ansm
Agence nationale de sécurité du médicament et des produits de santé

Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel Au cours de leur Cycle de Vie

SEPTEMBRE 2022

La rédaction de ce document a été réalisée dans le cadre du Comité Scientifique Spécialisé Temporaire intitulé **« Cyber sécurité des logiciels dispositifs médicaux[1] »,** créé par décision du Directeur général de l'Agence nationale de sécurité du médicament et des produits de santé (l'ANSM) et dont le secrétariat est assuré par la Direction des Dispositifs Médicaux, des Cosmétiques et des Dispositifs de Diagnostic In Vitro (DMCDIV).

Auteur : Sophie NOGARET, Evaluateur Vigilance et Technico-réglementaire DMCDIV – Equipe produits diagnostic, des systèmes radiogènes et des systèmes d'information (DIALOG)

Relecteurs/ valideurs : Hélène BRUYERE Chef de Pôle équipe DIALOG ; Gwennaelle EVEN Directrice Adjointe DMCDIV ; Thierry SIRDEY, Directeur DMCDIV.

Composition du Comité Scientifique Spécialisé Temporaire (CSST) ayant conduit à l'élaboration du rapport et à sa validation :

- Monsieur ARCHET Vincent – Responsable Sécurité des systèmes d'information - INSERM
- Monsieur BLANCHET Bruno – Directeur de recherche – INRIA Paris
- Monsieur CARTAU Cédric – Responsable sécurité des systèmes d'information et CIL au CHU de Nantes
- Monsieur CASSOU-MOUNAT Bernard, Chargé de mission Ministère des Affaires sociales, de la Santé
- Monsieur CHAUSSON Luc – Auditeur Santé / Cybersécurité, LNE
- Monsieur GUILLEMAUD Régis - Responsable scientifique du département santé du LETI – CEA Grenoble
- Monsieur LOUDENOT Philippe - Fonctionnaire de sécurité des systèmes d'information pour les ministères chargés des affaires sociales
- Monsieur LOUIS Vincent – Expert en sécurité des systèmes et logiciels - DGA
- Monsieur MERLE Alain – Ingénieur chercheur spécialiste en cybersécurité – CEA Grenoble
- Monsieur PASQUIER Stéphane - Fonctionnaire de Sécurité des Systèmes d'Information adjoint aux ministères chargés des affaires sociales

[1] Décision DG n° 2017-243 du 08/06/2017 - Création CSST Cyber sécurité des logiciels dispositifs médicaux, Décision DG n° 2018-160 du 22/06/2018 - prorogation CSST Cyber sécurité des logiciels dispositifs médicaux, Décision DG n° 2019 – 385 du 29/11/2019 - Création CST Cyber sécurité des dispositifs médicaux et nouveaux enjeux des technologies de l'information - Poursuite des travaux

Sommaire

LISTE DES ACRONYMES ET DEFINITIONS UTILES

Cloud	Serveur à distance où certaines parties de l'infrastructure peuvent être gérées par un tiers (service d'hébergement ou autres parties engagées par contrat pour utiliser l'infrastructure)
COTS	« Commercial Off-The-Shelf » Produit informatique standard, fabriqué en série
Cybersécurité	Sécurité informatique qui traite de tous les aspects concernant la protection des données transitant par internet tels que leur disponibilité, leur confidentialité, et leur intégrité. Elle a pour objectif de résister aux cyberattaques (acte malveillant envers un dispositif informatique via un réseau cybernétique)
Dispositif médical connecté	Dispositif connecté directement ou à distance à un système d'information de santé. Il est composé de matériel (serveurs, périphériques, dispositifs électroniques spécifiques), de logiciels et de données (fichiers, bases de données). Il s'inscrit dans une activité de production de soins en réalisant des fonctions de traitement médical, d'analyse médicale, de surveillance médicale, de diagnostic ou de supervision.
DGOS	« Direction générale de l'Offre de Soins »
DMIA	« Dispositifs médicaux implantables actifs »
DIVIL	« Dispositifs médicaux de diagnostic *in vitro* intégrant du logiciel »
DMIL	« Dispositifs médicaux intégrant du logiciel» Note : L'acronyme anglophone SaMD (« Software as a Medical Device ») correspond en français aux logiciels dispositifs médicaux DMIL = MDIS « Medical device integrating software»
EBIOS	Méthode d'appréciation et de traitement des risques numériques publiée par l'ANSSI[1]
FIRMWARE	Micrologiciel, microcode, logiciel interne, logiciel embarqué ou microprogramme Programme « intermédiaire » entre le matériel et les applications, permettant au système de fonctionner. Il permet d'assurer la gestion des requêtes des logiciels applicatifs.
HDS	Hébergeur des données de santé
IOT	« Internet of things - internet des objets » Notion désignant l'interconnexion entre Internet et des objets, des lieux et des environnements physiques
IT	« Information Technology » Technologies de l'information et de la communication (TIC) : techniques utilisées dans le traitement et la transmission des informations
LOGS	En informatique, il s'agit du journal comprenant l'ensemble de l'historique des évènements (enregistrement séquentiel ou base de données contenant l'ensemble des actions réalisées)
Maintenance	Dans ce référentiel le terme, « Maintenance » utilisé sans qualificatif englobe à la fois la maintenance corrective des logiciels (« maintenance exécutée après détection d'une panne et destinée à remettre un bien dans un état dans lequel il peut accomplir une fonction requise », extrait de la norme NF EN 13306 X 60-319) et la maintenance évolutive des logiciels (« action consistant, par exemple à la suite de demandes d'utilisateurs, à modifier le comportement ou à proposer de nouvelles fonctions d'un dispositif logiciel »).
MEHARI	Méthode harmonisée d'analyse des risques portée par l'association loi 1901 CLUSIF (Club de la sécurité de l'information français)
Middleware	Intergiciel Logiciel créant des connexions entre différentes applications informatiques
Mise à jour à chaud	Possibilité de mettre à jour le code d'une application sans interrompre le service
Mode dégradé	Mode de fonctionnement d'un système informatique qui offre un accès réduit ou minimum au système lorsque ce dernier dysfonctionne (panne d'un élément par exemple)
Mode SaaS	Le logiciel en tant que service ou en anglais "*Software as a Service*" est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence. Les ressources (données, application, serveurs …) sont externalisées au lieu d'être chez le client
NIS	« Network and Information Security » Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les infrastructures : mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
NVM	« Non Volatile Memory » - mémoire non volatile Mémoire informatique qui conserve ses données en l'absence d'alimentation électrique
PACS	« Picture Archiving and Communication system » ou Système d'archivage et de transmission d'images Système permettant de gérer les images médicales grâce à des fonctions d'archivage. Il permet la communication via réseau des images (format DICOM par exemple) et le traitement à distance ou en réseau local avec des ordinateurs disposant de moniteurs à haute définition pour la visualisation des examens effectués en imagerie.

[1] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

Patch	Tout élément modificateur du code source ou correctif portant sur des configurations du logiciel non spécifiques au client et n'embarquant aucune évolution fonctionnelle du logiciel. L'objectif est de corriger une faille identifiée dans le logiciel. La notion de patch est liée à la notion de faille, en sécurité
PGSSI-S	Politique générale de Sécurité des systèmes d'Information de Santé
RGS	Référentiel général de sécurité (rendu officiel par arrêté du premier ministre applicable depuis le 1er juillet 2014) : il garantit la sécurité des systèmes d'information en charge de la mise en œuvre des systèmes de téléservices et des échanges électroniques entre l'administration et les usagers.
RGPD	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, dit règlement général sur la protection des données
SIS	Système d'information de santé
SNMP	« Simple Network Management Protocol » - Protocole simple de gestion de réseau Protocole de communication qui permet aux administrateurs réseaux de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
SOUP	« Software of Unknown Pedigree or Provenance » Logiciels tiers utilisés (*librairies, drivers, …*) mais dont l'utilisateur n'a pas la preuve des performances.
SSI	Sécurité des systèmes d'information
TIC	Technologies de l'Information et de la Communication (TIC) Voir définition IT
Version majeure	Version qui apporte des fonctionnalités nouvelles qui ont un impact sur le reste de l'application ou qui modifient le mode de fonctionnement, l'organisation de l'utilisateur
Version mineure/intermédiaire	Version qui corrige des bugs et/ou apporte des fonctionnalités nouvelles qui n'ont pas d'impact sur le reste du logiciel et qui ne modifient pas le mode de fonctionnement, l'organisation de l'utilisateur

PREAMBULE

Ce document fournit des recommandations dont l'objectif est de proposer un ensemble de bonnes pratiques. Il ne s'agit pas d'un texte normatif.

Il s'adresse principalement aux fabricants de DM comportant des logiciels et aux logiciels DM. Le terme « éditeur de logiciel » est bien employé dans le sens de fabricant en terme réglementaire.

Certaines recommandations impliquent néanmoins une responsabilité conjointe. En effet, il apparait difficile d'exclure de ces bonnes pratiques les autres parties prenantes tels que les utilisateurs, les établissements de santé, les patients, etc....Certains éléments figurant dans ces recommandations ne seront donc pas uniquement du ressort des fabricants. Dans ce cas, les intervenants seront précisés dans le texte. Néanmoins, si les fabricants ne sont pas les seuls responsables, ils doivent fournir les moyens de sécuriser leurs dispositifs dans les environnements d'utilisation. L'objectif de ce document n'est pas de définir les moyens mais de fournir les clés pour atteindre ce but.

Pour des questions de lisibilité, il a été choisi d'utiliser la terminologie générique « **dispositifs médicaux intégrant du logiciel** » ou « **DMIL** » pour définir à la fois les logiciels dispositifs médicaux et les dispositifs médicaux connectés. L'acronyme DM sera employé de manière générique. Il couvre tous les types de DM : DM, DMDIV (dispositifs de diagnostic in vitro), DMIL (dispositifs médicaux intégrant du logiciel) et DMIA (dispositifs médicaux implantables actifs). Lorsqu'un type spécifique de DM est concerné, l'acronyme correspondant sera alors utilisé.

De même, le terme « **cybersécurité** » désignera la sécurité informatique face à des menaces.

CONTEXTE

Dans le secteur de la santé plus qu'ailleurs, la protection des personnes, des biens et des données personnelles est une nécessité. En effet, l'exploitation d'une vulnérabilité peut avoir des conséquences néfastes jusqu'à impacter directement la sécurité des soins et la santé des patients.

Ces dernières années, les logiciels et applications mobiles dédiés au domaine de la santé connaissent un essor grandissant. Ces produits sont très variés : ils couvrent les logiciels d'échanges de données, de maintenance, de télésurveillance, de prédiction d'un risque ou encore les programmes de pilotage de dispositifs médicaux.

Certains de ces logiciels ou applications destinés par leurs fabricants à être utilisés à des fins médicales sont qualifiés de dispositifs médicaux (DM) ou de dispositifs médicaux de diagnostic *in vitro* (DMDIV). Ils sont marqués CE au titre des nouveaux règlements européens[1] et entrent dans le champ de surveillance de l'ANSM.

Si la mise sur le marché des dispositifs médicaux est bien encadrée d'un point de vue réglementaire, la culture de la cybersécurité est très hétérogène au sein des fabricants de DM. Les causes en sont multiples : absence d'analyse de risque spécifique (notion de risque de malveillance généralement non identifiée en santé), méconnaissance des exigences de cybersécurité, défaut de prise en compte de la cybersécurité dans le processus de conception et de développement du DM. De plus, il n'existe pas encore de textes, de normes internationales ou européennes dédiées spécifiquement à la sécurité informatique.

Or, si les dispositifs médicaux intégrant du logiciel sont de plus en plus connectés aux réseaux (wifi, radiofréquence, Bluetooth...), ils doivent s'adapter aux nouvelles menaces engendrées par les progrès technologiques notamment dans le domaine des malveillances informatiques, de la cybercriminalité et du cyberterrorisme.

Il devient donc essentiel que les fabricants de dispositifs médicaux soient en capacité d'intégrer, dès la conception de leurs produits, des processus de base et des exigences relatives aux produits permettant de garantir un niveau minimum de sécurité face à la malveillance informatique.

Ce document a pour objectif de fournir des recommandations à l'attention des fabricants de dispositifs médicaux afin qu'ils prennent les mesures nécessaires pour réduire au maximum les risques d'attaque à l'encontre de leurs DM et ainsi prévenir la compromission des données et l'utilisation détournée des DM qu'ils mettent sur le marché. Ceci est permis par la mise en place de bonnes pratiques et standards adéquats en matière de cybersécurité.

[1] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE ;
Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic *in vitro* et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission.

CHAMP D'APPLICATION

Les produits concernés

La règlementation relative aux dispositifs médicaux a été revue en profondeur et a conduit à la publication, le 5 mai 2017, de deux nouveaux règlements : l'un concernant les dispositifs médicaux (**Règlement (UE) 2017/745 du parlement européen et du Conseil du 5 avril 2017**) et l'autre concernant les dispositifs médicaux de diagnostic *in vitro* (**Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017**). Ces deux règlements sont entrés en vigueur le 26 mai 2017. Ils entreront en application respectivement le 26 mai 2021 pour le règlement relatif aux dispositifs médicaux et le 26 mai 2022 pour le règlement relatif aux dispositifs médicaux de diagnostic in vitro, entraînant alors l'abrogation des directives 93/42/CEE (DM), 98/79/CE (DMDIV) et 90/385/CEE (DMIA). Les certificats délivrés par les organismes notifiés au titre des directives avant le 26 mai 2021 pour les DM ou 26 mai 2022 pour les DMDIV resteront valides jusqu'à la fin de leur période de validité et au plus tard, pour les derniers, le 27 mai 2024 pour les DM et 26 mai 2025 pour les DMDIV, date à laquelle, ils seront invalidés.

L'**article 2.1** du nouveau règlement DM définit le dispositif médical comme :
« 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, et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens.
Les produits ci-après sont également réputés être des dispositifs médicaux:
-les dispositifs destinés à la maîtrise de la conception ou à l'assistance à celle-ci,
-les produits spécifiquement destinés au nettoyage, à la désinfection ou à la stérilisation des dispositifs».

