Santé Canada Health Canada

Ligne directrice

Sur les exigences relatives à la cybersécurité des instruments médicaux avant leur mise en marché

Date d'adoption : 2019/06/17
Date d'entrée en vigueur : 2019/06/26

Canada

Santé Canada a pour mandat d'aider les Canadiens à conserver et à améliorer leur santé. Il s'assure d'offrir des services de santé de grande qualité, et cherche à réduire les risques pour la santé.

Also available in English under the title :
Pre-market Requirements for Medical Device Cybersecurity

Pour obtenir plus d'information, veuillez communiquer avec :

Santé Canada
Indice de l'adresse 0900C2
Ottawa (Ontario) K1A 0K9
Tél. : 613-957-2991
Sans frais : 1-866-225-0709
Téléc. : 613-941-5366
ATS : 1-800-465-7735
Courriel : hc.publications-publications.sc@canada.ca

Date de publication : Juin 2019

Cat. : H164-278/2019F-PDF
ISBN : 978-0-660-31118-0
Pub. : 190080

Avant-propos

Les lignes directrices sont destinées à guider l'industrie et les professionnels de la santé de la façon de se conformer aux lois et aux règlements en vigueur. Les lignes directrices fournissent également aux membres du personnel des renseignements concernant la façon de mettre en œuvre le mandat et les objectifs de Santé Canada de manière juste, uniforme et efficace.

Les lignes directrices sont des outils administratifs n'ayant pas force de loi, ce qui permet une certaine souplesse d'approche. Les principes et les pratiques énoncés dans le présent document pourraient être remplacés par d'autres approches, à condition que celles-ci s'appuient sur une justification adéquate. Il faut tout d'abord discuter d'autres approches avec le programme concerné pour s'assurer qu'elles respectent les exigences des lois et des règlements applicables.

Corollairement à ce qui précède, il importe également de mentionner que Santé Canada se réserve le droit de demander des renseignements ou du matériel supplémentaire, ou de définir des conditions dont il n'est pas explicitement question dans la ligne directrice afin que le Ministère puisse être en mesure d'évaluer adéquatement l'innocuité, l'efficacité ou la qualité d'un produit thérapeutique donné. Santé Canada s'engage à justifier de telles demandes et à documenter clairement ses décisions.

Le présent document devrait être lu en parallèle avec l'avis d'accompagnement et les sections pertinentes des autres lignes directrices qui s'appliquent.

Table des matières

1. Introduction

Les instruments médicaux ont évolué d'appareils principalement analogiques, non reliés à un réseau et isolés vers des instruments en réseau qui incorporent des accès à distance, une technologie sans fil et un logiciel complexe. L'accroissement de l'interconnexion et de l'échange de données entre les instruments médicaux offrent de grands avantages aux patients et au système de soins de santé, mais peuvent laisser les instruments exposés aux accès non autorisés. Ces vulnérabilités peuvent avoir des répercussions négatives sur la sécurité en entraînant des erreurs diagnostiques ou thérapeutiques, ou en ayant une influence sur la pratique clinique.

La Loi sur les aliments et drogues (LAD) précise le cadre législatif en vertu duquel les instruments médicaux sont réglementés au Canada. Santé Canada, en tant qu'organisme fédéral de réglementation de la sûreté et de l'efficacité des instruments médicaux, considère les vulnérabilités en matière de cybersécurité des instruments médicaux comme un risque potentiel pour les patients que les fabricants doivent atténuer ou éliminer.

1.1 Portée et application

La présente ligne directrice s'applique aux produits qui sont ou qui contiennent un logiciel et qui sont réglementés comme des instruments médicaux (classes I à IV) en vertu du Règlement sur les instruments médicaux.

Les preuves de sûreté et d'efficacité des instruments médicaux de classe III et de classe IV doivent être évaluées avant de répondre à la demande d'homologation connexe. Par conséquent, une partie de la présente ligne directrice porte sur les exigences d'homologation et les éléments à prendre en considération concernant la cybersécurité dans une demande d'homologation d'un instrument médical de classe III ou IV.

Le présent document devrait être lu en parallèle avec les lignes directrices (https://www.canada.ca/fr/sante-canada/services/medicaments-produits-sante/instruments-medicaux/information-demandes/lignes-directrices.html) sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification. Le contenu décrit dans la présente ligne directrice doit être soumis à des fins d'examen, de même que les données générales énumérées aux paragraphes 32(3) et (4) du Règlement.

Le document fournit une orientation aux fabricants relativement aux données à fournir à l'appui des demandes d'homologation des instruments médicaux de classe III et de classe IV et des demandes de modification d'homologation. Les facteurs à considérer relativement à la conception, à la gestion des risques, aux tests de vérification et de validation et à la planification des futurs événements sont inclus dans le présent document. Cependant, les facteurs ne s'appliqueront pas tous à chaque type d'instrument.

Bien que le présent document recommande que les fabricants démontrent dans leur demande d'homologation ou de modification d'homologation avant la mise en marché que des dispositions adéquates sont en place pour surveiller ou prévenir les événements de

cybersécurité après la mise en marché et intervenir au besoin, le présent document ne fournit pas de ligne directrice sur les activités suivant la mise en marché devant être effectuées par le fabricant.

1.2 Objectifs stratégiques

Santé Canada considère que l'inclusion de mesures de maîtrise des risques relatifs à la cybersécurité est un facteur important dans la délivrance des homologations d'instruments médicaux. Par conséquent, la présente ligne directrice fournit aux fabricants des instruments médicaux des conseils sur les pratiques, les interventions et les mesures de gestion qui peuvent améliorer la cybersécurité de leur instrument. La présente ligne directrice décrit également l'information à présenter dans le cadre d'une demande d'homologation d'instrument médical ou de modification d'homologation pour démontrer qu'un instrument médical, qui est ou qui contient un logiciel, est suffisamment protégé contre les menaces visant à exploiter une vulnérabilité de l'instrument dans le but de causer des dommages evntuels.

1.3 Énoncés de politique

Santé Canada considère la cybersécurité comme étant un élément de la conception et du cycle de vie de l'instrument médical pouvant affecter la sûreté et l'efficacité. Les fabricants doivent tenir compte de la cybersécurité lorsqu'ils conçoivent leur instrument médical.

Comme preuve de la sûreté et de l'efficacité d'un instrument médical de classe III ou IV, le fabricant doit inclure les renseignements supplémentaires précisés dans la présente ligne directrice à sa demande. L'absence de ces renseignements supplémentaires dans une demande peut entraîner une demande de renseignements supplémentaires aux termes de la section 35(1) du Règlement à tout moment durant le traitement (lors du tri ou de l'évaluation).

La gestion des risques est requise pour tous les instruments médicaux durant tout leur cycle de vie. Les fabricants doivent intégrer la cybersécurité dans le processus de gestion des risques pour chaque instrument qui est ou qui contient un logiciel. On encourage également les fabricants à élaborer et à maintenir un cadre de gestion des risques pour la cybersécurité dans toutes leurs organisations.

Toutes les mesures de contrôle des risques pour la cybersécurité doivent être vérifiées et validées avec succès par rapport aux exigences de conception ou aux spécifications de conception de l'instrument. Les fabricants doivent être en mesure de retracer toutes les activités de vérification et de validation jusqu'aux exigences de conception ou aux spécifications de conception de l'instrument.

