
Détectabilité de la panne du dispositif médical, ou de son environnement technique	Facilement détectable	Détectable	Difficilement détectable	Non détectable/Aucun signe avant-coureur	
	◉	○	○	○	1
Délai de la maintenance du dispositif médical, ou de son environnement technique	Délai court / dispositif de remplacement disponible	Service après vente rapidement disponible	Délai plus ou moins tolérable	Délai très long et absence de dispositif de remplacement	
	◉	○	○	○	1

Étape 2 : Analyser la vulnérabilité

Critères de vulnérabilité numérique selon le questionnaire de l'AFIB

Dispositif médical :	Moniteur multiparamétrique		
Taux de vulnérabilité :	50%	Type de vulnérabilité :	*Modérée*

CRITERE	REPONSE (OUI/NO)
L'équipement est sur un réseau segmenté	Oui
Le système d'exploitation est supporté et les mises à jour de sécurité sont réalisées	Oui
Le code d'accès est sécurisé	Non
Le dispositif médical ne communique pas en Wifi ou la communication se fait sur un réseau Wifi sécurisé	Oui
Les données sont stockées et sauvegardées de manière délocalisée	Oui
Les ports d'entrée non utilisés sont bloqués et les autres sont sécurisés	Non
Les interfaces entre des applications externes au DM sont connues, sécurisées et limitées au strict nécessaire	Non
La fiche d'identification du système d'information est conservée par la personne compétente et les mises à jour et changement de protocoles sont suivies	Non
Le patch de sécurité est installé et mis à jour	Oui
Des audits de sécurité et des tests d'intrusions sont réalisés avec une fréquence acceptable	Non

Figure 5. Exemple d'utilisation de l'outil d'analyse des risques cyber avec un moniteur multiparamétrique en renseignant à gauche le questionnaire d'analyse de la criticité de l'équipement selon la méthode MACE (étape 1), et à droite le questionnaire d'analyse de sa vulnérabilité numérique (étape 2).

3. Conclusion

La gestion des risques cyber, notamment associés aux dispositifs médicaux, est au cœur des préoccupations de la gouvernance des établissements de santé pour garantir la sécurité soins. C'est un enjeu de certification des établissements de santé pour la qualité des soins par la Haute Autorité de Santé qui a introduit la notion de gestion des risques numériques dans la dernière version de son référentiel, applicable depuis le 1er janvier.

Pour pallier ces nouveaux risques, les services responsables que sont le service biomédical et le service informatique doivent absolument en acquérir la maîtrise. Une lutte efficiente contre les cybermenaces implique néanmoins d'accompagner la mutation de la fonction d'ingénieur biomédical.

Pour ce faire, l'Association Française des Ingénieurs Biomédicaux (AFIB) et l'Ecole des Hautes En Santé Publique ont présenté en mars lors de leur séminaire en ligne conjoint l'ensemble des chantiers menés l'AFIB pour guider les ingénieurs biomédicaux et les centrales d'achat dans l'évaluation du niveau de sécurité des dispositifs médicaux en appel d'offres. Nous proposons quatre outils d'appropriation des recommandations AFIB dont l'utilisation permet d'élaborer un état des lieux des risques encourus par un établissement de santé en cas de

cyberattaque et de s'en prémunir. Ces outils, ergonomiques et mis à disposition de tous, visent sur le plan pratique à :

- Établir une collaboration efficiente et sereine entre les équipes biomédicales et de la direction des systèmes d'information ;
- Sensibiliser l'ensemble des professionnels de santé aux risques associés à d'utilisation des périphériques de stockage à connectique USB avec les dispositifs médicaux ;
- Optimiser la lecture et la complétude du questionnaire standardisé produit par l'AFIB sur la prise en compte de la sécurité numérique dans les procédures d'acquisition de nouveaux dispositifs médicaux ;
- Mettre en place une politique d'analyse et de gestion des risques cyber associés aux dispositifs médicaux pertinente aux implications terrain concrètes.

4. Références Bibliographiques

1. Lefebvre MJ. tic santé. Cybersécurité : 467 structures de santé ont déclaré un incident au CERT Santé en 2023. https://www.ticsante.com/Story?id=7158, 2024 (accessed 2 avril 2024).

2. Agence du Numérique en Santé, Computer Emergency Response Team Santé. Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social (2022) https://www.cyberveille-sante.gouv.fr/sites/default/files/media/document/2023-06/ANS_CERTSant%C3%A9_Rapport_Public_Observatoire_Signalements_ISSIS_2022_VF.pdf, 2023 (accessed 19 décembre 2023).

3. Lefebvre MJ, Decottignies B. tic santé. Retour au papier-crayon au CH de Cannes après la cyberattaque. https://www.ticsante.com/Story?id=7183, 2024 (accessed 19 avril 2024).

4. Le Monde avec Associated Press. Le Monde.fr. En Allemagne, une attaque informatique contre une clinique provoque une mort. https://www.lemonde.fr/pixels/article/2020/09/17/en-allemagne-une-attaque-informatique-contre-une-clinique-provoque-une-mort_6052638_4408996.html, 2020 (accessed 15 février 2024).

5. Gaubert E, Jallat F. Healthcare Data Institute. Une première analyse de l'impact des cyberattaques sur les établissements de soin. https://healthcaredatainstitute.com/2023/07/11/une-premiere-analyse-de-limpact-des-cyberattaques-sur-les-etablissements-de-soin/, 2023 (accessed 3 novembre 2023).

6. Citalid, Relyens. Menaces et risques cyber pesant sur les établissements de santé en France. 2023. p. 1-14. https://www.relyens.eu/fr/wp-content/uploads/sites/4/2023/07/202306_CITALID_Menace_EtablissementsSante.pdf

7. Agence Régionale de Santé Auvergne-Rhône-Alpes. Webinaire de sensibilisation à la cybersécurité - Etablissements de santé. 2022 [cité 1 oct 2023]. Disponible sur: https://www.youtube.com/watch?v=eBXcychtSO8

8. Haute Autorité de Santé. Manuel et référentiel de certification des établissements de santé pour la qualité des soins - Version 2024. 2023. p. 1-327. https://www.has-sante.fr/jcms/p_3460794/fr/manuel-et-referentiel-de-certification-des-etablissements-de-sante-pour-la-qualite-des-soins-version-2024

9. Boissart V, Laurent D, Monnin L, Ory MJ, Raji F, Roussel S. Groupe de travail AFIB 2019–2020 : Sécurité numérique des équipements biomédicaux. IRBM News. 2021;42(1):100298.

10. Barbier B, Bossard M, Durand M, Robin T. IDS213 - Outiller l'ingénieur biomédical dans la prévention des cyberattaques [mémoire de projet]. Université de Technologie de Compiègne. 2024 https://doi.org/10.34746/ids213.

11. Lhomme J, Humbert J, Farges G. La criticité des dispositifs médicaux : état de l'art et calcul. IRBM News. oct 2013;34(5-6):150-4.