De même, le nouveau règlement DMDIV définit les DMDIV comme :
« tout dispositif médical qui consiste en un réactif, un produit réactif, un matériau d'étalonnage, un matériau de contrôle, une trousse, un instrument, un appareil, un équipement ou un système, utilisé seul ou en combinaison, destiné par le fabricant à être utilisé *in vitro* dans l'examen d'échantillons provenant du corps humain, y compris les dons de sang et de tissus, uniquement ou principalement dans le but de fournir une information:
-concernant un processus ou un état physiologique ou pathologique ou
-concernant une anomalie congénitale ou
-concernant la prédisposition à une affection ou à une maladie.
-permettant de déterminer si un traitement donné est sûr pour les receveurs potentiels et compatibles avec eux
-permettant de prévoir la réponse ou les réactions à un traitement
-permettant de définir ou de contrôler des mesures thérapeutiques. »

Les logiciels (applications mobiles ou sur ordinateur, système embarqué et même intelligence artificielle) sont de plus en plus proposés comme solutions médicales (diagnostic, suivi, mesures,…). Ils peuvent fonctionner seuls comme un dispositif médical à part entière (ex : application mobile de diagnostic) ou en association avec un dispositif médical (ex : logiciel exploitant les mesures d'un capteur).

Le règlement DM précise également que les logiciels sont réputés être des dispositifs actifs : « tout dispositif dont le fonctionnement dépend d'une source d'énergie autre que celle générée par le corps humain à cette fin ou par la pesanteur et agissant par modification de la densité de cette énergie ou par

conversion de celle-ci. Les dispositifs destinés à la transmission d'énergie, de substances ou d'autres éléments, sans modification significative, entre un dispositif actif et le patient ne sont pas réputés être des dispositifs actifs ».

Exemples de dispositifs médicaux intégrant du logiciel (DMIL)
Logiciels dispositifs médicaux :

- logiciel de planification de traitement en radiothérapie (TPS) ;
- application mobile d'évaluation des grains de beauté à risque de cancer ;
- application mobile pour le calcul personnalisé des doses d'insuline.

DM utilisant un logiciel pour leur fonctionnement et leur supervision :

- pacemakers, pompes à perfusion ;
- stations de monitoring ou d'anesthésie.

Les règlements précisent que « les logiciels destinés à des usages généraux (par exemple un logiciel administratif général utilisé pour gérer le dossier médical patient), même lorsqu'ils sont utilisés dans un environnement de soins, ou les logiciels destinés à des usages ayant trait au mode de vie ou au bien-être, ne constituent pas des dispositifs médicaux ». En effet, ce n'est pas l'environnement d'utilisation qui induit un statut de DM. La notion de logiciel d'usage général permet d'écarter des outils comme Excel (excepté le codage de macros à finalité médicale). Pour l'instant, la notion de style de vie / bien-être autorise la création d'applications pour le sport, la quantification du soi, ou l'évaluation de la qualité du sommeil par exemple sans contraintes inhérentes au marquage CE.

Exemples de logiciels non dispositifs médicaux

- les logiciels dits de suivi de la condition physique, coaching ;
- les produits de bien être qui ne sont pas des DM (bracelet connecté) ;
- logiciels d'observance.

D'autres exemples de logiciels et applications mobiles illustrant le positionnement réglementaire sont disponibles sur le site de l'ANSM : www.ansm.sante.fr.

Les règlements européens se sont adaptés aux évolutions technologiques et ont pris en compte les dispositifs médicaux intégrant du logiciel ou DMIL dans la définition des produits.

Les bases réglementaires

Afin de se conformer à la règlementation, les dispositifs médicaux intégrant du logiciel[1] doivent répondre à certains critères.

En particulier, l'**Annexe I** des nouveaux règlements définit les **exigences générales en matière de sécurité et de performance**. Certaines d'entre elles visent spécifiquement les DMIL. Les numéros d'articles ci-dessous se réfèrent à l'annexe I du règlement DM (2017/745). Le règlement DMDIV (2017/746) inclut des exigences similaires.

L'**article 14.2** indique que « les dispositifs sont conçus et fabriqués de manière à éliminer ou à réduire autant que possible (…) tout risque associé à une éventuelle interaction négative entre les logiciels et l'environnement informatique dans lequel ceux-ci fonctionnement et avec lequel ils interagissent ». *Exemple: les logiciels reliés à un système de PACS*.

L'**article 14.5** précise que « les dispositifs destinés à être mis en œuvre avec d'autres dispositifs ou produits doivent être conçus et fabriqués de manière à ce que leur interopérabilité et leur compatibilité soient fiables et sures ».

[1] https://www.ansm.sante.fr/Dossiers/Dispositifs-medicaux/Qu-est-ce-qu-un-dispositif-medical/(offset)/0; Règlement (UE) 2017/745 Chapitre V, Section 1, Article 51 Classification des dispositifs

Le point 17 des exigences générales est dédié spécifiquement aux DMIL. Il indique que leur conception doit garantir la répétabilité, la fiabilité, ainsi que les performances conformes à l'usage qui en est prévu. Des mesures doivent ainsi être prises afin d'éliminer ou de réduire tous les risques ou dégradations des performances de ces dispositifs. Les éléments suivants sont détaillés :

- 🖹 **Article 17.1.** : « Les dispositifs comportant des systèmes électroniques programmables, notamment des logiciels, ou les logiciels qui sont des dispositifs à part entière sont conçus de manière à garantir la répétabilité, la fiabilité et les performances eu égard à leur utilisation prévue. En condition de premier défaut, des moyens adéquats sont adoptés pour éliminer ou réduire autant que possible les risques qui en résultent ou la dégradation des performances ».
- 🖹 **Article 17.2.** : « Pour les dispositifs qui comprennent des logiciels ou pour les logiciels qui sont des dispositifs à part entière, ces logiciels sont développés et fabriqués conformément à l'état de l'art, compte tenu des principes du cycle de développement, de gestion des risques, y compris la sécurité de l'information, de vérification et de validation ».
- 🖹 **Article 17.3.** : « Les logiciels visés à la présente section qui sont destinés à être utilisés en combinaison avec des plateformes informatiques mobiles sont conçus et fabriqués en tenant compte des caractéristiques spécifiques de la plateforme mobile (par exemple, taille et rapport de contraste de l'écran) et des facteurs externes liés à leur utilisation (variation du niveau sonore ou de la luminosité dans l'environnement) ».
- 🖹 **Article 17.4.** : « Les fabricants énoncent les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu ».

Les règlements précise également la nature de la documentation nécessaire autour du logiciel pour en justifier la conformité.

🖹 L'**article 6.1. de l'annexe II** porte sur la vérification, la validation du logiciel, la description de la conception et du processus de développement du logiciel et la preuve de la validation de celui-ci, tel qu'il est utilisé dans le dispositif fini. Ces informations incluent en règle générale un résumé des résultats de l'ensemble de la vérification, de la validation et des essais réalisés en interne et dans un environnement d'utilisation simulé ou réel avant la libération finale. En outre, elles prennent en compte toutes les différentes configurations du matériel informatique et, le cas échéant, des différents systèmes d'exploitation figurant dans les informations fournies par le fabricant.

Les règlements européens précisent clairement les exigences sur les logiciels, autant d'éléments non présents dans les directives 93/42/CE, 98/79/CE et 90/385/CEE relatives aux DM, DMDIV et DMIA. Dans ce contexte, les fabricants devront appliquer des procédures de marquage CE plus contraignantes, avec une obligation plus fréquente de gérer un système de management de la qualité et un système de surveillance post-commercialisation.

Distinguer sûreté et sécurité

Pour aborder la problématique de la sécurisation des dispositifs médicaux intégrant du logiciel, il est nécessaire de définir en amont deux notions fondamentales : la sûreté et la sécurité.
Souvent confondues, elles se différencient pourtant par la nature des risques contre lesquels lutter.

Sûreté

La sûreté de fonctionnement d'un dispositif médical consiste à s'assurer qu'il fonctionne correctement et à prévenir les risques aléatoires et involontaires. La sureté prend également en compte les erreurs d'utilisation.
La sûreté de fonctionnement d'un système informatique est définie comme la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans le service délivré[1]. L'obtention d'un système sûr de

[1] « Sûreté de fonctionnement des systèmes informatiques », J.-C. Laprie, B. Courtois, M.-C. Gaudel, D. Powell, 1996

fonctionnement passe par l'utilisation d'une combinaison de méthodes visant à contrer des actions, internes ou externes, pouvant conduire à la survenue d'une défaillance du système.
Exemple : s'assurer qu'une pompe à perfusion délivre le débit programmé, avec la précision prévue par le fabricant

Sécurité

La sécurité consiste à s'assurer que le DM est protégé contre les attaques extérieures pouvant compromettre le fonctionnement du DM[1]. Elle résulte de l'établissement et du maintien de mesures de protection qui assurent un état d'inviolabilité contre des actes ou des influences hostiles[2].
Exemple : le piratage d'une pompe à perfusion, avec prise de contrôle à distance de la programmation peut conduire à la délivrance non voulue de produit ou à la modification des débits.

La principale différence entre sûreté et sécurité porte donc sur la nature des erreurs identifiées. La sûreté de fonctionnement s'intéresse majoritairement aux *erreurs accidentelles*. La sécurité prend en compte les *actions intentionnelles*, c'est-à-dire créées dans l'intention de nuire. Cette différence est fondamentale. Un système peut en effet être sûr de fonctionnement parce que la probabilité d'occurrence d'un événement redouté est jugée négligeable ; ce système ne sera pas nécessairement *sécurisé*, parce qu'un attaquant cherche précisément à déclencher l'événement redouté. Un système sécurisé doit délivrer les services attendus (c'est-à-dire, être conforme à sa spécification), et *seulement* ce service.

Les notions de sécurité et de sûreté ne sont évidemment pas antinomiques. Les méthodes préconisées dans le domaine de la sûreté de fonctionnement permettent de satisfaire de nombreuses exigences de sécurité. Il est d'ailleurs essentiel de prendre en considération le caractère intentionnel des fautes dans l'analyse de risque qui gouverne la conception d'un système sécurisé. Néanmoins, il est utile de préciser que quelles que soient les mesures de sûreté et de sécurité mises en place, l'innocuité d'un dispositif médical sur le plan médical est un prérequis. Ceci doit être vrai tout au long du cycle de vie du dispositif médical.

La prise en compte des recommandations de sécurité complète celles qui concourent à la sûreté et à la qualité d'un dispositif médical.

La sûreté de fonctionnement n'entre pas dans le champ de ce document. Il traitera uniquement de la notion de sécurité.

Evaluation des menaces et de la vulnérabilité

Le développement des objets à usage médical connectés ainsi que le déploiement de la télémédecine représentent les principaux nouveaux facteurs de risques. Ils exposent la population à de nouvelles menaces. Leur impact n'est pas uniquement individuel mais peut également toucher une population.

Les mesures de sécurité d'un DM peuvent donc non seulement concourir à la protection du DM en tant que *cible* d'une attaque, mais aussi en tant que *relai ou point d'entrée* d'une intrusion au sein du système d'information de l'établissement de santé qui l'héberge.

- Les attaques ciblant uniquement le DM sont destinées à modifier/altérer son fonctionnement ou sa disponibilité.
  Par exemples :
  - **Attaques contre la disponibilité du dispositif** médical: déni de service, avec comme exemples la surcharge des requêtes au DM entrainant son incapacité à y répondre et

[1] https://ansm.sante.fr/var/ansm_site/storage/original/application/edd12a5999dc24a7fa6d6cda4e39469f.pdf
[2] IEC GUIDE 120:2018

le blocage du réseau, la perte de données sur les patients, la surconsommation énergétique entraînant l'épuisement de la batterie ;
    - **Attaques contre l'intégrité** : données modifiées, fonctionnement altéré du dispositif médical (perte de contrôle, ralentissement, perturbation des soins..), la destruction physique, la perturbation de fonctionnement du dispositif médical due aux rayonnements électromagnétiques (se référer aux normes de compatibilité électromagnétiques - directive européenne 2014/30/UE) ;

- Les attaques ciblant le DM comme point d'entrée ont pour objectif d'altérer le fonctionnement de l'infrastructure ou les autres dispositifs au sein de cette infrastructure :
    - la perturbation de fonctionnement du dispositif médical à partir du SIS ou de son réseau, et vice versa ;
    - la capture ou la modification de données échangées entre le dispositif médical et le SIS.

Exemples d'attaques

Ces dernières années, plusieurs établissements français ont fait l'objet de cyberattaques de grande ampleur. En 2015, le système informatique du service de radiothérapie de Valence a été piraté donnant l'accès aux données des patients contenues dans les dispositifs médicaux. Les séances de radiothérapie ont été stoppées pendant 24 heures[1].
En 2016, un certain nombre de vulnérabilités sur les dispositifs médicaux connectés ont été identifiées. Par exemple, une faille de sécurité a été découverte dans une pompe à insuline, qui pourrait permettre à quelqu'un de la contrôler à distance en interférant avec ses communications sans fil[2].
La même année, des failles de sécurité ont été identifiées sur des DM implantables connectés. L'exploitation des failles pouvait permettre à une personne non autorisée d'accéder à l'appareil et de modifier les commandes du pacemaker en déchargeant rapidement la batterie de l'appareil implanté ou encore en provoquant des chocs inopportuns qui pourraient entraîner la mort du patient. Une mise à jour logicielle a été ordonnée par la FDA[3].

Au fil des années, les dispositifs médicaux ont connu des progrès technologiques spectaculaires avec le développement de logiciels d'échange de données, de surveillance, de prévision d'un risque, les logiciels de pilotage. Ces évolutions ont rapidement été intégrées dans la pratique médicale quotidienne sans que les risques associés soient parfaitement maitrisés. En effet, si les fabricants sont capables de garantir des produits sûrs en termes d'innocuité biologique et d'efficacité clinique, ils n'ont pas encore de culture spécifique dans le domaine de la sécurité informatique.

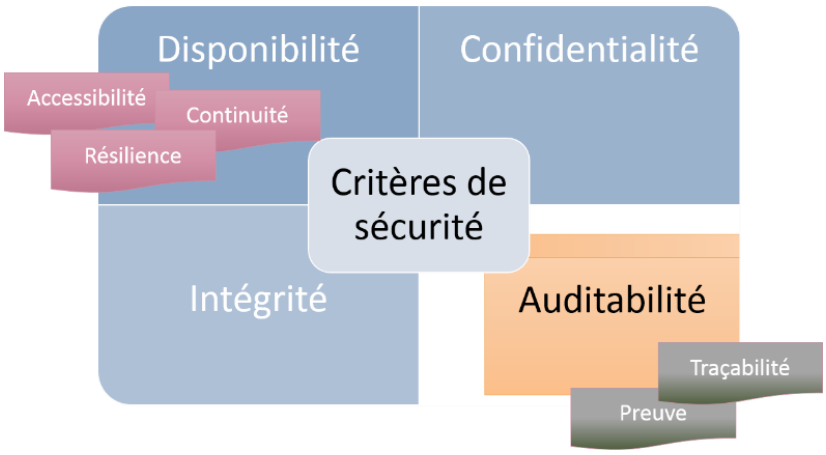
Les règlements européens introduisent maintenant des exigences propres aux DMIL en termes de sécurité et de performance. La notion de cybersécurité n'est pas explicitement nommée et développée mais l'application de ces nouvelles règles et l'évolution constante des technologies et de la connectivité ouvrent la voie vers la mise en place d'une nouvelle démarche de gestion des risques et de sécurisation des systèmes par le fabricant. Ces dispositions peuvent être pensées en amont et revendiquées dans les spécifications des produits.