1.4 Abréviations et définitions

1.4.1 Abréviations

AAMI
Association for the Advancement of Medical Instrumentation

ANSI
American National Standards Institute

BMM
Bureau des matériels médicaux

CEI
Commission électrotechnique internationale

DPT
Direction des produits thérapeutiques

IMDRF
International Medical Device Regulators Forum

ISO
Organisation internationale de normalisation

LA
Laboratoires des assureurs LLC

NIST
National Institute of Standards and Technology

NMP
Nomenclature des matériaux et produits

RIT
Rapport d'information technique

1.4.2 Définitions

attaque : tentative d'accéder sans autorisation aux services, ressources ou renseignements du système, ou de compromettre l'intégrité du système.

authentification : vérifier l'identité d'un utilisateur, d'un processus ou d'un instrument, souvent comme conditions préalables à l'autorisation de l'accès aux ressources dans un système d'information. [AAMI TIR57: 2016]

confidentialité : l'information est une propriété privé qui n'est pas à etre divulguer ou donner à des personnes, entités ou processus non autorisés. La protection de la vie privée est sous-jacente à la confidentialité.

cybersécurité : l'ensemble des technologies, processus, pratiques, mesures d'intervention et de gestion dont la raison d'être est de protéger un instrument médical contre l'accès non autorisé, la modification, le mauvais usage ou le refus d'utilisation, et contre l'utilisation non autorisée d'information stockée dans un instrument médical, accédée ou transférée à partir d'un instrument médical, ou transférée vers un instrument médical.

danger : une source potentielle de dommage.

disponibilité : accessibilité et l'utilité des données, des renseignements et des systèmes d'information en temps voulu de la manière prévue (l'assurance que l'information sera disponible au besoin).

instrument : appareil, dispositif ou article semblable ou tout réactif in vitro, y compris un composant, une partie ou un accessoire de l'un ou l'autre de ceux-ci, fabriqué ou vendu pour servir à l'une ou l'autre des fins ci-après ou présenté comme pouvant y servir :

(a) le diagnostic, le traitement, l'atténuation ou la prévention d'une maladie, d'un trouble ou d'un état physique anormal ou de leurs symptômes, chez l'être humain ou les animaux

(b) la restauration, la modification ou la correction de la structure d'un corps humain ou animal, ou la fonction d'une partie d'un corps humain ou animal

(c) le diagnostic de grossesse chez la femme ou un animal

(d) les soins pour une femme durant la grossesse ou un animal durant la gestation, à la naissance et après la naissance, y compris les soins pour le nouveau-né

(e) la prévention de grossesse chez la femme ou l'animal

Par contre, sont exclus les appareils, dispositifs ou articles semblables ou tout réactif in vitro, y compris les composants, parties ou accessoires de l'un ou l'autre de ceux-ci, ayant les effets décrits aux points (a) à (e) uniquement à partir de moyens pharmacologiques, immunologiques ou métaboliques, ou uniquement à partir de moyens chimiques dans ou sur le corps humain ou animal.

intégrité : l'exactitude et l'intégralité des données, renseignements et logiciels, et l'absence de modifications inadéquates à ceux-ci.

logiciel : système logiciel mis au point dans le but d'être intégré dans l'instrument médical en train d'être mis au point ou destiné à être utilisé comme un instrument médical de plein droit. [CEI 62304:2006]

maliciel : logiciel conçu avec l'intention malveillante de perturber le fonctionnement normal, de rassembler des informations sensibles et / ou d'accéder à d'autres systèmes connectés.

menace : tout événement ou circonstance ayant le potentiel de porter atteinte à la santé et la sécurité par un accès non autorisé, une destruction, une divulgation, une modification de l'information et/ou un refus de service. [Définition modifiée de l'AAMI TIR57:2016]

nomenclature des matériaux et produits (NMP) de la cybersécurité : liste qui comprend entre autres les composants commerciaux, de logiciel à sources ouvertes, et de logiciel ou matériel informatique prêt à l'emploi dans l'instrument médical vulnérables ou possiblement vulnérables.

risque : combinaison de la probabilité d'un dommage et de sa gravité. [ISO 13485: 2016]

source de menace : intention et méthode ciblée pour intentionnellement exploiter une vulnérabilité, ou une situation et méthode pouvant accidentellement déclencher une vulnérabilité. Synonyme d'agent de menace

système : instrument médical qui est formé de composants ou de parties destinés à être utilisés ensemble pour remplir certaines ou la totalité des fonctions auxquelles il est destiné et qui est vendu sous un seul nom. (system) [Règlement sur les instruments médicaux]

validation : confirmation par examen et apport de preuves tangibles que les exigences particulières pour une utilisation donnée sont respectées, selon la définition figurant à l'article 2.18 de la norme ISO 8402:1994 de l'Organisation internationale de normalisation, intitulée Management de la qualité et assurance de la qualité - Vocabulaire, avec ses modifications successives. (validation)

vérification : confirmation par apport de preuves tangibles que des exigences particulières sont respectées. [CEI 62304:2006]

vulnérabilité : faiblesse dans un système d'information, des procédures de sécurité de système, des contrôles internes ou une mise en œuvre qui pourrait être exploitée ou déclenchée par une source de menace. [AAMI TIR57:2016]

2. Ligne directrice concernant la mise en œuvre

La cybersécurité des instruments médicaux est une responsabilité partagée entre le fabricant, l'organisme de réglementation, l'utilisateur et le fournisseur de soins de santé. Les fabricants ont la responsabilité de surveiller, évaluer et atténuer les risques liés à la cybersécurité tout au long du cycle de vie de leur produit.

Santé Canada recommande aux fabricants d'envisager une méthodologie qui aborde les risques pour la cybersécurité de ses produits. Le document NIST « Framework for Improving Critical Infrastructure Cybersecurity » est un cadre établi pouvant servir en totalité ou en partie par le fabricant comme guide des meilleures pratiques en matière de cybersécurité, y compris la gestion des risques. Voir l'annexe A pour de plus amples renseignements sur la façon dont le cadre pourrait s'appliquer aux instruments médicaux.

De plus, un fabricant doit se doter d'une stratégie pour traiter les risques pour la cybersécurité d'un instrument médical (classes I à IV) qui exécute un code de logiciel. Cette stratégie doit inclure les éléments suivants :

- Conception sécuritaire
- Gestion des risques
- Tests de vérification et de validation
- Planification de la surveillance continue des nouveaux risques, nouvelles vulnérabilités et nouvelles menaces et de la réponse à ceux-ci

Lors de l'évaluation des demandes d'homologation d'instruments médicaux de classe III et de classe IV et des demandes de modification d'homologation, Santé Canada tiendra compte de ces éléments dans l'évaluation de la sûreté et de l'efficacité de l'instrument. Les éléments énumérés ci-dessus, et les attentes de Santé Canada à l'égard de chaque élément, sont brièvement décrits dans des sections ultérieures de la présente ligne directrice.

