1

Agence nationale de sécurité du médicament et des produits de santé

RAPPORT

ANSM'S GUIDELINE

Cybersecurity of medical devices integrating software during their life cycle

JULY 2019

This report was written by the Medical Devices, Cosmetics and In Vitro Diagnostic Devices Department.

This document is intended for DM manufacturers with software and DM software developers.

Sommaire

79 # RELEVANT ABBREVIATIONS AND DEFINITIONS

80

AIMD	Active implantable medical device
CLOUD	Remote server whose infrastructure is managed by a third party and therefore cannot be controlled
CONNECTED MEDICAL DEVICE	Device connected directly or remotely to a health information system. This is comprised of hardware (servers, peripheral equipment, specific electronic devices), software and data (files, databases). Its activity within healthcare delivery involves performing functions related to medical treatment, medical analysis, medical monitoring, diagnostics or supervision.
DMIL	Dispositifs médicaux intégrant du logiciel
EBIOS	Method of appraisal and treatment of digital risk published by the French National Cybersecurity Agency (ANSSI).
FAILSAFE MODE	Failsafe mode denotes a specific system status which is activated upon detection of an incident, an attack or identification of a malfunction. It must have a certain number of properties, in particular the fact that it can never be modified; this mode is basic, verifiable, controllable, and unchangeable.
GRPD	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, the so-called General Data Protection Regulation
HDS	Healthcare data hosting system.
HIS	Health information system
HOT UPDATE	Ability to update the code within an application without interrupting the service.
ICT	Information and communications technology
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
IVDMIL	*In vitro* diagnostic medical devices integrating software
MAINTENANCE	In these guidelines, the unqualified term "Maintenance" encompasses both corrective software maintenance ("maintenance which is carried out after failure detection and is aimed at restoring an asset to a condition in which it can perform its intended function", extracted from standard BS EN 13306 X 60-319) and progressive software maintenance ("action which involves, following requests by users, for example, modifying the behaviour of or providing new functions to software").
MAJOR RELEASE	Release which adds new functionality that have an impact on the rest of the application or modify the mode of operation or user organisation.
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
MINOR/INTERMEDIATE RELEASE	Release that fixes bugs and/or adds new features that do not have an impact on the rest of the software and do not modify the mode of operation or user organisation.
NIS	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the Union
NVM	Non Volatile Memory : computer memory that stores its data in the absence of power supply

PACS	(Picture Archiving and Communication system): system that uses archiving functions for the management of medical imaging. It enables the communication of medical imaging information via network (DICOM format) and its processing either remotely or via local area network using computers with high-definition monitors to view image-based examinations.
PATCH	Any set of changes to the source code or fix applied to the software configurations that are not customer-specific and have no embedded functional software development. The aim is to fix a flaw identified in the software. The notion of patch is related to the notion of vulnerabilities, in security terms.
PGSSI-S	General Security Policy for Health Information Systems.
RGS	General Security Framework drawn up by the French government
SAAS MODE	Software as a Service is a concept that involves offering subscription-based use of software rather than the purchase of a licence. The resources (data, application, servers, etc.) are outsourced rather than hosted by the client.
SNMP	Simple Network Management Protocol
SOUP	Software of Unknown (or uncertain) Pedigree (or provenance)

CONTEXT

In the healthcare sector more than any other area, the protection of assets and personal data cannot be compromised. Any abuse of vulnerabilities can indeed have harmful repercussions including a direct impact on safety of care and patient health.

In recent years, there has been a tremendous growth in healthcare-specific software and mobile applications. Such programmes take a variety of forms, covering software for data exchange, maintenance, remote monitoring, risk prediction or programmes for controlling medical devices.

Some of these applications or software programmes – intended by their manufacturers to be used for medical purposes – are classified as medical devices (MD) or *in vitro* diagnostic medical devices (IVDMD). They feature the CE marking under the new European regulations and fall within the oversight of the ANSM.

Although there is a clear regulatory framework for the introduction to the market of medical devices, the culture of cybersecurity is still very inconsistent among MD manufacturers. There are multiple reasons for this: lack of specific risk analysis, ignorance of cybersecurity requirements, failure to include cybersecurity in the MD design and development process. In addition, there are not yet any guidelines or recommendations dedicated specifically to IT cybersecurity.

Medical devices incorporating software are increasingly likely to feature network connectivity (Wi-Fi, radiofrequency, Bluetooth, etc.), and yet they are not equipped to deal with the new threats brought about by technological progress, particularly in the area of computer abuse.