[1] « Cyberattaques : les établissements de santé tentent de se protéger », Marion Guérin, 23/10/2015
[2] https://www.jnj.com/innovation/johnson-and-johnson-leading-fight-to-prevent-cyberattacks
[3] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

CYBERSÉCURITÉ APPLIQUÉE AUX DMIL

Sécurité des systèmes d'information (SSI)

On entend par cybersécurité « l'ensemble des mesures techniques ou organisationnelles mises en places pour assurer l'intégrité et la disponibilité d'un DM ainsi que la confidentialité des informations contenues ou issues de ce DM contre le risque d'attaques dont il pourrait faire l'objet » [↳Fig.1].



↳Figure 1. Critères prioritaires en matière de cybersécurité

Définition des critères

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

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

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

Selon le Référentiel général de sécurité (RGS), qui s'applique aux SI, ces critères, disponibilité, intégrité et confidentialité, représentent les objectifs de base à atteindre en matière de sécurité.

Ils sont complétés par un critère additionnel : l'**auditabilité**[1] qui correspond à la faculté d'un système à conserver les traces des opérations effectuées sur les biens à protéger (par exemple, les accès ou tentatives d'accès à des informations) et à garantir l'exploitabilité de ces traces à des fins de contrôle ou d'investigation : enregistrement des actions avec leur date et heure dans un fichier journal.

Précisions concernant la confidentialité et la protection des données

[1] https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf

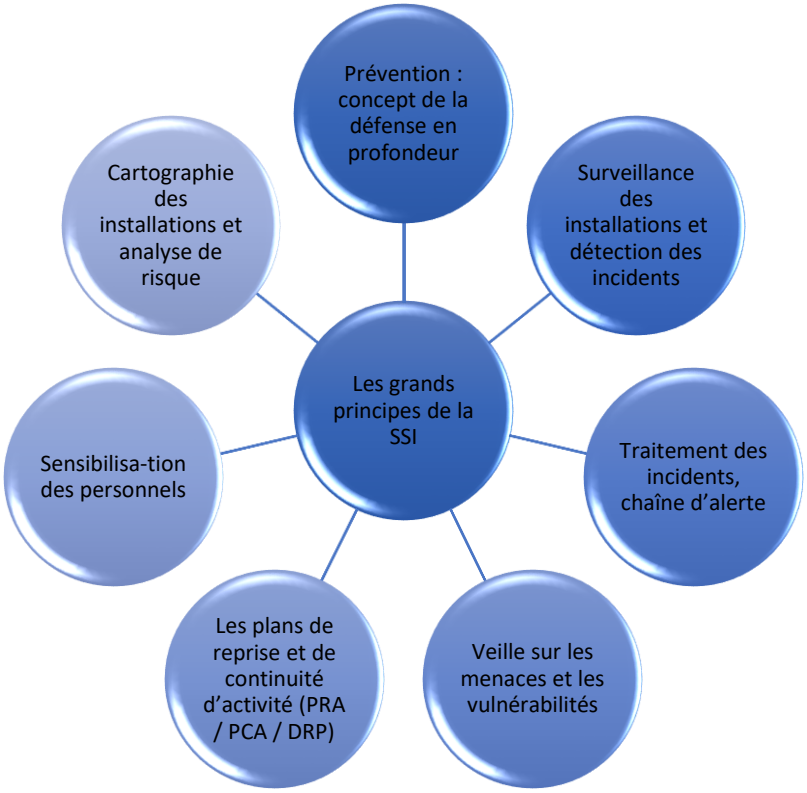
La confidentialité des données dans le sens « protection de la vie privée » doit être au centre des préoccupations des fabricants de dispositifs médicaux. Plusieurs référentiels traitent de la protection de la confidentialité des données. Le fabricant pourra notamment se référer au **Référentiel Général de Sécurité** (RGS) qui comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité »[1]. A titre d'exemple, tout dispositif connecté doit embarquer un dispositif de chiffrement des données afin de garantir la confidentialité des données médicales personnelles lors de leur stockage ou de leur transfert. Le règlement général sur la protection des données (RGPD), entré en vigueur le 24 mai 2016 et en application le 25 mai 2018, définit ce que sont les données à caractère personnel et impose les dispositions pour leur protection.

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

Les recommandations ANSM porteront principalement sur la disponibilité et l'intégrité des DMIL dont l'atteinte peut avoir des conséquences néfastes sur la santé du/des patient(s).

Gestion des risques en matière de technologie de l'information (IT)

La sécurisation des systèmes d'information (SSI) repose sur un certain nombre de grands principes. Il s'agit d'empêcher l'utilisation non-autorisée, le mésusage, la modification, la copie « silencieuse » ou le détournement du système d'information [↳Fig. 2].



↳Figure 2. Grands principes de la SSI

En France, la protection des systèmes d'information de l'État et la vérification de l'application des mesures dépendent de **l'Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI)[2].

[1] https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf;
http://references.modernisation.gouv.fr/sites/default/files/RGS_fonction_de_securite_Confidentialite_V2_3.pdf;
http://references.modernisation.gouv.fr/sites/default/files/RGS_PC-Type_Confidentialite_V2_3.pdf
[2] https://www.ssi.gouv.fr/

L'ANSSI met à disposition un ensemble de guides de bonnes pratiques et de guides de recommandations[1] destinés aux professionnels de la sécurité informatique et au grand public afin de les sensibiliser aux différentes méthodologies de sécurité numérique.

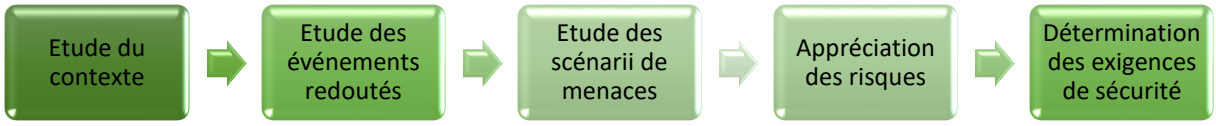
Exemples de guides disponibles :
-Recommandations pour choisir des pare-feu maîtrisés dans les zones exposées à Internet ;[2]
-Recommandations pour la mise en place de cloisonnement système ;[3]
-Cartographie du système d'information ;[4]
-Guide hygiène informatique.[5]

Méthodes d'analyse de risques

Il existe plusieurs méthodes d'analyse de risque en SSI qui reposent sur l'identification **des biens essentiels à protéger**. Ces biens sont les éléments qui peuvent, en étant attaqués, avoir des conséquences sur les biens ou les personnes.

L'ANSSI a développé une méthode d'analyse et de gestion du risque appelée **EBIOS**[6] [↳Fig. 3]. Elle permet d'apprécier les risques, de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en œuvre, de préparer l'ensemble du dossier de sécurité nécessaire à l'acceptation des risques et de fournir les éléments utiles à la communication relative aux risques.

Cette méthode peut s'appliquer aux dispositifs médicaux.



↳*Figure 3. Différentes étapes de la démarche EBIOS*

La méthode EBIOS est citée ici à titre d'exemple et d'illustration. D'autres méthodes d'analyse équivalentes à EBIOS existent et sont acceptables (MEHARI, ISO 27005…).
La norme ISO 27005 est par exemple une norme internationale traitant de la gestion des risques dans le contexte de la sécurité des systèmes d'information. Elle fait l'objet d'une certification.

Les nombreux documents et outils proposés par l'ANSSI peuvent être appliqués aux DMIL. Ils ont servi de source pour l'élaboration de ces recommandations.

Gestion des risques en matière de dispositifs médicaux

La gestion des risques appliquée aux dispositifs médicaux est définie dans la **norme ISO 14971 (NF EN ISO 14971:2019)** et développée spécifiquement à l'attention des fabricants de dispositifs médicaux. Elle traite des processus de gestion des risques concernant principalement le patient, mais également l'opérateur, l'ensemble des intervenants, les équipements ainsi que l'environnement d'utilisation. En complément et en matière de gestion des risques pour les logiciels, il existe également la norme **IEC 62304** qui aborde le développement du logiciel dispositif médical et son cycle de vie
L'analyse de risque est réalisée aux différentes étapes du cycle de vie du dispositif médical [↳Fig.4].

[1] Lien : https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[2] https://www.ssi.gouv.fr/guide/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-a-internet/
[3] https://www.ssi.gouv.fr/uploads/2017/12/guide_cloisonnement_systeme_anssi_pg_040_v1.pdf
[4] https://www.ssi.gouv.fr/administration/guide/cartographie-du-systeme-dinformation/
[5] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
[6] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

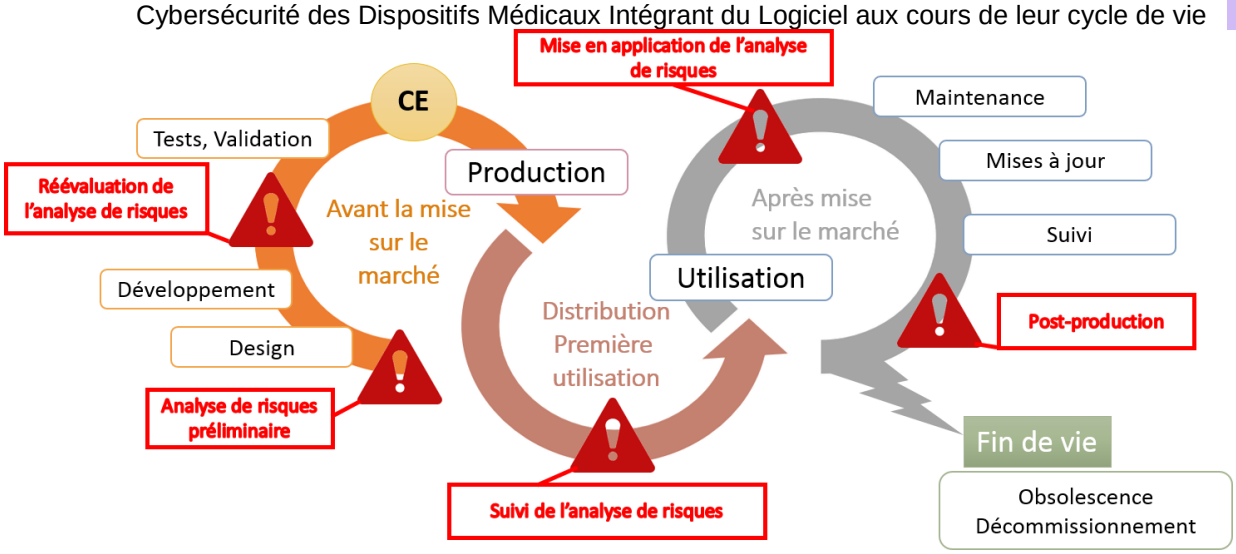


Figure 4. Analyse de risque au cours du cycle de vie du DM

Selon la **norme ISO 14971,** le fabricant doit évaluer, pour un dispositif médical donné, dans un contexte d'utilisation défini par le fabricant lui-même, les vulnérabilités qui existent et caractériser l'impact potentiel qui peut en résulter. On parle de vulnérabilité du matériel, du logiciel, de failles dans les procédures et également de problématiques liées à des aspects humains.

Une fois la vulnérabilité identifiée, il détermine le **niveau acceptable de risque** en définissant le seuil de tolérance au risque.
L'acceptation des risques est évaluée au regard du rapport bénéfices / risques. Un risque est acceptable si :

- il est maitrisé autant que possible,
- la réduction du risque n'altère pas le rapport bénéfice / risque global,
- il présente un rapport bénéfice / risque favorable, et
- les mesures de surveillance après commercialisation sont planifiées.

Par exemple :
☒ Décès – atteinte irréversible ⇒ *intolérable*,
☒ Atteinte réversible ⇒ *possible acceptabilité si les avantages médicaux sont supérieurs au risque résiduel global*,
☒ Altération de l'image de marque, perte financière ⇒ *acceptable en dessous d'un seuil défini.*

Afin de minimiser l'impact potentiel de cette vulnérabilité, il faut prévoir les mesures à mettre en place et comment les déployer. En effet, le déploiement des mesures permet d'assurer la continuité des fonctions à un niveau tolérable. La définition des mesures de réduction du risque est formalisée dans la norme via l'élaboration d'un document comprenant le plan de gestion des risques et le rapport de sécurité du logiciel

Faire converger le monde du DM et celui de l'IT

Principe

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

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

Pour intégrer les risques liés à la cybersécurité, l'idée est de proposer aux fabricants de réaliser une analyse de risque combinant les deux approches : analyse de risque en SSI (par exemple, selon l'ISO 27005) et analyse de risque DM (ISO 14971).

Plus précisément,

- Pour remplir le cahier des charges du marquage CE**, le fabricant doit garantir que son dispositif médical répond aux exigences générales** en matière de sureté et de performance tout le long de son cycle de vie, des phases de conception jusqu'à la mise au rebut.
- Pour penser en termes de cybersécurité, le fabricant doit identifier les biens essentiels à protéger et garantir leur intégrité, disponibilité, confidentialité et auditabilité.

Concevoir une analyse de risque combinant les deux approches consistera à compléter l'analyse de risque « classique » en introduisant les critères de sécurité « cyber » tout au long du cycle de vie du dispositif médical. Le but est de décliner les mesures à même de couvrir les menaces identifiées.

Dans son approche, le fabricant devra prendre en compte les différences de risques selon les types de DM concernés et adapter la conception du DM en fonction de cela. De même, il devra prendre en compte les spécificités liées à la topologie, l'environnement d'utilisation du DMIL.

Par exemple :

- Dispositifs médicaux implantés ou portés par le patient (Exemple pacemakers, pompes à insulines, etc.)

⇒ *Risque pour la santé du patient*

- Dispositifs médicaux connectés au réseau hospitalier plutôt orientés « diagnostic »

⇒ *Risque principal : vecteur d'attaque pour le réseau*

- Dispositifs médicaux connectés au réseau hospitalier à des fins de soins

⇒ *Risques pour le patient et le réseau*

Les systèmes étant de plus en plus imbriqués/interconnectés, il apparait limitant de réaliser uniquement une analyse de risques système par système. Ce schéma d'évaluation apparait insuffisant pour les architectures complexes, tel qu'un réseau informatique d'un hôpital.