2.1 Stratégie relative à la cybersécurité des instruments médicaux

2.1.1 Conception sécuritaire

Les fabricants doivent tenir compte de la cybersécurité au début du cycle de vie du produit lors de l'élaboration des exigences de conception. Il s'agit notamment des risques et contrôles

associés à la cybersécurité lors des choix en matière de conception; et les choix de conception qui maximisent la cybersécurité de l'instrument sans affecter excessivement les autres aspects sécuritaires de l'instrument (p. ex., l'utilisation).

Les intrants de conception saisis dans une spécification des besoins doivent comprendre ceux liés à la cybersécurité. La prise en considération des risques pour la cybersécurité à l'étape de la conception peut atténuer les risques associés à la cybersécurité pouvant contribuer : à la défaillance thérapeutique de l'instrument, à enfreindre la confidentialité, à compromettre l'intégrité et la disponibilité des données de l'instrument médical, ou à donner intentionnellement un accès non autorisé à l'instrument médical ou au réseau. Le cas échéant, ces exigences en matière de cybersécurité doivent être recoupées avec les dangers pour la cybersécurité de l'instrument particulier si les besoins consistent à atténuer les dangers identifiés. De plus, le fabricant doit envisager certains contrôles de conception qui permettent à l'instrument de détecter des attaques à la cybersécurité, d'y résister, d'y répondre et de permettre la reprise après incident.

Le tableau suivant contient quelques contrôles de conception.

Tableau 1 : **Intrants de conception qui pourraient être pris en considération durant la conception de l'instrument médical**

Principe de conception	**Description**
Communications sécurisées	Le fabricant doit considérer la façon dont l'instrument interfacerait avec d'autres instruments ou réseaux. Les interfaces peuvent comprendre des raccordements fixes et/ou des communications sans fil. Pour chaque type d'interface, le fabricant doit déterminer la méthode que l'instrument utilisera pour communiquer avec les utilisateurs (p. ex. les patients ou les professionnels de la santé), d'autres instruments/capteurs médicaux ou systèmes de soins de santé. À titre d'exemples de méthodes d'interface, citons Wi-Fi, Ethernet, Bluetooth et USB.
	Le fabricant doit considérer la façon dont le transfert de données à destination et en provenance de l'instrument est sécurisé pour empêcher les modifications et perturbations non autorisées. Le fabricant doit définir la façon dont les instruments/systèmes s'authentifieront.
Intégrité et confidentialité des données	Le fabricant doit vérifier si les données qui sont stockées dans l'instrument ou transférées vers celui-ci ou à partir de celui-ci nécessitent un certain niveau de chiffrement (c.-à-d. la transformation cryptographique des données sous une forme qui dissimule la signification d'origine pour qu'il soit impossible de les comprendre ou utiliser).

	Le fabricant doit envisager des contrôles de conception qui tiennent compte d'un instrument qui communique avec un système et/ou un dispositif qui est moins sécuritaire (p. ex. un dispositif qui se branche sur un réseau domestique ou un dispositif patrimonial sans contrôles de sécurité du dispositif). La confidentialité des renseignements médicaux d'un patient doit être prise en considération lors de la conception. Selon le Règlement sur les instruments médicaux, Santé Canada a autorité uniquement si la violation de données entraîne des dommages à un patient[1].
Accès utilisateur	Le fabricant doit envisager des restrictions d'accès qui valident qui peut utiliser l'instrument. Il pourrait aussi y avoir une exigence d'autorisation qui accorde des privilèges à différentes classes d'utilisateurs. À titre d'exemples d'authentification ou d'autorisation de l'accès, citons les mots de passe, les clés matérielles ou la biométrie.
Maintenance du logiciel	Le fabricant doit considérer la façon dont le logiciel sera mis à jour pour protéger l'appareil contre les menaces à la cybersécurité nouvellement découvertes. Il doit déterminer si les mises à jour nécessiteront l'intervention de l'utilisateur ou si elles seront déclenchées par l'instrument.
	Le fabricant doit déterminer quelles connexions seront requises pour effectuer les mises à jour.
	Le fabricant doit déterminer la fréquence à laquelle un instrument devra être mis à jour à partir d'un correctif régulier ou de routine.
	Le fabricant doit considérer la façon dont le logiciel d'exploitation, le logiciel tiers (p. ex. les bibliothèques) ou le logiciel ouvert seront mis à jour ou contrôlés.
Conception matérielle ou physique	Le fabricant doit envisager des contrôles pour empêcher une personne non autorisée d'apporter des modifications physiques ou logicielles à l'instrument afin de passer outre aux contrôles de sécurité (p. ex. désactiver un port USB pour empêcher son utilisation non-autorisée).
Fiabilité et disponibilité	Le fabricant doit envisager des contrôles de conception qui permettront à l'instrument de détecter les attaques à la cybersécurité, d'y résister, d'y répondre et de permettre la reprise après incident.

2.1.2 Gestion des risques propres à l'instrument

La gestion des risques est requise pour un instrument médical pendant tout son cycle de vie. Les fabricants doivent intégrer la cybersécurité des instruments médicaux dans le processus de gestion des risques de chaque instrument et ils doivent élaborer et maintenir un cadre organisationnel de gestion des risques pour la cybersécurité.

De solides principes de gestion des risques, comme décrits dans la norme ISO 14971-07:2007 Dispositifs médicaux – Application de la gestion des risques (ISO 14971), doivent être intégrés pendant tout le cycle de vie d'un instrument médical. Santé Canada recommande que les fabricants étendent ces principes de gestion des risques à la cybersécurité avec des facteurs à considérer supplémentaires.

Généralement un fabricant doit[2] :

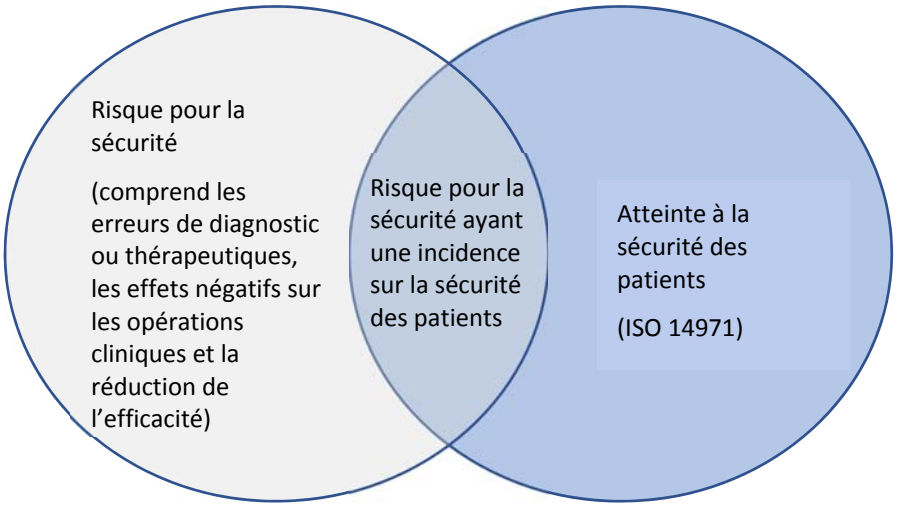
- Identifier les risques de cybersécurité
- estimer et évaluer les risques connexes
- contrôler ces risques jusqu'à un niveau acceptable
- surveiller l'efficacité des contrôles des risques

Comme l'illustre la figure 1, il existe des risques pour la cybersécurité qui pourraient avoir une incidence sur la sûreté ou l'efficacité de l'instrument médical.