This has led to an increased need for manufacturers of medical devices to incorporate basic requirements that can guarantee a minimum level of security to combat computer abuse, and this from an early stage in the product design.
.

The aim of this document is to provide recommendations specifically for manufacturers of medical devices in order that they take such measures as necessary to minimise the risk of attack against their MDs and thus to prevent data compromise or inappropriate use of the MDs that they introduce to the market.

This is made possible by the implementation of best practice guidelines and appropriate standards in terms of cybersecurity.

FOREWORD

For ease of reading, the generic term "**medical devices integrating software**" or "**MDIS**" has been chosen to specify both medical device software programmes and connected medical devices.

Similarly, the term "**cybersecurity**" will denote information security against cyber threats.

SCOPE OF APPLICATION

The products

The regulations on medical devices have been thoroughly reviewed and led to the publication on 5 May 2017 of two new regulations: one on medical devices (Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017) and the other on in vitro diagnostic medical devices (Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017). These two regulations came into force on May 26, 2017. They will enter into force on 26 May 2020 for the Regulation on medical devices and on 26 May 2022 for the Regulation on in vitro diagnostic medical devices, respectively, leading to the repeal of Directives 93/42/EEC (DM), 98/79/EC (DMDIV) and 90/385/EEC (DMIA). Certificates issued by notified bodies under the Directives before 26 May 2020 for DMs or 26 May 2022 for DMDIVs shall remain valid until the end of their period of validity and at the latest, for the latter, on 27 May 2024, dates on which they shall be invalidated.

Article 2(1) of the new regulation on MDs defines medical device as:
"any instrument, apparatus, appliance, **software**, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
– diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
– diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
– investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
– providing information by means of *in vitro* examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.
The following products shall also be deemed to be medical devices:
– devices for the control or support of conception;
– products specifically intended for the cleaning, disinfection or sterilisation of devices."

Similarly, the new Regulation applied to IVDMDs gives the following definition:
"any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used *in vitro* for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information:
– concerning a physiological or pathological process or state, or
– concerning congenital physical or mental impairments, or
– concerning the predisposition to a medical condition or disease
– to determine the safety and compatibility with potential recipients
– to predict treatment response or reactions
– to define or monitor therapeutic measures."

Software programmes (mobile or computer applications, embedded system and even artificial intelligence) are increasingly being proposed as medical solutions (diagnostics, monitoring, measurement, etc.). This can mean standalone software operating as a medical device in itself (e.g. a diagnostic mobile app) or in combination with a medical device (e.g. software utilising measurements from a sensor).

The MD Regulation also stipulates that software is deemed to be an active device: "any device, the operation of which depends on a source of energy other than that generated by the human body for that purpose, or by gravity, and which acts by changing the density of or converting that energy. Devices intended to transmit energy, substances or other elements between an active device and the patient, without any significant change, shall not be deemed to be active devices.

Examples of medical device software
Standalone software:
- radiotherapy treatment planning software (TPS)

- mobile apps for the assessment of potentially cancerous moles
- mobile app for the personalised calculation of insulin doses

MDs that use software for their operation and monitoring:

- pacemakers, infusion pumps
- monitoring or anaesthesia station

The regulation stipulates that “software for general purposes (for example, general administrative software used to manage the patient medical records), even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device.” In effect, it is not the environment in which the software is used that determines the MD status. The notion of general purpose software precludes tools such as Excel (except macro coding for medical purposes). For the time being, the notion of lifestyle/wellbeing permits the creation of apps for sport, quantified self, quality of sleep, for example, without any of the constraints inherent to CE marking.

Examples of non-medical devices

- software categorised as monitoring physical condition, coaching
- wellbeing products that are not MDs (connected bracelet)
- compliance software

Other examples of software and mobile apps used to illustrate the regulatory framework are available on the ANSM website: www.ansm.sante.fr.

The European Regulations have been modified in line with technological developments and medical devices incorporating software, or MDIS, are taken into account in the definition of products

The regulatory basis

In order to achieve compliance with the regulation, the medical devices incorporating software[1] must fulfil certain criteria.

In particular, **Annex I** of the new Regulations defines the **general requirements in terms of safety and performance**. Some of these specifically refer to MDIS.

Article 14.2 states that the devices shall be designed and manufactured in such a way as to remove or reduce as far as possible (...) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts. *For example, software linked to a PACS system.*

Article 14.5 states that devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the interoperability and compatibility are reliable and safe.