Or, lorsque le DM est intégré dans un SIH, il peut être le vecteur de propagation d'une menace. Il faudrait alors suggérer une analyse de risque sur un système complet ce qui apparait difficile sachant que l'on ne connait généralement pas le SI global dans lequel le DMIL sera intégré. Il serait donc utile de proposer au fabricant d'évaluer le risque de propagation des menaces dans le système en cas d'attaque et de le rendre le système robuste face à une défaillance.

Il existe des outils informatiques facilitant la démarche via des systèmes de modélisation tels que ceux développés dans le secteur de l'aéronautique. Cependant, compte tenu des pratiques actuelles, ce type de démarche constituera l'objectif à atteindre à plus long terme.

Méthodologie

La satisfaction des exigences de sécurité s'inscrit dans le cadre général **d'un système de management de la qualité « classique »** (**NF ISO 13485 : 2016**) auquel s'ajoutent les éléments suivants :

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

Les biens à protéger sont, *a minima* :

- Le firmware
- Le paramétrage médical : *par exemple,* au niveau du processus de pilotage du capteur à injection, il s'agit de l'ensemble des algorithmes et techniques qui mesurent la quantité à injecter / calculateur de débit etc.
- Les clés cryptographiques
- Le journal d'évènement / les logs
- Les données relatives aux patients

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

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

La démarche se déroulera selon la manière suivante :

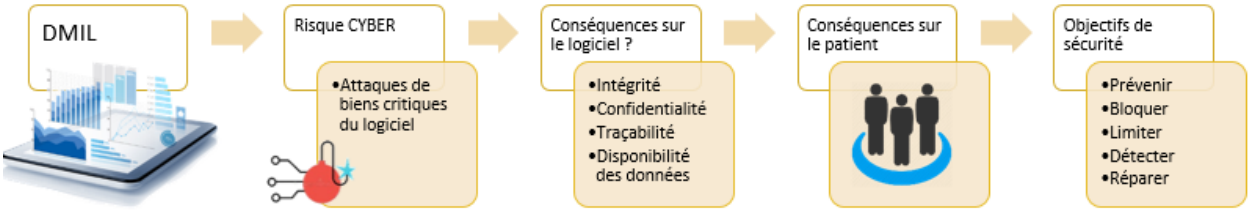


Figure 5. Démarche de sécurisation

Il existe un certain nombre d'approches pour garantir l'intégrité, la disponibilité, la confidentialité et l'auditabilité :
- prévenir : éviter l'existence ou l'émergence de vulnérabilités ;
- bloquer : empêcher une attaque d'atteindre des éléments sensibles ou vulnérables ;
- limiter : minimiser les conséquences d'une attaque ;
- détecter : identifier une intrusion afin de fournir une réponse à l'attaque (traçabilité) ;
- réparer : avoir les moyens de rétablir le fonctionnement normal du système après une attaque (notion de résilience).

Par exemple

Biens à protéger	*Objectifs de sécurité*	*Systèmes de protection*
Le logiciel et le paramétrage médical	*Intégrité et confidentialité*	- ***Bloquer*** Signature des données - ***Bloquer*** Chiffrement des mémoires - ***Limiter*** Gestion des droits (initialisation / première utilisation / modification)
Le firmware (	*Garantir l'intégrité dans le cadre d'une mise à jour par exemple*	- ***Bloquer*** Séquence d'amorçage (boot) sécurisée du DM associée à un mécanisme de vérification d'une signature cryptographique du firmware
Les clés cryptographiques	*Intégrité, confidentialité et traçabilité*	- ***Prévenir*** Protéger le secret des clés, ne pas les déplacer
Le journal d'événement	*Intégrité, confidentialité et traçabilité*	- ***Limiter*** Sauvegardes régulières, analyses de dysfonctionnements
Les données relatives aux patients	*Intégrité et confidentialité*	- ***Bloquer*** Chiffrement - ***Limiter*** Collecter uniquement les données essentielles

Ces recommandations ont donc pour objectif de guider les fabricants dans leur démarche de cybersécurisation des logiciels dispositifs médicaux, du développement à la mise sur le marché, à l'utilisation et la surveillance post-marché.

Il s'agit de donner les grands principes sans détailler les aspects techniques qui rendraient ce document rapidement obsolète compte tenu de l'évolution rapide des dispositifs médicaux et des attaques.

Sur la base des éléments décrits précédemment, le document s'appuie sur les méthodologies d'analyses de risques développées dans le monde du DM et celui de la SSI. Il s'agira d'atteindre un niveau de risque minimum acceptable. Ces dispositions s'inscrivent dans une démarche de mise en œuvre d'un système de management de la qualité (QMS). La partie III du document précisera donc les points particuliers relatifs à la cybersécurité.

RECOMMANDATIONS DÉCOULANT DE L'ANALYSE DE RISQUES

Les recommandations sont divisées en 5 grands axes basés sur le cycle de vie du logiciel :

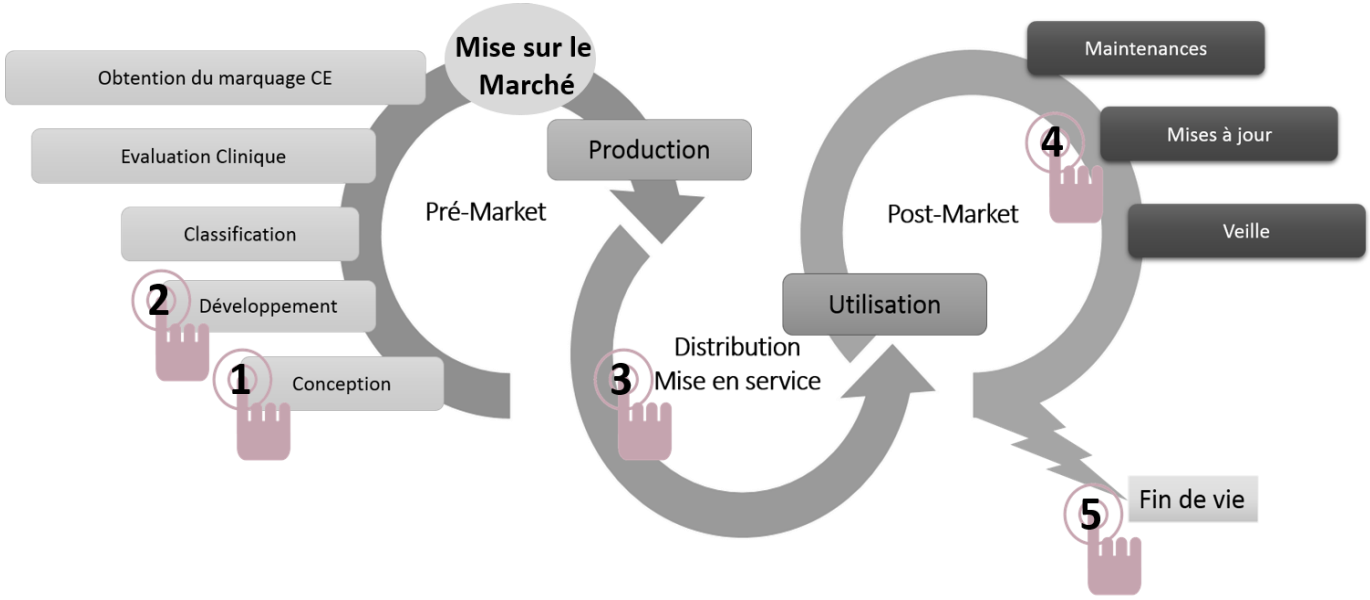


Figure 6 : Cycle de vie du logiciel

Compte tenu de la diversité des produits et de leur utilisation, il s'agit d'une liste de recommandations générales uniformisées pour l'ensemble des DMIL : DM, DIV et DMIA. Cependant, certaines recommandations ne pourront pas s'appliquer. Les recommandations sont récapitulées dans l'annexe A3.

1 Activité de conception du logiciel

Dispositions générales

[R1] Mettre en œuvre un processus de gestion des risques liés à la cybersécurité qui permettrait d'orienter et de justifier ce qui est mis en place pour garantir la protection du DM et de son environnement. L'analyse de risque liée à la cybersécurité fait partie du processus d'analyse de risques global. Ce processus doit être géré selon les exigences de l'ISO 13485. Elle constitue la première et la principale des recommandations. Toutes les autres recommandations vont découler de l'analyse de risque (Cf. partie II).

[R2] Il est recommandé de prendre en compte dans l'analyse de risque de cybersécurité, les risques provenant des outils logiciels utilisés durant le cycle de vie du DMIL.
Par exemple : logiciels en environnement de développement, logiciels de télémaintenance, logiciels de gestion de clés ou de licences.

[R3] Il est recommandé de proscrire la sécurité par l'obscurité (i.e. non divulgation d'information relative à la structure) et de mettre en place un contrôle de sécurité clair, transparent et bien documenté. En effet, la sécurité d'un système ne devrait pas reposer sur le secret de sa conception ou de sa mise en œuvre. Il faut considérer qu'un attaquant peut toujours avoir accès au fonctionnement interne d'un dispositif médical, notamment au code logiciel qu'il exécute (*par exemple, via des procédés de rétro-conception*), au secret d'un algorithme, d'un protocole. Le fabricant peut s'appuyer sur des standards et normes conformes à l'état de l'art en termes de cryptographie.

[R4] Il est recommandé de minimiser les fonctionnalités en ne conservant que les données, les composants logiciels, le code strictement nécessaires au bon fonctionnement du dispositif médical. La suppression des composants superflus participe à la réduction de la surface d'attaque exposée par le dispositif médical. Dans la mesure du possible, il est recommandé de désactiver les fonctions ou les logiciels qui ne sont pas nécessaires. Il est également préconisé au fabricant de minimiser la complexité de la partie sécuritaire du DMIL. Pour cela, un processus de segmentation du logiciel en zone critique et zone non critique peut être réalisé.
[R5] Il est recommandé de documenter les exigences en matière de sécurité sur la documentation de conception du logiciel. Ces exigences peuvent être soit de l'analyse fonctionnelle du logiciel soit de l'analyse de risques du logiciel (norme IEC 62304).

[R6] Il est conseillé de mettre en place une politique de gestion des achats, des composants logiciels et de la sous-traitance (« Acceptance Check » ou Processus de contrôle d'acceptabilité). La gestion des fournisseurs comprend de nombreux aspects tels que les contrôles de qualité, la mise à jour et la modernisation des feuilles de route, l'échange d'informations sur la sécurité y compris la notification des problèmes de sécurité des logiciels découverts par le vendeur[1].
Par exemple : *dans le cas de logiciels de type SOUP, leur utilisation doit être justifiée et une étude de leur sécurité doit être menée et prise en compte.*

[R7] Il est recommandé de prévoir dès la conception du produit, des moyens de remédiation (remise en condition de sécurité). *Par exemple* : update du firmware et des secrets (clés cryptographiques).
Il est proposé d'appliquer le principe de moindre privilège à l'ensemble des composants du dispositif médical et de s'efforcer de limiter au strict minimum les processus privilégiés.
Par exemple :
- Paramétrage par défaut des droits d'accès minimaux ;
- Accès à un appareil via un badge d'authentification définissant les droits et privilèges associés ;
- Limiter l'accès au compte administrateur.

Définir le contexte d'utilisation du DM

[R8] La destination d'usage est un élément essentiel à prendre en compte au moment de l'expression des besoins. Il est recommandé de trouver un équilibre entre le mécanisme d'authentification de l'utilisateur et la destination d'usage. Le fabricant doit définir la destination d'usage du DM, décrire et prévoir les différentes configurations possibles.
Par exemple : l'utilisation d'un logiciel DM dans un contexte d'urgence ne pourrait pas requérir les mêmes mécanismes d'authentification qu'un logiciel utilisé dans un cadre de non urgence.

[R9] Il est conseillé de prendre en considération l'environnement d'utilisation dès la phase de conception afin d'identifier les systèmes de contrôles appropriés.
Par exemple, le contrôle d'accès ne sera pas pensé de la même manière entre un logiciel utilisé à domicile et un logiciel d'un établissement de santé. Il sera plus exigeant à domicile. Par contre, le niveau de sécurité sera le même.

Contrôle des accès

[R10] Il est recommandé de définir clairement les rôles et les privilèges des acteurs/utilisateurs : tous les utilisateurs ne doivent pas avoir les mêmes droits. Les accès vont dépendre des fonctions des utilisateurs.

i. Les privilèges attribués aux utilisateurs peuvent être réduits au minimum nécessaire pour assurer les fonctions dédiées au rôle associé ;
ii. Les droits d'accès des utilisateurs peuvent être organisés selon des rôles/profils (administration, maintenance, …) ;

[1] Norme 13485 : Dispositifs médicaux - Systèmes de management de la qualité - Exigences à des fins réglementaires

iii. L'accès aux fonctions d'export de données du dispositif médical connecté peut être limité à des personnes dûment habilitées ;
iv. L'accès aux fonctions de mise à jour des logiciels ou de modification des paramètres sensibles pourra nécessiter une authentification forte des utilisateurs. Toute action de validation dans ces contextes pourra demander une double confirmation ;
v. Le dispositif médical connecté pourra comporter une fonction d'authentification des utilisateurs sur la base de comptes nominatifs. Les postes utilisateurs pourront être protégés en confidentialité et intégrité.
   En fonction des possibilités et de l'utilisation du DMIL, une politique d'authentification matérielle (badges, puces) ou multi-facteurs pourra être mise en place :
   a. Support physique (badge, carte à puce) ;
   b. Empreinte (information biométrique) ;
   c. Login/Mot de passe.

En cas d'utilisation d'un système de mot de passe, des précautions rigoureuses pourront être proposées : mot de passe robuste (nombre minimum de caractère, caractères spéciaux, changement périodique du mot de passe, périodicité définie dans la politique de gestion des mots de passe…) et sécurisé (contrôle du nombre de tentatives de saisie, période de renouvellement limitée, impossibilité de réutilisation d'anciens mots de passe, …).[1] Le dispositif médical doit être capable de mettre en œuvre la politique des hôpitaux en matière de mots de passe

Gestion des authentifications

[R11] Il est recommandé de réguler l'accès aux données et aux composants du système par une authentification préalable : authentification d'un utilisateur vis-à-vis du système, authentification d'un logiciel, authentification d'un message envoyé ou reçu par le DM, etc.
Par exemple : s'authentifier avant d'accéder à un DMIL à l'hôpital
En fonction du contexte d'utilisation, des éléments de contrôle pourront être rajoutés comme par exemple la vérification de la date de dernière connexion.