Un risque pour la cybersécurité qui réduit l'efficacité, a des effets négatifs sur les opérations cliniques ou entraîne des erreurs de diagnostic ou thérapeutiques doit être pris en considération dans le processus de gestion des risques de l'instrument médical. Ce facteur est pris en considération dans la norme AAMI TIR57:2016 Principles for medical device security – Risk management (Principes pour la sécurité des instruments médicaux – Gestion des risques) qui laissent entendre que les risques associés à la cybersécurité d'un instrument peut comprendre l'atteinte directe et indirecte à la sécurité des patients (comme décrit dans la norme ISO 14971).

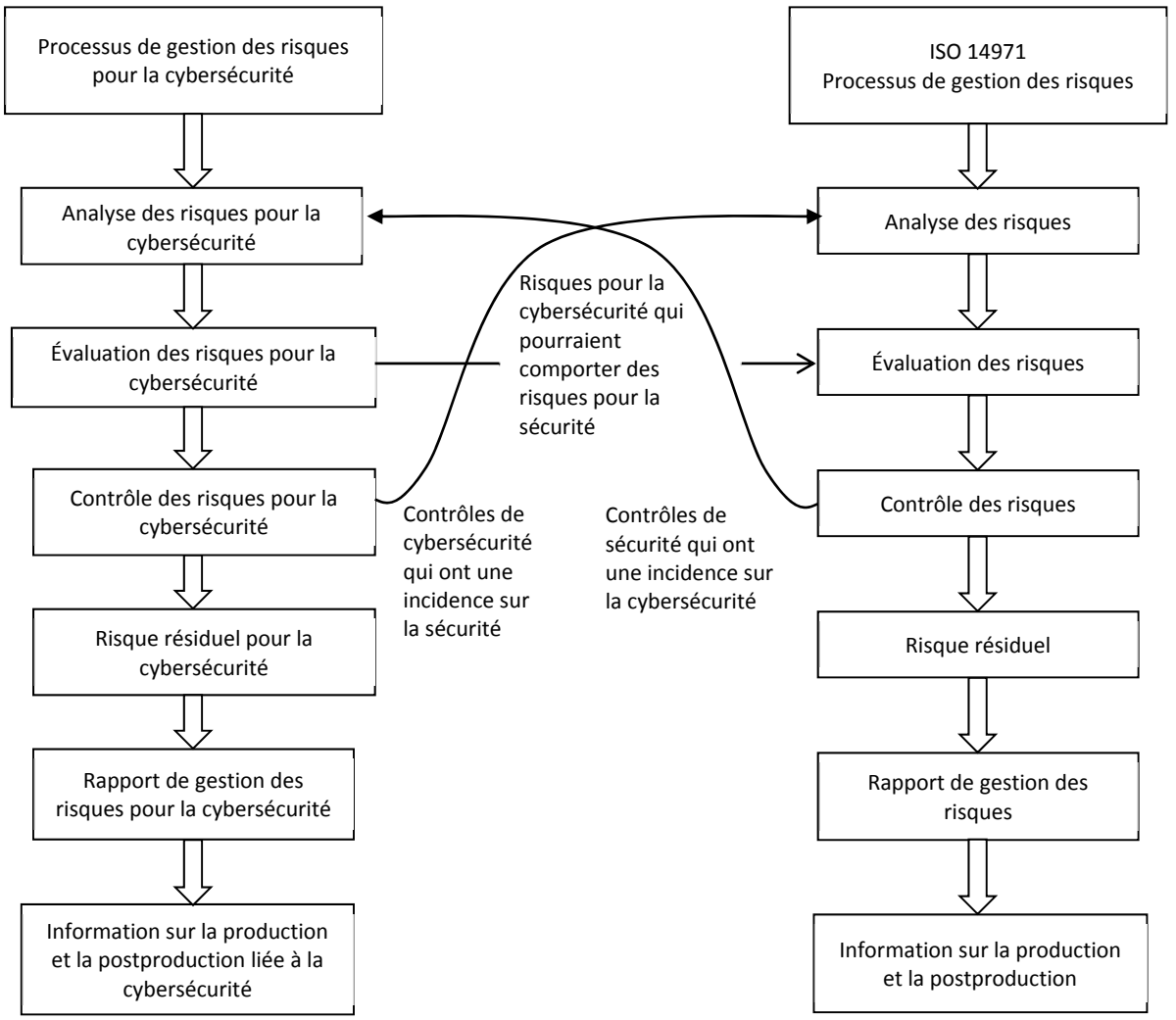
Le diagramme de Venn à la figure 1 illustre ce concept du risque pour la cybersécurité.

Figure 1 – Diagramme de Venn illustrant la relation entre un risque pour la cybersécurité et les risques pour la sécurité au sens de la norme ISO 14971 (adapté de AAMI TIR57:2016)



Santé Canada recommande que des processus de gestion des risques pour la cybersécurité propres à l'instrument soient effectués en parallèle avec le processus de gestion des risques pour la sécurité décrits dans la norme ISO 14971. Ce processus parallèle est présenté à la figure 2 et est nécessaire en raison de la relation entre la sûreté et la sécurité.

Figure 2 – Illustration de la relation entre le processus de gestion des risques pour la cybersécurité et le processus de gestion des risques pour la sécurité au sens de la norme ISO 14971 (adapté de AAMI TIR57:2016)



Les diagrammes à l'annexe B présentent quatre exemples de la relation entre la gestion des risques pour la cybersécurité et la gestion des risques pour la sécurité.

Santé Canada recommande de consulter les normes suivantes pour aider les fabricants à mener leurs processus de gestion des risques pour la cybersécurité en parallèle, et possiblement de manière itérative, avec leur processus de gestion des risques actuel :

- AAMI TIR57:2016 – Principles for medical device security – Risk management
- ANSI/CAN/UL 2900-1:2017 – Standard for Software Security Network-Connectable Products, Part 1: General Requirements

- ANSI/CAN/UL 2900-2-1:2018 – Software Cybersecurity for Network Connectable Products
- IEC 80001-1: 2010 – Application of risk management for IT-networks incorporating medical devices
- NIST 800-30 Revision 1 Guide for Conducting Risk Assessments, septembre 2012

2.1.3 Tests de vérification et de validation

Toutes les mesures de contrôle des risques pour la cybersécurité doivent être vérifiées et validées avec succès par rapport aux spécifications de conception et/ou aux exigences de conception. Les fabricants doivent être en mesure de retracer toutes les activités de vérification et de validation jusqu'aux exigences de conception ou aux spécifications de conception de l'instrument.

Les tests doivent comprendre la vérification et la validation des fonctions, des caractéristiques et des éléments de conception qui ont été mis en œuvre pour atténuer les dangers identifiés pour la cybersécurité. Santé Canada recommande de consulter les normes UL 2900-1:2017 et UL 2900-2-1:2018 pour les tests concernant la cybersécurité.

Le tableau suivant décrit brièvement les types de tests que pourraient envisager les fabricants durant le processus de vérification et de validation de logiciel.

Tableau 2 : Types de tests

Catégorie de test	Description du test
Test des vulnérabilités et des exploits	Test des vulnérabilités connues : Le code de logiciel est testé par rapport à une base de données des vulnérabilités connues, telle que la base de données nationales sur les vulnérabilités.
	Test de maliciel : Des outils de détection de maliciel sont utilisés pour scanner le code afin de déterminer si tout maliciel connu existe.
	Test d'entrée malformée (p. ex., test FUZZ) : L'instrument est assujetti à des quantités massives d'entrées malformées (invalides ou inattendues) afin d'observer s'il se comportera d'une manière peu orthodoxe ou s'il « se plantera ».
	Test de pénétration structuré : Ce type de test requiert un expert en cybersécurité qui connaît bien les techniques de piratage (chapeau blanc ou hacker éthique). L'expert en cybersécurité tente de contourner les

	couches de défense qui ont été conçues dans l'instrument.
Test des faiblesses de logiciel	Analyse statique du code source : Utilisation d'un outil logiciel pour examiner (c.-à-d. déboguer) le code source sans exécuter le code de logiciel.
	Analyse binaire et de code à octet statique : Utilisation d'outils qui examineront le code compilé créé à partir du code source.

2.2 Surveillance et gestion des nouveaux risques

Il est essentiel que les fabricants surveillent, identifient et abordent de manière proactive les vulnérabilités et les exploits dans le cadre de leur gestion suivant la mise en marché parce que les risques pour la cybersécurité des instruments médicaux évoluent sans cesse. Dans leur demande d'homologation avant la mise en marché, les fabricants doivent démontrer un plan de gestion et surveillance continue des nouvelles menaces à la cybersécurité de leur instrument. Ce plan doit être appliqué tout au long de la durée de vie prévue de l'instrument.

La gestion et la surveillance des risques émergents et peut inclures les points suivants :

- **Vigilance après la mise en marché :** un plan pour suivre et évaluer les nouvelles vulnérabilités, et y répondre.
- **Correction :** un plan pour mettre à niveau le logiciel et ainsi maintenir la sécurité et l'efficacité de l'instrument, soit régulièrement, soit en réponse à une vulnérabilité trouvée.
- **Divulgation de vulnérabilité :** un processus officiel pour obtenir de l'information sur les vulnérabilités de cybersécurité, évaluer les vulnérabilités, élaborer des stratégies d'atténuation et de correction, et divulguer l'existence des vulnérabilités et des approches d'atténuation ou de correction aux intervenants.
- **Échange d'information :** participation aux organismes d'analyse d'échange d'information (OAEI) ou aux centres d'échange et d'analyse d'information (CEAI) qui favorisent la communication des plus récents renseignements sur les menaces de sécurité et les vulnérabilités.

Dans le cadre de la stratégie de vigilance après la mise en marché, les fabricants doivent avoir en place un processus pour évaluer les possibilités d'exploitation des vulnérabilités de cybersécurité. Dans certains cas, il est peut-être difficile d'estimer la probabilité d'exploitation de la cybersécurité en raison de différents facteurs, notamment la complexité de l'exploitation, sa disponibilité, et les trousses à outils d'exploitation. En l'absence de chiffres sur la probabilité de dommage, il convient, selon les approches conventionnelles de gestion des risques des instruments médicaux, d'utiliser une « estimation raisonnable du pire scénario possible » ou une analyse des possibilités d'exploitation. Ces approches sont acceptables, mais les fabricants doivent tout de même songer à utiliser un outil d'évaluation de la vulnérabilité de la cybersécurité ou un système d'évaluation similaire pour mesurer les vulnérabilités et déterminer le besoin et l'urgence d'une intervention.

2.3 Demandes d'homologation d'instruments médicaux : exigences relatives à la cybersécurité

Les demandes d'homologation d'instruments médicaux de classe III et de classe IV et les demandes de modification de l'homologation doivent comprendre suffisamment de renseignements pour que Santé Canada puisse évaluer les éléments suivants relativement à la cybersécurité.

- Conception sécuritaire
- Activités de contrôle des risques
- Tests de vérification et de validation
- Le plan de surveillance continue et mesures d'actions contre les nouvelles menaces, vulnérabilités et les nouveaux risques

Les détails sur les éléments de donnée généraux requis pour les demandes d'homologation d'instruments médicaux et les demandes de modification d'homologation se trouvent dans la Ligne directrice sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification, à l'exception des instruments de diagnostic in vitro (IDIV) (https://www.canada.ca/fr/sante-canada/services/medicaments-produits-sante/instruments-medicaux/information-demandes/lignes-directrices/ligne-directrice-donnees-fournir-demandes-homologation-instruments-medicaux-classe.html). Les éléments de donnée suivants sont pertinents pour la cybersécurité :

- Étiquettes de l'instrument, étiquette de l'emballage et documentation
- Historique de marketing
- Évaluation des risques
- Plan de qualité propre à l'instrument
- Sûreté et efficacité

Les fabricants peuvent aussi soumettre leur demande dans le format de la table des matières. L'annexe C contient de plus amples renseignements sur les sections correspondantes suivantes :

I. Ligne directrice sur les exigences relatives à la cybersécurité des instruments médicaux avant leur mise en marché
II. Ligne directrice sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification, à l'exception des instruments de diagnostic in vitro (IDIV)
III. Dossier de la table des matières pour les demandes d'homologation d'IDIV ou non de classe III et de classe IV

2.3.1 Étiquette de l'instrument, étiquette de l'emballage et documentation

Cette section doit contenir les étiquettes, les notices, les brochures et les fiches à utiliser relativement à l'instrument.

Cela comprend les renseignements suivants en ce qui a trait à la cybersécurité.

- La NMP de cybersécurité qui énumère tous les composants de logiciel ouvert ou tiers inclus dans le logiciel de l'instrument médical. La version des composants doit être incluse dans la NMP.
- Lorsqu'une évaluation des risques a permis de constater que d'autres contrôles des risques sont nécessaires, la NMP de cybersécurité doit inclure les instructions ou informations en lien avec :
  - l'opération de l'instrument qui vise à réduire ou à éliminer le risque de cybersécurité;
  - les caractéristiques qui protègent la fonction essentielle de l'instrument, y compris lors d'un problème de cybersécurité;
  - les fonctions de sauvegarde et de restauration;
  - la façon dont les utilisateurs téléchargent le logiciel/micrologiciel, le cas échéant;
  - les caractéristiques d'ouverture de session (syslog, affichage d'événement, registres d'applications, etc.);
  - l'information sur la fin de vie;
  - la façon dont l'instrument mettra à niveau le logiciel;
  - les façons de renforcer l'instrument dans son environnement (protection du point limite, configuration de pare-feu, ouverture de session, etc.);
  - l'environnement des TI dans lequel il est prévu de déployer le produit, et les contrôles de système de réseau additionnels qui doivent être mis en place au-delà des normes de l'industrie.

2.3.2 Historique de marketing

Cette section doit comprendre un résumé des problèmes signalés et les détails de tout rappel associé à des incidents de cybersécurité (p. ex. un rappel pour traiter la vulnérabilité découverte dans un instrument).

2.3.3 Évaluation des risques

Les demandes d'homologation pour les instruments de classe III et de classe IV doivent inclure :

- une analyse des risques pour la cybersécurité
- un rapport de gestion des risques pour la cybersécurité

De plus, le rapport doit inclure les mesures de réduction des risques adoptées pour satisfaire aux exigences en matière de sûreté et d'efficacité telles qu'elles sont décrites à la section 2.1.2 de la présente ligne directrice.