[R12] Un mécanisme d'authentification pourra être établi en accord avec le contexte d'utilisation du DM.
Par exemple : alléger l'authentification des DMIL utilisés dans un contexte d'urgence
Il est recommandé de suivre des préconisations pour la mise en place de mécanismes d'authentification.
Par exemple, l'accès au système dispositif médical connecté pourra nécessiter une authentification préalable en fonction de l'utilisation du DM

Hébergement

[R13] Les risques liés à l'hébergement doivent être pris en compte comme un des éléments du processus de maitrise de risques.
Le fabricant pourra donc fixer les conditions minimales d'hébergement du DMIL (proposition de service ou sous-traitance) afin de garantir la sécurisation des données. Il est proposé d'indiquer à l'utilisateur et dans sa documentation, ses préconisations en termes d'hébergement du logiciel DM en accord avec l'analyse de risques.
Par exemple:
- *Le logiciel DM communique avec des serveurs **locaux** ou partagés : un établissement de santé peut avoir l'applicatif en local et en donner l'accès à d'autres établissements de santé*
- *Le logiciel DM utilise des serveurs externes, en passant par des hébergeurs de données qui offrent ce service spécifique*

Le secteur de l'hébergement est très réglementé. Le fournisseur d'hébergement de données peut se référer à la règlementation de certification HDS[2] (Hébergeurs de données de santé).

[1] Authentification par mot de passe : les mesures de sécurité élémentaires (https://www.cnil.fr/fr/mot-de-passe)
[2] L.1111-8 du code de la santé publique (esante.gouv.fr > Rubrique Services > Hébergement des données de santé)
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_niveau_essentiel.pdf
http://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/procedures-pour-les-hebergeurs-de-donnees-de-sante

La DGOS a publié un mémento sur la cybersécurité à l'usage des directeurs d'établissements de santé[1]. La directive NIS[2] publiée au journal officiel le 19 juillet 2016 vise à « améliorer la capacité à résister à des cyber-attaques » des entreprises fournissant des « services essentiels », les OSE, ou opérateurs de services essentiels tels que les établissements de santé.

Par exemple : si un fabricant veut stocker les données dans le cloud, il devrait être vigilant au moyen de stockage des données et renvoyer vers la règlementation en la matière ou à des documents qui fixent la sécurité du cloud.
Si un fabricant vend un ensemble de services associés à un DM, il devra respecter les réglementations en lien avec ces services : dans le cas d'une prestation d'hébergement des données de santé, le fabricant doit respecter la réglementation HDS.

Environnement d'utilisation

[R14] On entend par environnement prévu du DMIL, les éléments logiciels dans lesquels il fonctionne et avec lesquels il interagit (systèmes d'exploitation, réseau d'établissement de santé etc.).
Il est recommandé que le DM soit le plus autonome possible dans sa sécurité. Pour cela, il est proposé de minimiser le nombre d'hypothèses sur l'environnement (exigence générale en matière de sécurité et de performance : Articles 17.4 et 16.4 de l'annexe I des règlements DM et DMDIV respectivement).

Le fabricant pourra préciser les hypothèses sur l'environnement pour un fonctionnement sécurisé de son dispositif médical. Il s'agit de vérifier que ses hypothèses de sécurité peuvent être satisfaites par l'environnement d'exécution du logiciel DM. Elles ne doivent cependant pas être abusives. Le fabricant ne peut pas faire reposer la sécurité de son DMIL exclusivement sur la sécurité de l'environnement. Il doit rechercher l'environnement prévisible de son DM et prescrire un niveau minimal d'exigence en termes de compatibilité.

[R15] Le bon fonctionnement du DMIL ne devrait pas freiner ou entraver l'application des exigences de sécurité de l'environnement d'exécution du logiciel DM Lors de la conception d'un nouveau DM, il est donc recommandé que le fabricant se conforme à l'état de l'art en utilisant les versions à jour de tous les composants y compris les OS.
Par exemple : empêcher l'établissement hospitalier de mettre à jour son parc de machine sous Windows 10, sous prétexte qu'un logiciel DM ne fonctionne que sous une version obsolète de Windows XP n'est pas acceptable.

[R16] Conformément aux exigences relatives au système de management de la qualité3, le fabricant est également incité à définir les compatibilités entre logiciels et matériels. Pour rappel, les incompatibilités doivent être au moins gérées et maitrisées et au mieux les plus réduites possibles. En effet, une incompatibilité est potentiellement un frein à la sécurité.
Les fabricants doivent faire de leur mieux pour maintenir la compatibilité avec des versions futures de l'OS. Il est donc souhaitable que le fabricant mette en place un suivi afin d'analyser la compatibilité avec les nouvelles versions de logiciels/ matériel. La garantit d'évolution est limitée dans le temps et précisée de façon contractuelle le plus souvent.

[R17] Le DM devrait pouvoir disposer de fonctions de base permettant d'intégration sécurisée. Plus précisément, le fabricant devrait anticiper et prévoir le fonctionnement du dispositif médical dans un environnement de fonctionnement sécurisé (de manière physique ou logique selon le DM - postes de travail type ordinateur, consoles de commande, dispositif médical au domicile du patient / ambulatoire, DM mobile) et utiliser des mesures de protection telles que :

- Le chiffrement des données sensibles (identifiées par l'analyse de risques au préalable) ;
- Prévoir la possibilité de cloisonnement du réseau pour contrer toute attaque numérique provenant de l'extérieur ;
- Avoir un accès physique règlementé et sécurisé (badge, login/mot de passe …) ;

[1] Lien: https://solidarites-sante.gouv.fr/IMG/pdf/dgos_memento_ssi_131117.pdf (page 18)
[2] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016

[3] Norme ISO 13485:2016 (fr), Dispositifs médicaux — Systèmes de management de la qualité — Exigences à des fins réglementaires

- Préconiser un environnement stable : le dispositif médical doit être relativement autonome en termes de sécurité (accès sécurisé au réseau) ;
- L'utilisation d'un anti-virus (ceci sera dépendant du DMIL concerné : en effet, l'utilisation d'un antivirus n'est pas recommandable dans tous les contextes).

Par contre, la mise en place dans l'environnement d'utilisation est de la responsabilité de l'utilisateur.

[R18] En fonction de la nature du DMIL, de l'utilisation prévue, de l'environnement opérationnel envisagé et du niveau de sécurité à atteindre qui en découle, les postes utilisateurs des dispositifs médicaux connectés devraient disposer de moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants. Pour cela, le fabricant peut proposer une configuration minimale sécurisée pour le poste de travail supportant le DM.
Dans ce sens, les logiciels spécifiques à la gestion des dispositifs médicaux connectés installés sur les postes utilisateurs devraient être compatibles avec des solutions de sécurité contre les codes malveillants.
Par exemple : Un DM qui est composé d'une station de travail et d'un logiciel devrait intégrer un anti-virus

[R19] En fonction du type de DMIL, un processus de durcissement du système d'exploitation pourra être mis en place ou proposé afin de bloquer ou de freiner les tentatives d'exécution de code arbitraire ou de programmes illégitimes sur le DMIL (segments de mémoire dédiés, exclusion mutuelle des privilèges de modification et d'exécution, mécanismes de protection de la pile d'exécution des processus, dispositif d'agencement aléatoire des zones mémoire, etc.).
[R20] En fonction du type de DM et de son degré d'intégration dans un système plus complexe, il est recommandé de proposer des mécanismes de cloisonnement.
Par exemple :
-en cas d'attaque réussie sur le DMIL, une vérification de l'intégrité du logiciel pourrait être réalisée et des mesures doivent avoir été prévues pour éviter la propagation à l'ensemble du système.
-cloisonnement entre l'interface graphique et les données critiques, cloisonnement entre le logiciel du DMIL et le reste du réseau.

L'impact de ces mécanismes de cloisonnement doit être évalué vis-à-vis d'éventuels autres mécanismes de cloisonnement, mis en œuvre pour la sécurité du patient.

Sécurité physique

[R21] Il est conseillé au fabricant de spécifier les mesures permettant d'assurer la sécurité physique du dispositif médical (accès physique) afin de garantir son utilisation en toute sécurité. Les éléments physiques dans lesquels il fonctionne et avec lesquels il interagit.(par exemple : l'accès à un port de maintenance d'un équipement médical, supprimer l'ensemble des connectiques non indispensables au fonctionnement du DM et de sécuriser l'accès aux interfaces restantes.) devraient être protégés et utilisables uniquement par les personnes habilitées. Ceci dépendra du type de dispositif médical.
Il faut souligner que certaines dispositions incombent au fabricant et d'autres aux utilisateurs comme la sécurité des locaux. Tout ce qui concerne la protection de l'accès relève bien du fabricant.

Cas du DM connecté à un réseau

[R22] Pour les dispositifs connectés à un réseau, il faudrait s'assurer de la maitrise des accès distants : seuls certains profils, définis en amont, pourraient se connecter à distance avec mise en place de moyens d'accès sécurisé (VPN, authentification double facteur, gestion des secrets, etc.).

[R23] La notice d'utilisation du dispositif médical connecté devrait comporter une matrice des flux réseau exhaustive (types de protocoles, origine/destination des flux, plan d'adressage…).

[R24] Les dispositifs médicaux connectés devraient comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, …). Dans ce sens, les logiciels spécifiques à la gestion des dispositifs médicaux connectés, installés sur les postes de travail, devraient être compatibles avec les solutions de sécurité de filtrage réseaux de type firewall personnel.

[R25] En cas de mise en œuvre de communications sans fil par exemple, Il est conseillé que le dispositif médical connecté soit conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode Wi-Fi, il est proposé de se référer aux documents de référence dans le domaine disponibles sur le site de l'ANSSI : Bonnes pratiques : sécuriser les accès Wi-Fi[1].

[R26] Si le type du DMIL le permet, il est recommandé de prévoir dès la phase de conception et en fonction de la finalité médicale, la capacité d'isoler le logiciel DM du réseau ou de tout moyen de communication en cas d'attaque ou de menace. Cette disposition ne devra pas affecter la disponibilité du DM.

[R27] Il est proposé la possibilité d'utiliser un réseau privé virtuel (VPN) pour préserver la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Ceci n'est pas applicable à tous les types de DMIL.
Par exemple, dans le cas d'un DMIL utilisé au domicile d'un patient, utilisation d'un VPN entre le DMIL à domicile et l'hôpital, afin de protéger les données échangées.
Les fabricants pourront se référer aux éléments de la **norme Communication de sécurité sur des systèmes de transmission [NF EN 50159]** qui recommande les défenses suivantes :

i. Numéro de séquence (anti-rejeu)
ii. Datation (anti-rejeu)
iii. Délai d'attente
iv. Identificateurs de source et de destination (= authentification)
v. Message en retour (intégrité)
vi. Procédure d'identification
vii. Code de sécurité
viii. Techniques cryptographiques[2].

[R28] Il est conseillé de s'assurer que toutes les communications soient sécurisées. Pour cela, il est recommandé de définir les mécanismes assurant :

i. Des critères de base : intégrité, confidentialité (utilisation de clé de chiffrement par exemple)
ii. Le non-rejeu des communications (dépend du DM et du contexte d'utilisation)
iii. L'authenticité des communications

Traçabilité et logs - journalisation

[R29] Le dispositif médical connecté devrait comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif médical connecté et de tout événement, notamment ceux pouvant avoir un impact critique sur son fonctionnement.

[R30] Il est proposé au fabricant d'indiquer dans sa documentation les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif médical connecté et les recommandations en matière de sauvegarde et d'exploitation des journaux. Ces éléments devront être protégés en intégrité.

Prévoir la surveillance pendant le fonctionnement du DM

[R31] Le fabricant est incité à vérifier dès la phase de conception, l'état de l'art relatif à la cybersécurité afin d'identifier les vulnérabilités connues pouvant affecter le produit (publications notamment).

[R32] Le dispositif médical connecté devrait comporter une fonction d'autocontrôle (contrôle d'intégrité) et une fonction d'alerte locale permettant de surveiller le bon fonctionnement, et tout événement pouvant avoir un impact critique sur son fonctionnement.
Par exemple : Vérification au démarrage que le code n'a pas été modifié, vérification de la signature au démarrage

[1] https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/
[2] https://www.ssi.gouv.fr/guide/cryptographie-les-regles-du-rgs/

[R33] Dans la mesure du possible, il est recommandé aux fabricants de concevoir leur DM en anticipant la nécessité pour tous les composants du DM (systèmes d'exploitation, matériels et logiciels) d' être tenus à jour afin qu'ils ne puissent pas propager des virus qui exploitent les faiblesses de versions obsolètes de ces systèmes d'exploitation (comme dans le cas de Mirai21, de ransomware, de vers, etc.)

[R34] Dans le cadre de l'intégration à un autre SI, Il est recommandé que le dispositif médical comporte une fonction d'alerte s'appuyant sur des mécanismes standards permettant au SIS de surveiller le bon fonctionnement du DM, les connexions au dispositif médical, et tout événement pouvant avoir un impact critique sur son fonctionnement (mise à jour du logiciel, modification de paramètre critiques,). La responsabilité du fabricant est de fournir les mécanismes de base qui vont permettre les opérations de surveillance, de contrôle. Par contre, il n'est pas du ressort du fabricant d'opérer ces mécanismes de contrôle.
Dans le cas de DM reliés à un réseau d'un établissement de santé, une mesure de maitrise des risques peut être la génération d'une alerte qui pourra être exploitée dans le dispositif de supervision des incidents de l'établissement.

Fonctionnement en mode dégradé

[R35] Certains dispositifs médicaux connectés peuvent disposer d'un mode dégradé (sécurisé) permettant d'assurer une fonction de reprise des données lors du retour en mode nominal. Le mode dégradé pourrait être déclenché lors de la détection d'une attaque ou lors de la détection de l'effet de l'attaque.
Pour certains types de DM, une continuité de service pourrait être proposée, en particulier pour les dispositifs portés ou implantés (Pacemaker *par exemple*). Des mécanismes garantissant la disponibilité des fonctions critiques même en cas de compromission de la sécurité ou de détection d'une altération de l'intégrité pourraient être mis en place.

[R36] La documentation produit remise ou mise à disposition du client devrait comprendre les procédures d'utilisation du produit en mode dégradé (protocole bien décrit et documenté), notamment :
- le périmètre fonctionnel du mode dégradé ;
- les éventuelles restrictions de performance ;
- les procédures de mise en œuvre du mode dégradé ;
- les procédures de retour au mode nominal.

Ces procédures pourraient éventuellement être adaptées au contexte du client.