2.3.4 Plan de qualité propre à l'instrument

Les fabricants sont tenus de présenter un plan de qualité pour une demande d'homologation de classe IV. Le plan de qualité doit démontrer qu'un cadre de cybersécurité fait partie intégrante des normes de qualité de l'instrument médical.

2.3.5 Sécurité et efficacité ou études de performance

Les détails des tests sur la cybersécurité sur laquelle a compté le fabricant pour s'assurer que l'instrument satisfait aux exigences de sécurité et d'efficacité doivent être inclus dans la section de la présentation portant sur la sécurité et l'efficacité (ou la section sur la performance s'il s'agit d'une demande d'homologation d'un IDIV). Habituellement, les normes de cybersécurité

n’ont pas de critères de réussite ou d’échec et les fabricants doivent fournir les comptes rendus des tests pour démontrer la sécurité et l’efficacité de l’instrument relativement à la cybersécurité.

2.3.5.1 Normes

Une liste de toutes les normes appliquées, en tout ou en partie, relativement à la cybersécurité dans la conception et la fabrication de l’instrument devrait être incluse dans la demande. Les preuves que l’instrument proposé est sûre et efficace doivent accompagner une déclaration de conformité (https://www.canada.ca/fr/sante-canada/services/medicaments-produits-sante/instruments-medicaux/information-demandes/formulaires/declaration-conformite-formulaires-instruments-medicaux.html) pour les normes reconnues par Santé Canada.

2.3.5.2 Test de cybersécurité

Les preuves du test de cybersécurité devraient être inclus dans la demande et comprendre ce qui suit :

- Dans le cas des instruments de classe III et de classe IV, un résumé détaillé du test qui a été effectué pour vérifier et valider la sécurité de l’instrument.
- Dans le cas des instruments de classe IV, les rapports qui prouvent l’exécution de tests de cybersécurité.

2.3.4.3 Matrice de traçabilité

Une matrice de traçabilité devrait être incluse dans la demande. Cette matrice doit cartographier tous les risques pour la cybersécurité relatifs :

- aux spécifications des besoins (c.-à-d. les intrants de conception)
- aux spécifications de conception (c.-à-d. les extrants de conception)
- aux tests de vérification et de validation de la conception

2.3.5.4 Plan d’entretien

Un sommaire du plan d’entretien de l’instrument doit être inclus. Ce sommaire doit contenir une description du processus après la mise en marché selon lesquels le fabricant compte assurer la sûreté et l’efficacité continues de l’instrument pendant tout son cycle de vie. Conformément à la description à la section 2.2 de cette ligne directrice, ces processus planifiés peuvent inclure : vigilance après la mise en marché, correction, politiques de divulgation des vulnérabilités, et échange d’information.

Références

- AAMI TIR57: 2016 Principles for medical device security – Risk management (en anglais seulement)
- ANSI/CAN/UK 2900-1:2017 Software Cybersecurity for Network-Connectable Products, Part1: General Requirements (en anglais seulement)
- ANSI/CAN/UL 2900-2-1:2018 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems (en anglais seulement)
- CEI 62304 Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel
- CEI 62304 Modification 1 de Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel
- Contenu de demandes auprès de la Food and Drug Administration (FDA) avant la mise en marché pour la gestion de la cybersécurité des instruments médicaux
- Gestion de la cybersécurité des instruments médicaux après la mise en marché selon la Food and Drug Administration (FDA)
- IEC 80001-1 Application de la gestion des risques pour les réseaux des TI qui incorporent des instruments médicaux – 1re partie : rôles, responsabilités et activités
- Logiciel du International Medical Devices Regulatory Forum (IMDRF) en tant qu'instrument médical (LIM) : principales définitions
- Logiciels à titre d'instruments médicaux (LIM) : définitions clés de l'IMDRF
- ISO 14971 Dispositifs médicaux – Application de la gestion des risques aux dispositifs médicaux
- National Institute of Standards and Technology (NIST) : Framework for Improving Critical Infrastructure Cybersecurity (en anglais seulement)
- National Institute of Standards and Technology (NIST) : Guide for Conducting Risk Assessments, September 2012
- NIST: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (en anglais seulement)
- NIST: Guide for Conducting Risk Assessments, septembre 2012 (en anglais seulement)
- Therapeutic Goods Administration - Medical device cyber security v. 1.0, (en anglais seulement), décembre 2018, version provisoire du guide pour consultation

Annexes

Annexe A - Cadre de gestion des risques pour la cybersécurité du fabricant

Les fabricants devraient considérer le « Framework for Improving Critical Infrastructure Cybersecurity » du NIST comme un plan directeur des pratiques exemplaires pour guider leurs activités de cybersécurité, y compris celles liées à la gestion des risques. Ce document vise à améliorer les activités de gestion des risques pour la cybersécurité pour les infrastructures essentielles, mais Santé Canada soutient le cadre comme moyen d'améliorer et de maintenir la cybersécurité des instruments médicaux.

Santé Canada a défini cinq fonctions de base du cadre qui se rapportent plus particulièrement aux contrôles de conception des instruments médicaux.

1. **Identifier :** Le fabricant doit effectuer une analyse des risques pour identifier les risques pour la cybersécurité dans ses produits.
2. **Protéger :** Des contrôles de conception doivent être mis en œuvre pour limiter le risque associé aux risques pour la cybersécurité identifiés.
3. **Détecter :** Des processus ou mesures doivent être en place pour déterminer quand l'instrument a été compromis par suite d'un événement de cybersécurité.
4. **Répondre :** Un processus ou plan défini doit être élaboré sur la façon dont l'instrument, le fabricant ou l'utilisateur répondra à un événement de cybersécurité.
5. **Reprendre :** Un plan décrivant les activités que l'instrument, le fabricant ou l'utilisateur doit entreprendre pour remettre l'instrument en état normal de fonctionnement par suite d'un événement de cybersécurité. Le résultat de toute enquête sur des reprises antérieures pourrait être utilisé comme rétroaction dans le processus de gestion des risques.

Le cadre est conçu pour compléter les processus de gestion des risques de la norme ISO 14971. On encourage le fabricant d'instruments médicaux qui a un processus standard de gestion des risques pour la cybersécurité à utiliser les concepts du cadre pour repérer les points à améliorer dans ses processus de gestion des risques pour la cybersécurité. Le fabricant qui n'a pas un processus établi de gestion des risques pour la cybersécurité pourrait envisager d'utiliser le cadre comme un guide pour établir des pratiques exemplaires dans la cybersécurité des instruments qu'il fabrique.

Annexe B – Quatre diagrammes pour illustrer la relation entre la gestion du risque pour la cybersécurité et la gestion du risque de sécurité

Figure 3 : exemple d'un risque de sécurité n'ayant aucune incidence sur la sécurité du patient

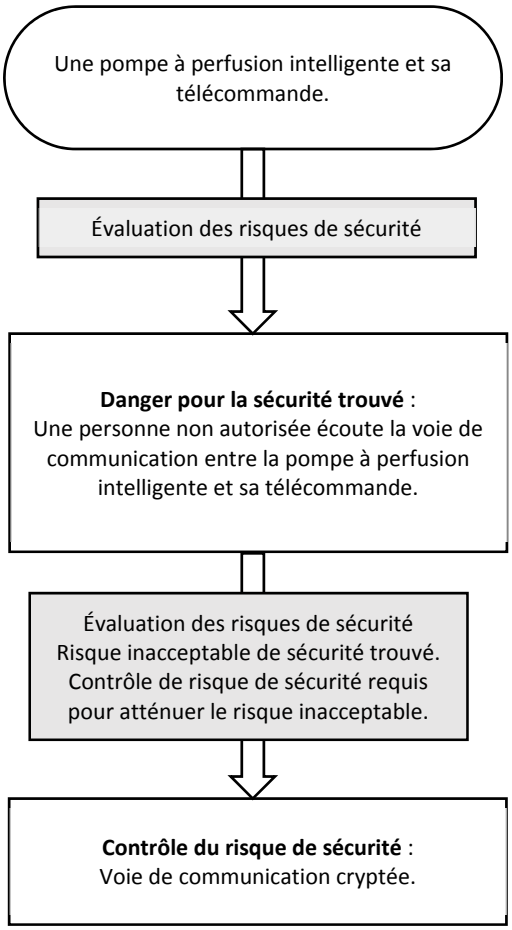


Figure 4 : exemple d'un risque de sécurité ayant une incidence sur la sécurité du patient

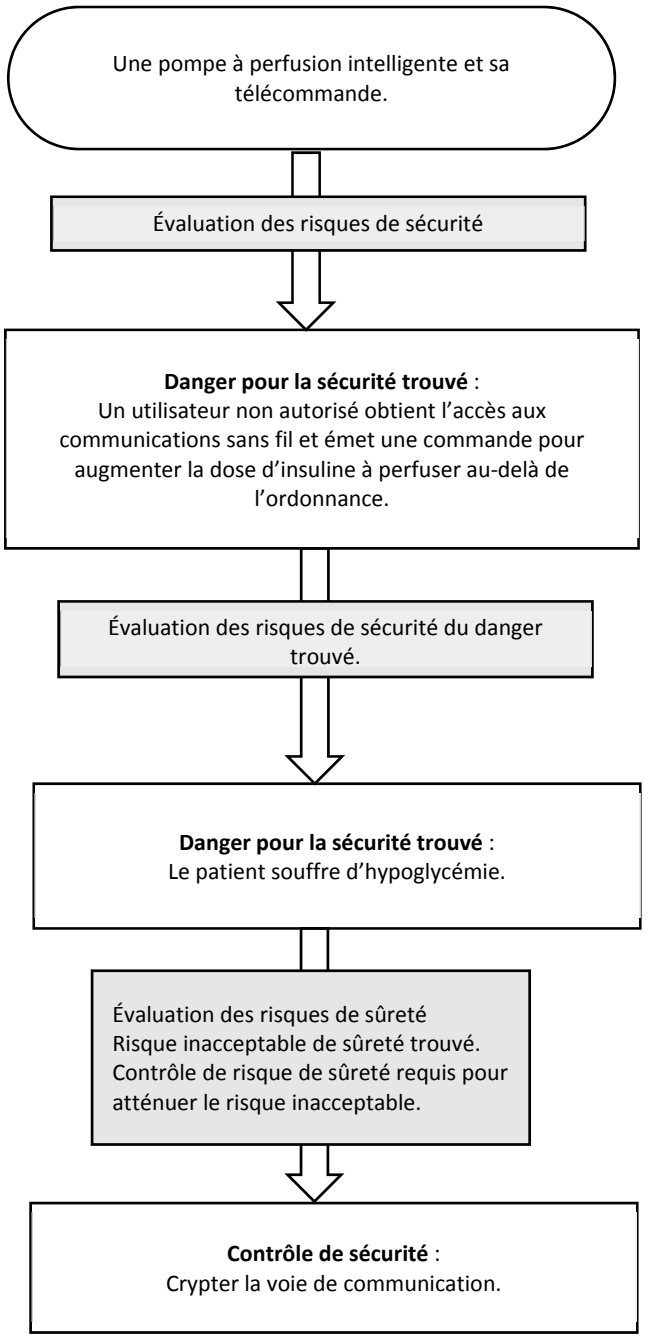


Figure 5 : exemple d'un contrôle de risque de sécurité ayant une incidence sur la sécurité du patient