Il est recommandé de prévoir :
- une identification du produit (numéro de série à minima)
- Comment entrer dans ce mode dégradé, c'est-à-dire les déclencheurs de ce mode après toute alerte de sécurité ou mauvais fonctionnement.
- Comment sortir du mode dégradé (via l'authentification forte d'une personne autorisée – à définir par le fabricant).

Activité de développement du logiciel DM

Choix DES REGLES de programmation

[R37] Le développement du logiciel DM devrait respecter des règles de programmation vérifiées automatiquement par une inspection continue. Ceci permet d'automatiser les détections des vulnérabilités. L'objectif est de produire un logiciel "Sécurisé par construction". Des outils open source, propriétaires ou personnalisés peuvent être utilisés. Ces outils devraient vérifier les propriétés décrites dans les standards reconnus MISRA C/C++, CWE, SANS Top 25, OWASP,… par exemple

[R38] Si le choix des règles de programmation est à l'initiative du fabricant, il devrait être justifié et les règles de spécifiées dans le système qualité du développeur (politique de sécurité de développement du logiciel avec des guides internes). L'objectif est de répondre aux bonnes pratiques en termes de qualité et sécurité.
Par exemple, un langage qui dispose d'un mécanisme de typage fort des données permet d'éviter certaines erreurs.

[R39] Il est préconisé de s'assurer de l'intégrité du code source développé ainsi que de la traçabilité des modifications apportés au code source (procédure de maitrise des environnements de développement). Une intrusion sur l'environnement utilisée pour le développement (poste de développement, gestionnaire de code source, ...) du logiciel du DM permettrait d'introduire des vulnérabilités.

Méthodes de vERIFICATION

[R40] Il est recommandé au fabricant de spécifier les fonctions logicielles attendues. Il peut développer des procédures et des types de tests associés à chaque fonction (Requirement Based Testing, Analyse de codes).
Lors de l'exécution des tests, il est proposé de mesurer la couverture structurelle du code par ces tests. Le code mort (code non utilisé et non testable) devrait être supprimé.

[R41] Il est recommandé d'appliquer des méthodes et outils de vérification appropriés :
- pour s'assurer l'absence de vulnérabilités dans le logiciel
- pour minimiser les risques d'apparitions d'anomalies et s'assurer que le logiciel est conforme aux spécifications.

[R42] Le fabricant est encouragé à soumettre son DM à un processus d'évaluation de la sécurité (CSPN ou Critères communs comme proposé par l'ANSSI1, Cybersecurity Act). Cette évaluation doit être réalisée avant la mise sur le marché du dispositif médical, puis actualisée à chaque révision majeure du dispositif médical.

Démarrage sécurisé et intégrité des mémoires et des données sensibles

[R43] Les dispositifs médicaux connectés devraient disposer d'une fonction permettant de vérifier l'intégrité et l'authenticité des logiciels et des données critiques du dispositif médical au démarrage et lors de son fonctionnement.

[R44] Le dispositif médical devrait disposer d'une fonction d'affichage de la dernière version des logiciels en cours d'utilisation et des données sensibles. Ceci s'applique également lors du processus de mise à jour.

[1] https://www.ssi.gouv.fr/administration/produits-certifies/cspn/, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/

[R45] Il est recommandé que le système dispositif médical connecté fournisse une interface permettant d'obtenir la configuration du système dispositif médical connecté et son état de fonctionnement.

Mécanisme de protection du DM

[R46] L'auto surveillance du DM inclut la mise en place d'un mécanisme d'autotest réalisé au démarrage du dispositif médical ainsi qu'au cours de son fonctionnement. Le principe serait donc de prévoir des contrôles en intégrité au moment approprié et aussi souvent que possible qui dépendra du type de DMIL concerné.
Par exemple

- Contrôles d'intégrité du firmware (Secure boot) réalisés au démarrage ;
- Contrôle d'intégrité de la mémoire lors de chaque accès au stockage permanent (NVM, stockage de masse) ;
- Auto surveillance de l'intégrité des logiciels réalisés à chaque démarrage ou activation par exemple ;
- Auto-surveillance de l'intégrité matérielle réalisée au démarrage ;
- Auto surveillance de la batterie d'un DM ;

[R47] Le fabricant doit envisager les cas où il est pratique d'utiliser des capteurs d'intégrité, d'intrusion ou d'attaque (capteur de lumière, détecteur de changement de température, détecteur d'ouverture d'un DM, etc.) pour détecter les anomalies en cas de mauvaise utilisation ou en cas d'attaque.

Si une anomalie est détectée, le dispositif médical émet une alerte et pourrait réagir suivant les spécifications en basculant d'un mode de fonctionnement standard à un mode de sécurité (mode dégradé sûr ou arrêt suivant le DM)
Par exemple : dispositifs scellés, les circuits intégrés sécurisés équipés de capteurs de conduite avec mode dégradé en cas d'alerte

Documentation

[R48] La documentation devrait mentionner la liste de l'ensemble des composants matériel (hardware) et logiciels (versions, système d'exploitation) constituant le dispositif médical. Ces informations pourront être accessibles soit *via* un espace utilisateur en ligne, soit sur format papier.
Elle devrait notamment préciser en fonction du DMIL:
-l'identification des composants
- les caractéristiques du poste d'administration du dispositif médical connecté : caractéristiques hardware, versions du système d'exploitation, middleware et pilotes, périphériques, etc… ;
- les caractéristiques des postes dédiés aux opérations d'utilisation : caractéristiques hardware, versions du système d'exploitation, middleware et pilotes, périphériques, etc… ;
- les spécifications du logiciel, l'exécutable et les procédures de test et les résultats.

Remarque : Ces recommandations peuvent être appliquées à chaque phase du cycle de vie du DMIL.

Mise en production et processus de validation

[R49] Il est conseillé au fabricant de fournir une liste de vérification de mise en production. Il met à disposition des intégrateurs, un référentiel d'exigences et de recommandations de sécurité relatives à l'intégration du DM au sein d'un système d'information de santé. Ce document serait actualisé à chaque révision majeure du DM.
Il est conseillé au fournisseur et/ou fabricant de n'installer que les logiciels nécessaires et de n'activer que les services indispensables au bon fonctionnement du dispositif médical connecté.
[R50] Dans le processus d'intégration des prestations externalisées (sous-traitants, gestion des achats, incorporation des SOUP), il est conseillé de mettre en place un système de contrôle de conformité (« acceptance check »). Pour cela, les spécifications devraient avoir été définies en amont et

l'intégration d'un élément ne devrait être validée qu'après vérification qu'il répond bien aux spécifications. Il s'agit de ne pas intégrer des éléments externes à l'aveugle.
Par exemple : librairies SSH : identification de failles dans certaines versions des librairies SSH, utilisation de librairies éprouvées en cas d'intégration d'un SOUP.

[R51] Interdire l'importation de données n'étant pas souhaitable, Il est proposé de mettre en œuvre des actions pour que celle-ci soit maitrisée. Il s'agit également d'une démarche de type contrôle de conformité (« acceptance check »). Il est recommandé que l'importation des données :
- fasse partie intégrante de l'analyse de risque du fabricant. *Par exemple* : réaliser une évaluation des risques liés à l'utilisation de supports physiques capables de détruire le système (USB killer) ;
- soit contrôlée : le fabricant est incité à prévoir un système de filtrage des données importées sur le DM (innocuité des données importées dans le DM). *Par exemple :* dans le cas d'une utilisation d'une clé USB sur un poste de travail connecté à un appareil IRM, il est recommandé que les données soient chiffrées ou qu'un système de détection des codes malveillants ait été prévu.

Mise en service – 1ère utilisation

Gestion des paramétrages initiaux et des configurations

[R52] Il est recommandé que les étapes de configuration et de paramétrage initial soient prévues et qu'elles soient accord avec l'analyse de risques globale qui aura été faite en amont (modalités définies par le fabricant)
Par exemple :
- Lors de la mise en service, les mots de passe par défaut doivent être changés l et être spécifiques à chaque utilisateur (processus automatique qui impose le changement)
- La diversification des clés cryptographiques est à prévoir en fonction de l'environnement d'utilisation.
- Le fabricant ne doit pas conserver de compte « constructeur » connu uniquement de celui-ci. La liste des comptes doit être connue et maitrisée par le propriétaire du DMIL.
- Dès la conception, il convient d'appliquer le principe « une clé, un usage ».
- Il est possible de mettre en place des solutions antivirales à condition que les antivirus n'entravent pas le bon fonctionnement du DM (Disposition non applicable aux DMIA par exemple).
- Les mises à jour doivent être prévues le plus souvent possible et notamment lors de l'étape d'installation/initialisation. En particulier, une mise à jour initiale doit être prévue pour les DMs potentiellement stockés durant une longue période entre la livraison et l'utilisation.

Dispositif de protection de l'intégrité du DM

[R53] Le DM devrait inclure un mécanisme de vérification de l'intégrité au démarrage. Il est conseillé au fabricant de fournir à l'utilisateur la liste des précautions à prendre lors de la phase de démarrage en fonction du type d'installation et du type de DM concerné. Les précautions vont dépendre du nombre de systèmes connectés, de leur utilisation, de l'arborescence des réseaux.
Par exemple, les précautions à prendre seront différentes entre un dispositif médical unique connecté au réseau du SI et un dispositif médical relié par un serveur à un sous-réseau du SI permettant un pilotage à distance du matériel, lui-même connecté par internet au système de télémaintenance.

Intégrer l'aptitude à l'utilisation / prendre en compte l'utilisateur

[R54] Il est conseillé au fabricant de mettre en place les mesures pour contrer les menaces et de les intégrer dans son plan de développement à l'aptitude à l'utilisation[1].

Les négligences/mésusages ne sont pas le fruit d'actions malveillantes, mais leurs effets peuvent être similaires à ceux des attaques. Elles peuvent créer des vulnérabilités qui pourront être exploitées par des attaquants ou simplement affecter la disponibilité des systèmes.
Exemples
- *La modification involontaire des réglages des messages d'avertissements d'alarme peut avoir des conséquences désastreuses sur la qualité des produits, des services délivrés, l'environnement, la santé ou la sécurité des personnes.*
- *L'utilisation d'une clé USB pour transférer des données entre des systèmes isolés peut entrainer une indisponibilité des systèmes si cette clé est porteuse de virus.*

Dans ces deux cas, issus d'expériences réelles, les intervenants n'ont pas eu la volonté de nuire. Cependant, les impacts sur les installations ont été bien tangibles.
Ces négligences peuvent avoir pour cause un manque de formation du personnel et d'information sur les enjeux. Les mesures de sécurité devraient être adaptées à des utilisateurs non sensibilisés à la sécurité et validées avec de tels utilisateurs. Il est donc recommandé d'associer les utilisateurs à la démarche de sécurité. Le logiciel devrait être pensé en matière d'accessibilité et d'ergonomie. Il devrait en découler un plan de formation adapté.

[1] EN IEC 62366-1 sur le processus d'ingénierie d'aptitude à l'utilisation

[R55] Il est conseillé au fabricant de prendre en compte l'utilisation du DM en situation d'urgence même en cas de menace.

[R56] Les prestations de services nécessaires à la bonne mise en œuvre du dispositif médical devraient être définies : besoins des utilisateurs en matière de formation, d'installation, de mise en production, d'appui à l'exploitation du système, d'assistance à la rédaction de documentations et d'assistance au paramétrage.
Plusieurs types d'utilisateurs devraient être distingués :

- Le technicien de maintenance, qui n'est ni l'utilisateur, ni un professionnel de santé, ni le fabricant ;
- Les utilisateurs finaux du DM qui vont utiliser le matériel de manière quotidienne ;
- Le ou les utilisateurs ayant des droits étendus qui auront en charge l'assistance de premier niveau en cas d'absence du fabricant sur place et suivront la qualification des changements (matériels ou logiciel). En pratique, c'est souvent l'ingénieur biomédical sur site qui remplit ce rôle. C'est au fabricant de prévoir une formation adaptée et spécifique à ces utilisateurs.

4 Surveillance – Gestion post-commercialisation

Les technologies évoluant sans cesse, il n'est pas possible d'identifier dès le départ l'ensemble des vulnérabilités d'un dispositif médical tout au long de son cycle de vie. Un suivi post-commercialisation de l'apparition de nouvelles failles est une démarche proactive indispensable afin de pouvoir agir en conséquence et réduire le risque patient.

Gestion des incidents et actions correctives

Pour rappel, il existe plusieurs moyens de déclaration des incidents de sécurité informatique en France.

Portail	Incidents	Acteur	Lien
ANSM	Signalement des incidents impliquant les dispositifs médicaux et dispositifs médicaux de diagnostics *in vitro*	Patient Professionnel de santé Fabricant / distributeur	materiovigilance@ansm.sante.fr
Ministère des solidarités et de la santé	Signalement des événements sanitaires indésirables liés aux produits de santé, produits de la vie courante et actes de soins	Patients consommateurs ou usagers	Signalement-sante.gouv.fr
ANS Santé	Incidents de sécurité informatique ou liés aux nouvelles technologies	Utilisateurs	https://www.cyberveille-sante.gouv.fr/
ANSSI	Déclaration d'une faille de sécurité ou d'une vulnérabilité	Utilisateurs	https://www.ssi.gouv.fr/

De plus, le « Cybersecurity Act » (**Règlement (UE) 2019/881 du parlement européen et du Conseil du 17 avril 2019)** demande explicitement aux fabricants de mettre en place un système de surveillance des vulnérabilités. D'autre part, dans le cadre de la certification des dispositifs médicaux, chaque fabricant doit proposer un système d'enregistrement des vulnérabilités.

[R57] Les nouveaux règlements DM et DMDIV définissent les prérogatives en termes de notification des incidents graves et les mesures correctives de sécurité. Elles sont détaillées de la manière suivante respectivement aux articles 87 et 82 des règlements DM et DMDIV :
« Les fabricants de dispositifs mis à disposition sur le marché de l'Union (…) notifient aux autorités compétentes concernés (…) les éléments suivants :

a) Tout incident grave concernant des dispositifs mis à disposition sur le marché de l'Union, à l'exception des effets secondaires attendus qui sont clairement documentés dans les informations relatives au produit et quantifiés dans la documentation technique et qui font l'objet d'un rapport de tendances en application de l'article 88 ;
b) Toute mesure corrective de sécurité prise à l'égard de dispositifs mis à disposition sur le marché de l'Union, ainsi que toute mesure corrective de sécurité prise dans un pays tiers concernant un dispositif qui est aussi légalement mis à disposition sur le marché de l'Union, lorsque la raison justifiant la mesure ne concerne pas exclusivement le dispositif mis à disposition dans le pays tiers ».

Les fabricants doivent donc signaler, tout incident ou risque d'incident concernant un dispositif médical ou dispositif médical de diagnostic in vitro. Ils fournissent également tous les éléments nécessaires à l'instruction du dossier : réponses aux questions complémentaires dans le délai demandé, et rapport final sous 60 jours. Le rapport doit contenir l'analyse permettant de justifier que les mesures prises sont adaptées ou de justifier l'absence de mesure (analyse des causes, fréquence…).

Les procédures et formulaires de déclaration (MEDDEV) sont disponibles sur le site de l'ANSM[1]. Il s'agit d'un processus continu de recueil, d'enregistrement, d'identification, de traitement, d'évaluation et d'investigation d'incidents ou d'effets indésirables liés à l'utilisation des produits de santé. L'objectif est

[1] https://ansm.sante.fr/documents/reference/declarer-un-effet-indesirable/comment-declarer-si-vous-etes-fabricant-ou-distributeur-de-dispositifs-medicaux

d'exercer une surveillance sur la sécurité d'emploi de ces produits et prévenir tout risque lié à leur utilisation par la mise en place d''actions correctives et/ou préventives.

[R58] Analyser l'ensemble des incidents impliquant le dispositif médical remontés par les utilisateurs.

[R59] Assurer un suivi permanent des vulnérabilités liées aux composantes matérielles et logicielles mises en œuvre dans les produits. Ce suivi doit intégrer l'ensemble des dépendances logicielles. La totalité des incidents doit être répertoriée. Ce suivi est nécessaire à la mise en place d'actions correctives
Pour les vulnérabilités qui ne pourraient pas être corrigées, un système de traçabilité devrait être mis en place. Il pourra décrire les raisons d'une absence de correctif pour un suivi sur le long terme.

[R60] Il est recommandé aux fabricants de créer un programme de divulgation des vulnérabilités pour faciliter la coopération avec les différents acteurs impliqués dans la sécurité.
Quand le fabricant a connaissance d'un risque d'incident (mise en évidence d'une vulnérabilité et/ou d'une menace), il y a toujours un risque que cette vulnérabilité soit exploitée. L'anticipation via un système de veille apparait donc essentielle. Les fabricants devraient être à l'écoute de l'ensemble des vulnérabilités identifiées, mettre en place sans délais des mesures correctives et diffuser des bulletins de sécurité des failles critiques lorsqu'elles sont identifiées.

Par exemple, un processus de gestion des anomalies des SOUP doit être effectif pour rattraper les vulnérabilités publiées par les éditeurs des SOUP (norme IEC 62304).

Modalités de Mise à jour / maintenance du logiciel

[R61] Il est recommandé de mettre en place une fonction de mise à jour sécurisée des logiciels permettant de garantir leur authenticité et leur intégrité. Les acteurs impliqués dans les procédures de mise à jour devraient être clairement identifiés. Leurs rôles sont définis. Une authentification forte lors de la mise à jour est fermement recommandée. De plus, lors des mises à jour de logiciels, il est recommandé de vérifier l'intégrité du firmware.

[R62] En cas de retrait de produit ou de nécessité de maintenance, les DMIL connectés doivent pouvoir envoyer un message d'alerte à l'utilisateur afin qu'il prenne les dispositions nécessaires au rappel ou à la mise à jour corrective.

Conduite à tenir en cas d'alerte de sécurité

En cas de détection d'une attaque, c'est bien l'utilisateur qui va agir. En revanche, il est conseillé au fabricant d'avoir prévu un plan d'action documenté afin que l'utilisateur ne se retrouve pas bloqué devant un message d'alerte.

[R63] Après une attaque ou une tentative d'attaque, le DM doit continuer à répondre aux critères de sureté et de sécurité. Quatre éléments devraient être pris en considération :

1. S'assurer du fonctionnement sûr du DM pour le patient (ou pour le SI de l'établissement de santé) ;
2. S'assurer de la disponibilité du DM : pour cela, mettre en place un mode dégradé ou l'isoler du système ;
3. Contrôler l'intégrité et la confidentialité des données du DM (la vérification de la cohérence pré/post-attaque permet de s'assurer que l'intégrité des données est préservée) ;
4. Informer l'utilisateur.

Le déclenchement d'un signal d'alerte va conduire au déclenchement du mode dégradé. Il s'agit du mode minimal qui garantit la sécurité du patient. Le mode dégradé est maintenu jusqu'à mise en place d'actions correctives permettant une remise en condition de sécurité du dispositif médical. Il est également recommandé au fabricant de définir un plan de continuité d'activité (PCA) permettant d'assurer la disponibilité des informations quels que soient les problèmes rencontrés. Il devrait également prévoir un plan de reprise d'activité après un incident.

Par exemple : pompes à insuline → en cas d'attaque, déclenchement d'un mode de fonctionnement autonome (débit préprogrammé) avec émission d'une alerte.

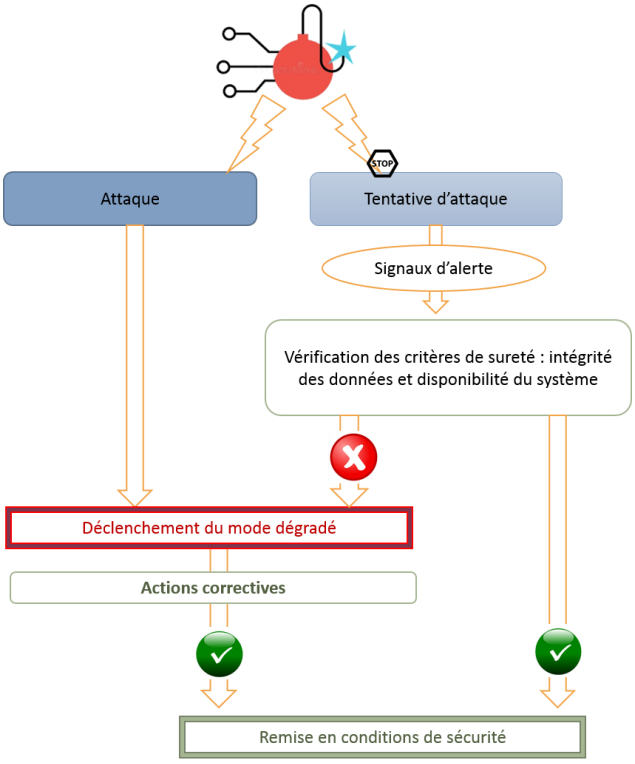


Figure 8 : plan d'action en cas d'alerte de sécurité

Fin de vie du DMIL

Différentes situations peuvent entrainer la fin de vie d'un logiciel :
- Le logiciel n'a plus vocation à être utilisé (expression de besoin) ;
- Une migration des données sur un autre support ou un autre DM est nécessaire : migration sur un système plus performant, récent ;
- Le logiciel et/ou le matériel devient obsolète par rapport aux évolutions de possibilités, capacités en termes de réglage, ajustements automatisés etc.

Si la partie logiciel du DMIL est obsolète, c'est-à-dire qu'elle ne peut être ni remplacée ni mise à jour, on considèrera que l'ensemble du DM est obsolète.

La fin de vie des composants tiers du DM (systèmes d'exploitation, bases de données, COTS etc.)

[R64] La fin de « vie » des éléments logiques et physiques qui composent le DM devrait être pensée dès la phase de conception. Il s'agit de gérer la fin de support des logiciels tiers (COTS) utilisés dans le DM. Il est conseillé au fabricant d'être en mesure de garantir ses supports dans la durée.

Il est donc proposé au fabricant d'anticiper la fin du support des logiciels tiers utilisés au sein de leurs produits.
Par exemple, si le système d'exploitation permettant d'utilisation du logiciel dispositif médical était Windows XP, il fallait prévoir, dès la conception, le moment où Windows XP serait obsolète. Aujourd'hui, la durée de vie d'un système d'exploitation étant en moyenne de 6 à 8 ans (création, maintenance, fin de maintenance), dans le cas des DM ayant une durée de vie de 10 ans, la problématique de la mise à jour du système d'exploitation va se poser.

La gestion de la fin de vie des données du DM

[R65] En amont de l'effacement des données et selon le type de DM et son utilisation, il peut s'avérer nécessaire de transférer les données du DM et de les récupérer en vue d'un stockage ou d'une réutilisation (réversibilité). Le mécanisme d'extraction des données vers un autre système devrait être sécurisé. Conformément au RGPD[1], le droit à la portabilité s'inscrit comme un principe de base.
Le transfert de données (virtuel ou sur du matériel) est un point de vulnérabilité. Il devrait donc être effectué dans des conditions de sécurité. Ceci nécessite la mise en place d'une procédure de portabilité des données et de bonnes pratiques en termes de cryptographie.

[R66] Lors de l'utilisation d'un DM, des données sensibles peuvent être stockées sur différents supports matériels informatiques (ex : disques durs, bandes magnétiques, clés USB, CD, DVD, ...), ou sur un serveur distant.
Il est conseillé au fournisseur de mettre en œuvre des fonctions de sécurité d'effacement des données conformes aux exigences en vigueur dans les bonnes pratiques. Par exemple : Le chiffrement intégral des supports de stockage.
L'effacement des données d'un support pose des difficultés de réalisation. Le chiffrement intégral des supports de stockage renforce la sécurité de ce type de procédure. A court terme, il suffit « d'oublier » la clé ayant servi à chiffrer les données sur le support de stockage, qui ne représente que quelques octets. Pour se protéger des progrès de la cryptographie à plus long terme, on appliquera quand même les procédures habituelles d'effacement par surcharge.
[R67] Le respect de l'article L.1111-8 du code de la santé publique, relatif aux hébergeurs de données de santé, est une base obligatoire[2]. De plus, le cas échéant, le fabricant pourra s'appuyer sur le référentiel SecNumCloud[3].

[1] https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf;
http://references.modernisation.gouv.fr/sites/default/files/RGS_fonction_de_securite_Confidentialite_V2_3.pdf;
http://references.modernisation.gouv.fr/sites/default/files/RGS_PC-Type_Confidentialite_V2_3.pdf
[2] L.1111-8 du code de la santé publique ; esante.gouv.fr > Rubrique Services > Hébergement des données de santé
[3]https://www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/

Le matériel

[R68] Une fois que l'on a géré les données contenues dans le DM, à savoir transfert et/ou effacement de ces données, le recyclage du matériel pourra se faire en sécurité.
L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a également publié des recommandations en matière d'effacement de supports de stockage magnétiques (disques durs ou bandes magnétiques) et non-magnétiques (clés USB ou cartes SD par exemple) ayant contenu des informations sensibles (références nº 1 et 2) :

- Recommandation : « Effacement des supports de stockage de masse » ;
- Guide : « GUIDE TECHNIQUE pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter ».

REFERENCES BIBLIOGRAPHIQUES

- ANSM. REALISATION D'UNE ETUDE SUR LA SECURITE DES LOGICIELS. 2015
- ANSSI. MAITRISER LA SSI POUR LES SYSTEMES INDUSTRIELS. VERSION 1.0 JUIN 2012.
- ANSSI. REFERENTIEL GENERAL DE SECURITE LISTE DES DOCUMENTS CONSTITUTIFS.
- BSI. CYBERSECURITE DES DISPOSITIFS MEDICAUX RICHAR PIGGIN 2017
- COLLECTIF RSSI ET INGENIEURS BIOMEDICAUX DES ETABLISSEMENTS DE SANTE EXIGENCES DE SECURITE DES SYSTEMES D'INFORMATION POUR LES EQUIPEMENTS BIOMEDICAUX
- COLLECTIF RSSI ET INGENIEURS BIOMEDICAUX DES ETABLISSEMENTS DE SANTE EXIGENCES DE SECURITE DES SYSTEMES D'INFORMATION POUR LES EQUIPEMENTS BIOMEDICAUX DES ETABLISSEMENTS DE SANTE
- DGA. REFERENTIEL D'EXIGENCES D'INGENIERIE DES LOGICIELS ET COMPOSANTS ELECTRONIQUES COMPLEXES POUR LA PRISE EN COMPTE DE LA SURETE DE FONCTIONNEMENT
- DGOS. CONNAITRE VOS RISQUES POUR MIEUX Y FAIRE FACE EDITION 2017
- DGOS. INTRODUCTION A LA SECURITE DES SI EN ETS DE SANTE NOVEMBRE 2013
- DGRIS. EVOLUTIONS DE LA CYBERSECURITE: CONTRAINTES, FACTEURS, VARIABLES JUIN 2015
- FDA WORKSHOP, ANURA FERNANDO PRINCIPAL ENGINEER NORMS. ESTABLISHING A BASELINE OF CYBERSECURITY HYGIENE. FDA.GOV.
- FDA. CONTENT OF PREMARKET CYBERSECURITY. 2014.
- FDA. CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE. 2005.
- FDA. POSTMARKED MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES. 2016.
- ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. NF EN ISO 14971 DISPOSITIFS MEDICAUX APPLICATION DE LA GESTION DES RISQUES AUX DISPOSITIFS MEDICAUX.
- LNE. CYBERSECURITE DES DISPOSITIFS MEDICAUX: PANORAMA DE LA REGLEMENTATION EN VIGUEUR LETTRE D'INFORMATION
- MCCARTHY TETRAULT. GESTION DES RISQUES LIES A LA CYBERSECURITE VERSION 3 JANVIER 2017
- PARLEMENT ET CONSEIL EUROPEEN. RGPD REGLEMENT (UE) 2016/679 DU 27 AVRIL 2016 RELATIF A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES. 2016.
- PARLEMENT ET CONSEIL EUROPÉEN. REGLEMENT (UE) 2017/745 DU 5 AVRIL 2017 RELATIF AUX DISPOSITIFS MEDICAUX. 2017.
- PGSSIS, ANS SANTE. GUIDE PRATIQUE REGLES POUR LES DISPOSITIFS MEDICAUX CONNECTES D'UN SYSTEME D'INFORMATION DE SANTE. NOVEMBRE 2013.
- PGSSIS, ANS SANTE. REFERENTIEL QUALITE HOPITAL NUMERIQUE. VERSION 1.1 OCTOBRE 2015.
- REV MED SUISSE. CYBERSECURITE DES DISPOSITIFS MEDICAUX : POINT SUR LA MENACE REELLE ET ROLE DU CORPS MEDICAL 2016
- SANTE, ANS. GUIDE PRATIQUE SPECIFIQUE A LA DESTRUCTION DE DONNEES LORS DU TRANSFERT DE MATERIELS INFORMATIQUES DES SYSTEMES D'INFORMATION DE SANTE (SIS)
- SANTE, ANS POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION DE SANTE (PGSSIS) DECEMBRE 2014 V1.0. 2014.
- SANTE, ANS. REGLES POUR LES INTERVENTIONS A DISTANCE SUR LES SYSTEMES D'INFORMATION DE SANTE. DECEMBRE 2014 V1.0.