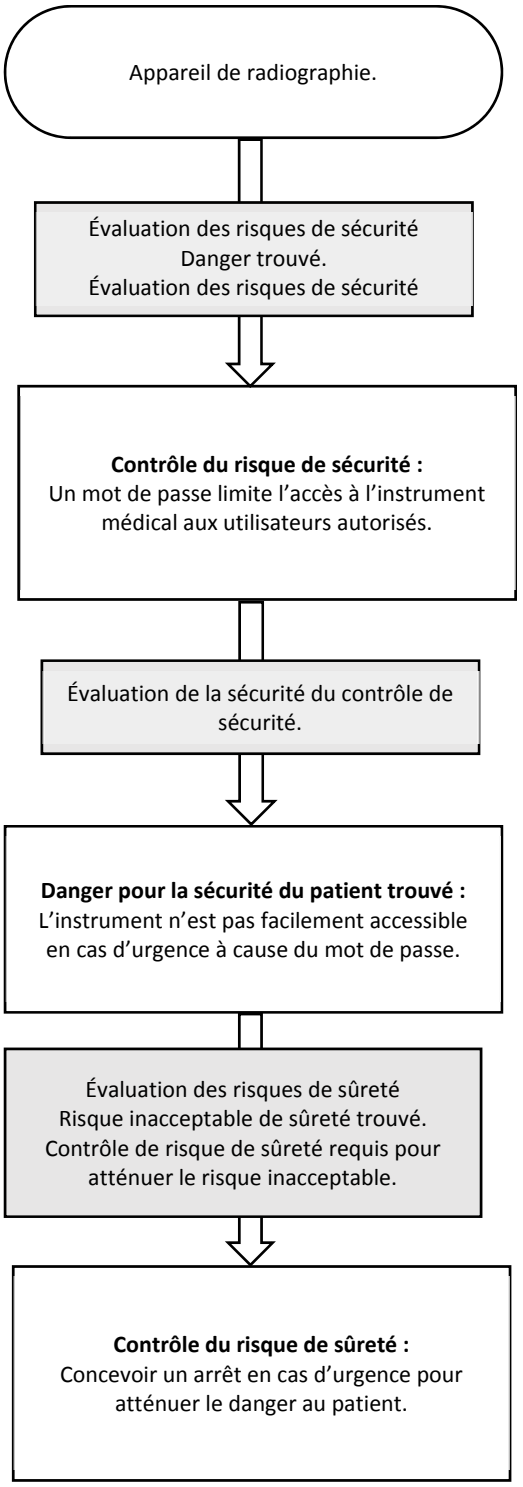
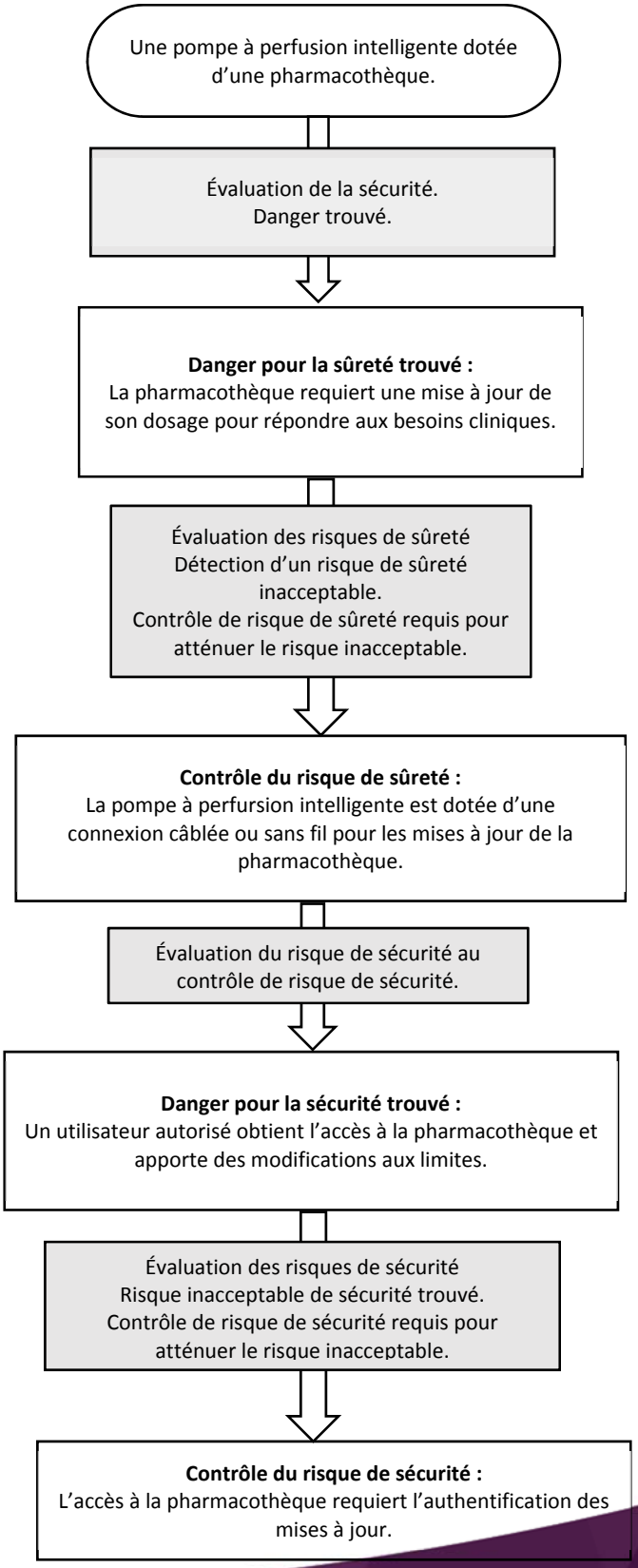


Figure 6 : exemple d'un contrôle de risque de sûreté ayant une incidence sur la sécurité du patient



Annexe C – Sections correspondantes de la ligne directrice ou du format de la table des matières de Santé Canada

Ligne directrice sur les exigences relatives à la cybersécurité avant leur mise en marché		Section correspondante : Ligne directrice sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification, à l'exception des instruments de diagnostic in vitro (IDIV)[3]		Section correspondante : Structure de dossier à table des matières[4]
Applicable aux demandes de classe III et de classe IV				
Titre des sections de la ligne directrice sur les exigences relatives à la cybersécurité avant leur mise en marché	Section	Classe III	Classe IV	Classe III et IV
Étiquettes de l'instrument, étiquetage de l'emballage et documentation	2.2.1	(3) 4.6	(4) 4.7	5.X
Historique de marketing	2.2.2	(3) 4.7[5]	(4) 4.8	2.06
Plan de qualité propre à l'instrument	2.2.4	(3) 4.7	(4)4.9.3	6B.05
Sûreté et efficacité ou études de performance				
Titre des sections	Section	Classe III	Classe IV	Classe III et IV
Liste des normes	2.2.1	(3) 5.1	(4) 5.1	3.04
Évaluation des risques	2.2.3	(3) 7.0[i]	(4)7.0	3.02
Vérification et validation de logiciel		(3)5.2.2	(4)5.2.2	3.05.05
• Test de cybersécurité	2.2.5.2	(3) 5.2.2	(4) 5.2.2	3.05.05.11

Ligne directrice sur les exigences relatives à la cybersécurité avant leur mise en marché		Section correspondante : Ligne directrice sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification, à l'exception des instruments de diagnostic in vitro (IDIV)[3]		Section correspondante : Structure de dossier à table des matières[4]
• Matrice de traçabilité	2.2.5.3	(3) 5.2.2	(4) 5.2.2	3.05.05.11
• Plan d'entretien	2.2.5.4	(3) 5.2.2	(4) 5.2.2	3.05.05.11

Ligne directrice sur les exigences relatives à la cybersécurité avant leur mise en marché (Sections applicables aux instruments de diagnostic in vitro [IDIV])		Section correspondante : Structure de dossier à table des matières IDIV
Titre des sections	Section	Classe III et IV
Étiquettes de l'instrument, étiquetage de l'emballage et documentation	2.2.1	5
Historique de marketing	2.2.2	2.06
Plan de qualité propre à l'instrument	2.2.4	6B.05 (classe IV uniquement)
Titre des sections	Section	Classe III et IV
Liste des normes	2.2.1	3.04
Évaluation des risques	2.2.3	3.02
Logiciel/micrologiciel		3.06.02
Test de cybersécurité	2.2.5.2	3.06.02.011

Ligne directrice sur les exigences relatives à la cybersécurité avant leur mise en marché (Sections applicables aux instruments de diagnostic in vitro [IDIV])		Section correspondante : Structure de dossier à table des matières IDIV
Matrice de traçabilité	2.2.5.3	3.06.02.06
Plan d'entretien	2.2.5.4	3.06.02.011

[1] Au Canada, la confidentialité des renseignements médicaux des patients est gouvernée par les lois provinciales et territoriales applicables (https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/lois-et-organismes-de-surveillance-provinciaux-et-territoriaux-en-matiere-de-protection-de-la-vie-privee/). De plus, les fabricants doivent vérifier si leurs activités sont soumises à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) (https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/lprpde_survol/).

[2] Le fabricant doit déterminer la fréquence à laquelle un instrument devra être mis à jour à partir d'un correctif régulier ou de routine.

[3] Pour les demandes qui ne sont pas au format de table des matières, les demandes d'homologation pour la classe III et IV doivent se conformer au format précisé dans la Ligne directrice sur les données à fournir pour étayer les demandes d'homologation des instruments médicaux de classe III et de classe IV et les demandes de modification, à l'exception des instruments de diagnostic in vitro (IDIV).

[4] Pour les demandes au format de table des matières, veuillez consulter la version provisoire de la ligne directrice de Santé Canada pour les demandes au format de la table des matières IMDRF pour connaître la structure et le contenu requis.

[5] Ce renseignement est nécessaire pour la sûreté et l'efficacité en lien avec la cybersécurité des instruments de classe III.