ANNEXE 1 : LISTE DES INSTITUTIONS

- ANSM : AGENCE NATIONALE DE SECURITE DU MEDICAMENT ET DES PRODUITS DE SANTE
  - HTTPS://ANSM.SANTE.FR/
- ANSSI : AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION
  - HTTPS://WWW.SSI.GOUV.FR/
- ANS : AGENCE DU NUMERIQUE EN SANTE
  - HTTP://ESANTE.GOUV.FR/
- CNIL : COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTES
  - HTTPS://WWW.CNIL.FR/FR
- DGOS : DIRECTION GENERALE DE L'OFFRE DE SOINS
  - HTTPS://SOLIDARITES-SANTE.GOUV.FR/MINISTERE/ ORGANISATION/DIRECTIONS/ARTICLE/DGOS-DIRECTION-GENERALE-DE-L-OFFRE-DE-SOINS
- DSSIS : DELEGATION A LA STRATEGIE DES SYSTEMES D'INFORMATION DE SANTE

https://solidarites-sante.gouv.fr/ministere/ organisation/directions/article/dssis-delegation-a-la-strategie-des-systemes-d-information-de-sante

- ENISA : EUROPEAN UNION AGENCY FOR CYBERSECURITY
  - HTTPS://WWW.ENISA.EUROPA.EU/

ANNEXE 2 : NORMES ET TEXTES REGLEMENTAIRES

Normes relatives aux DM

Europe et International

- Règlement DM UE 2017/745
- ISO TR 11633 : Informatique de santé - Management de la sécurité de l'information pour la maintenance à distance des dispositifs médicaux et des systèmes d'information médicale
- ISO 62366 – usability engineering of medical devices
- IMDRF SaMD
- FDA : Guidance for the content of Premarket submissions for management of Cybersecurity in medical devices Oct 2nd, 2014.
- FDA : Postmarked Management of Cybersecurity in Medical Devices
- FDA : Cybersecurity for Networked Medical Devices Containing Offthe-Shelf (OTS) Software (2005)
- IEEE Canada : Building Code for Medical Devices of the 21st Century – Cyberlex / Recommantations de Sociétés Savantes
- Building code for MD software security – IEEE (institute of Electrical and Electronic Engineers)
- AAMI TIR 57 :2016 principles for MD security – risk management
- AUTOAA-A2 information technology security for In vitro diagnostic instruments and software systems – Approved standards – second edition

France

- NF EN ISO 14971 : Application de la gestion des risques aux DM
- NF EN 60601 – 1 (exigences sur intégration d'un DM dans un réseau informatique) Art 14.13
- NF EN 62304 : Logiciels de dispositifs médicaux - Processus du cycle de vie du logiciel
- NF – EN 80001 : Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux
- PGSSIS - Guide sur les dispositifs connectés d'un SI de Santé *(contexte hospitalier, hors ambulatoire, et la cyber sécurité fait partie du périmètre des recommandations, mais pas uniquement)*
- Exigences de sécurité des SI pour les équipements biomédicaux des ES (collectif RSSI et ingénieurs biomédicaux des ES) *(adressé aux établissements de santé, recommandations de coopération entre RSSI et Ingénieurs Biomédicaux)*
- Etude sur la sécurité des logiciels de DM : analyse de la complétude normative de la norme NF EN 62304 et Recommandations ANSM pour compléter cette norme sur les aspects *security (aspects non intégrés dans la 62304 actuellement)*

Normes issus d'autres domaines

Europe et International

- ITU (International Telecommunication Union) Global Cybersecurity Agenda (GCA)
- Framework for Improving Critical Infrastructure Cybersecurity – NIST (National Institute of Standards and Technology)
- ISO 27032 : Technologies de l'information - Techniques de sécurité - Lignes directrices pour la cybersécurité
- NF ISO 27000 : Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Vue d'ensemble et vocabulaire
- NF ISO 27005 : Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information
- ISO 27001 : Management de la sécurité de l'information (système, pas produit)
- ISO 27018 : Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.
- NF EN 50519 - Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission
- ISO 15802 : Technologies de l'information - Télécommunications et échange d'information entre systèmes. Réseaux locaux et métropolitains. Spécifications communes - Partie 3 : points de contrôle d'accès au support
- Maîtrise des accès : Protocole IEEE 802.1X - Port Based Network Access Control

- Cybersecurity Act : Règlement du Parlement européen et du Conseil du 17 avril 2019 concernant l'ENISA et la certification en matière de cybersécurité des technologies de l'information et des communications
- ISO/IEC 27002
- IEC 62443
- ISO/IEC 15408
- ISO 25010
- ISO/IEC 27001 (Non MD)
- ISO/IEC82394

France

- PGSSIS : Règles pour les interventions à distance sur les SI de santé (télémaintenance)
- PGSSIS - Guide gestion des terminaux nomades
- Référentiel HAS Objets Connectés (GT 28)
- Label France Cyber sécurité
- Décret 2016-1214 (obligation de déclaration des incidents graves de sécurité des SI)
- ANSSI : Exigences de cyber sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels (Mars 2016)
- ANSSI : Maîtriser la SSI pour les systèmes industriels (Juin 2012)
- ANSSI : Référentiel Général sur la Sécurité
- ANS Santé : Référentiel Qualité Hôpital Numérique
- RGPD,
- Loi informatique et liberté,
- Loi santé (et notamment les exigences HDS),
- Déclinaison française de la directive NIS (Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret no 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

ANNEXE 3 : TABLEAU RECAPITULATIF DES RECOMMANDATIONS

[R1] Analyse de risques Identification des **Biens critiques à protéger** A mimima : le firmware, le paramètrage médical, les clés cryptographiques, le journal d'événement, les données relatives aux patients	**Index [Rx]**	Définir les **vulnérabilité et risques associés** **Confidentialité = C** **Disponibilité = D** **Intégrité = I** **Auditabilité = A**	**RECOMMANDATIONS** > Proposer des **systèmes de protection**

Recommandations	N°	Objectifs de sécurité		Mesures
DISPOSITIONS GENERALES	[R2]	DI	PREVENIR LIMITER	Prendre en compte les risques provenant des outils logiciels utilisés durant le cycle de vie du DMIL
	[R3]	DIC	PREVENIR	Proscrire la sécurité par l'obscurité
	[R4]	DI	PREVENIR LIMITER	Processus de segmentation du logiciel et minimiser la complexité sur la partie sécuritaire du DMIL
	[R5]	DIC	PREVENIR	Documenter les exigences en matière de sécurité sur la documentation de conception du logiciel
	[R6]	I	PREVENIR LIMITER	Mettre en place une politique de gestion des achats et des composants Processus de validation : Contrôle d'acceptabilité (« Acceptance Check »)
	[R7]	I	BLOQUER REPARER	Conserver le paramétrage des versions successives Prévoir des moyens de remédiation
CONTEXTE D'UTILISATION DU DM	[R8]	CDIA	PREVENIR	Prévoir la destination d'usage
	[R9]	CDIA	PREVENIR	Prévoir l'environnement d'usage
CONTROLE DES ACCES	[R10]	CDIA	PREVENIR BLOQUER LIMITER	Appliquer le principe de moindre privilège Définir les rôles et privilèges des acteurs / utilisateurs
GESTION DES AUTHENTIFICATIONS	[R11]	CDIA	LIMITER	Réguler l'accès aux données et aux composants du système par une authentification préalable
	[R12]	CDIA	PREVOIR	Prévoir une authentification en accord avec le contexte d'utilisation
HEBERGEMENT	[R13]	CDI	PREVOIR	Fixer les conditions minimales d'hébergement
ENVIRONNEMENT D'UTILISATION	[R14]	DI	LIMITER	Minimiser le nombre d'hypothèses sur l'environnement
	[R15]	DI	PREVOIR	Ne pas freiner ou entraver l'application des exigences de sécurité de l'environnement d'exécution du logiciel DM
	[R16]	CDI	PREVOIR LIMITER BLOQUER	Définir les compatibilités entre logiciels et matériels
	[R17]	CDI	PREVOIR	Sécuriser l'interface avec l'environnement d'utilisation
	[R18]	I	PREVOIR	Utilisation de systèmes de sécurité capables de détecter et de répondre aux menaces liées aux codes malveillants
	[R19]	I	PREVOIR	Utilisation de systèmes de sécurité capables de bloquer les menaces
	[R20]	DI	PREVOIR LIMITER	Utilisation de mécanisme de cloisonnement
SECURITE PHYSIQUE	[R21]	DI	PREVOIR	Mise en place de mesures permettant d'assurer la sécurité physique du dispositif
DM CONNECTE A UN RESEAU	[R22]	DIC	PREVOIR	S'assurer de la maitrise des accès distants
	[R23]	DIC	PREVOIR	Avoir une matrice des flux réseau exhaustive dans la notice

	[R24]	DIC	PREVOIR	Prévoir des moyens de sécurité permettant de filtrer les données échangées sur les réseaux
	[R25]	DIC	PREVOIR	Sécuriser les accès Wi-Fi
	[R26]	DI	PREVOIR	Prévoir la possibilité d'isoler le système du réseau
	[R27]	ICP	PREVOIR	Préserver la sécurité via un VPN
	[R28]	DIC	PREVOIR	Prévoir la sécurisation des communications
TRAÇABILITE ET LOGS	[R29]	A	PREVOIR	Prévoir une fonction de journalisation locale
	[R30]	DI	PREVOIR	Documenter les modalités de mise en œuvre de la journalisation
PREVOIR LA SURVEILLANCE PENDANT LE FONCTIONNEMENT DU DM	[R31]	DI	PREVOIR	Vérifier l'état de l'art
	[R32]	DI	PREVOIR	Fonction d'auto-contrôle
	[R33]	DI	PREVOIR	Prévoir la mise à jour
	[R34]	DI	PREVOIR	Prévoir une fonction d'alerte locale
FONCTIONNEMENT EN MODE DEGRADE	[R35]	DI	PREVOIR	Développer un mode dégradé sécurisé
	[R36]	DI	PREVOIR	Documenter la procédure d'utilisation du DMIL en mode dégradé
CHOIX DES REGLES DE PROGRAMMATION	[R37]	DI	PREVOIR	Produire un logiciel sécurisé par construction
	[R38]	DI	PREVOIR	Justifier le choix du langage (mise en place d'un système qualité)
	[R39]	DI	PREVOIR	S'assurer de l'intégrité du code source
METHODES DE VERIFICATION	[R40]	DI	PREVOIR LIMITER BLOQUER	Spécifier les fonctions logicielles attendues
	[R41]	DI	PREVOIR	Appliquer des méthodes et outils de vérification appropriés
	[R42]	DI	PREVOIR	Soumettre son DM à un processus d'évaluation de la sécurité
DEMARRAGE SECURISE ET INTEGRITE DES MEMOIRES ET DES DONNEES SEMSIBLES	[R43]	DI	PREVOIR LIMITER BLOQUER	Prévoir une fonction de vérification au démarrage et lors du fonctionnement
	[R44]	DI	PREVOIR	Disposer une fonction d'affichage de la dernière version
	[R45]		PREVOIR	Disposer d'une interface permettant d'obtenir la configuration du système
MECANISME DE PROTECTION DU DM	[R46]	DI	PREVOIR	Répertorier les caractéristiques techniques complètes du DMIL
	[R47]	DI	PREVOIR LIMITER BLOQUER	Envisager l'utilisation de capteurs d'intégrité, d'attaque
DOCUMENTATION	[R48]	DI	PREVOIR	Répertorier les caractéristiques techniques complètes du DMIL
MISE EN PRODUCTION ET PROCESSUS DE VALIDATION	[R49]	DI	PREVOIR	Fournir une check-list de mise en production
	[R50]	DI	PREVOIR LIMITER BLOQUER	Proposer un système de contrôle de conformité des prestations externalisées
	[R51]	DI	PREVOIR LIMITER BLOQUER	Proposer un système de contrôle de conformité des données importées
GESTION DES PARAMETRES INITIAUX ET DES CONFIGURATIONS	[R52]	ICA	LIMITER BLOQUER	Définir en amont les configurations initiales
DISPOSITIF DE PROTECTION DE L'INTEGRITE DU DM	[R53]	CDIA	PREVOIR LIMITER BLOQUER	Prévoir un processus de vérification au démarrage et lors des mises à jour
INTEGRER l'APTITUDE A l'UTILISATION	[R54]	DI	PREVOIR LIMITER BLOQUER	Anticiper les négligences
	[R55]	DI	PREVOIR LIMITER BLOQUER	Prévoir l'utilisation du DMIL en situation d'urgence
	[R56]	CDIA	PREVOIR LIMITER BLOQUER	Mettre en place les prestations garantissant une utilisation conforme du DMIL
GESTION DES INCIDENTS ET ACTIONS CORRECTIVES	[R57]	DIA	PREVOIR	Mettre en place un système de notification des incidents
	[R58]	DIA	PREVOIR	Prévoir une cellule d'analyse des incidents
	[R59]	DIA	PREVOIR	Assurer un suivi permanent et prospectif des vulnérabilités liées aux technologies mises en œuvre dans les produits
	[R60]	DIA	PREVOIR	Mettre en place un système de veille
MODALITES DE MISE A JOUR / MAINTENANCE DU LOGICIEL	[R61]	DCIA	PREVOIR LIMITER BLOQUER	Mettre en place une fonction de mise à jour sécurisée des logiciels
	[R62]	DCIA	PREVOIR LIMITER BLOQUER	Prévoir l'envoi d 'un message d'alerte
CONDUITE A TENIR EN CAS D'ALERTE DE SECURITE	[R63]	DCIA	PREVOIR LIMITER BLOQUER	Prévoir un processus de réponse en cas d'attaque

FIN DE VIE DES COMPOSANTS TIERS DU DM	[R64]	DI	PREVOIR LIMITER BLOQUER	Anticiper la fin du support des logiciels tiers
FIN DE VIE DES DONNEES DU DM	[R65]	ICP	PREVOIR	Prévoir un mécanisme d'extraction des données vers un autre système
	[R66]	C	PREVOIR	Mettre en œuvre des fonctions de sécurité d'effacement des données
	[R67]	DIC	PREVOIR	Répondre aux exigences aux prestataires de services d'informatique en nuage
MATERIEL	[R68]	C	PREVOIR	Prévoir le processus de recyclage du matériel

143/147, boulevard Anatole France
F-93285 Saint-Denis Cedex
Tél. : +33 (0) 1 55 87 30 00
@ansm

ansm.sante.fr