Point 17 of the essential requirements is dedicated specifically to MDIS. It states that their design must ensure repeatability, reliability and performance in line with their intended use. Measures must be taken to eliminate or reduce as far as possible all risk or impairment of performance of these devices. The following elements are detailed:

- **Article 17.1**: Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.

[1] https://www.ansm.sante.fr/Dossiers/Dispositifs-medicaux/Qu-est-ce-qu-un-dispositif-medical/(offset)/0;

- **Article 17.2**: For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
- **Article 17.3**. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
- **Article 17.4.** Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, as necessary to run the software as intended."
- The Regulation also demands detailed documentation on the software.

Article 6.1 of the Annex II concerns software verification and validation, describing the software design and development process and evidence of the validation of the software, as used in the finished device. This information shall typically include the summary results of all verification, validation and testing performed both in-house and in a simulated or actual user environment prior to final release. It shall also address all of the different hardware configurations and, where applicable, operating systems identified in the information supplied by the manufacturer.

The European Regulations clearly set out the requirements for software, and additional information that was not included in Directives 93/42/EC, 98/79/EC and 90/385/EEC relating to MDs, IVDMDs and AIMDs. Within this context, manufacturers will need to apply more restrictive CE marking procedures, with a more prevalent obligation to manage a quality management system and a post-market monitoring system.

Differentiating between safety and security

In order to broach the issue of safeguarding medical devices incorporating software, we first need to set out definitions of two fundamental concepts: safety and security.

Often confused, the two concepts differ according to the nature of the risks that they combat.

SAFETY

The operating safety of a medical device entails ensuring that it operates correctly and preventing random and unintentional risks. Safety also encompasses user error.
The operating safety of a computer system is defined as the property that enables its users to place reliance in the service delivered[2]. Obtaining a safe system of operation involves using a combination of methods that seek to counter *faults*, either internal or external, that could lead a system failure to occur. *For example, ensuring that an infusion pump dispenses at the programmed flow rate, with the precise dose intended by the manufacturer.*

SECURITY

Security entails ensuring that the MD is protected against outside attacks that could compromise the operation of the MD[3]. *Example, hacking an infusion pump and gaining remote control of the programming function could lead to unwanted product dispensing or modification of flow rates.*

The key difference between safety and security therefore lies in the nature of the faults envisaged. Operating safety mainly involves *accidental faults*. Security includes *intentional faults*, i.e. those created with malicious intent. This is a fundamental difference. A system can effectively be operationally safe because the probability of an adverse event occurring is deemed negligible; this same system will not

[2] "Sûreté de fonctionnement des systèmes informatiques", J.-C. Laprie, B. Courtois, M.-C. Gaudel, D. Powell, 1996
[3] http://docplayer.net/32998797-Study-on-safety-of-medical-devices-software.html

necessarily be *secure*, because an attacker will specifically seek to trigger the adverse event. A secure system must deliver the expected services (i.e. fulfil its specifications), and this service *only*.

The notions of security and safety are obviously not mutually exclusive. The methodologies recommended in the area of operating safety also satisfy various requirements in terms of security. It is indeed vital to take into consideration the intentional nature of faults during the risk analysis phase of the secure system design process. It is still worth stressing that whatever safety and security measures are introduced, the medical safety of a device is an absolute prerequisite. This must remain the case throughout the entire life cycle of the medical device.

Inclusion of the security recommendations comes in addition to the recommendations on device safety and quality.

Operating safety is not covered within the scope of this document. It only deals with the notion of security.

Assessment of threats

The growth of connected objects for medical use, alongside the deployment of telemedicine, are the main new vulnerabilities. They expose the population to new threats. Their impact is not solely individual but can also affect an entire population.

Security measures for a MD may therefore aim to protect the MD not just as the *destination* of an attack but also as the *relay or entry point* of an intrusion into the information system of the host healthcare facility.

- Attacks that target the MD itself are intended to modify/alter its operation or its availability.
  - **Attacks on the availability of the device**: denial of service, such as overloading the MD with requests which then overwhelm and block the network, unauthorised access, loss of patient data, excessive power consumption which depletes the battery,
  - **Attacks on the integrity of the device**: modified data, altered device operation (loss of control, slowed response, disruption to patient care, etc.), encryption of data rendering it inaccessible, physical destruction

- The aim of attacks that target the MD as an entry point is to alter the operation of the infrastructure.
  - disrupted operation of the medical device from the HIS or its network, and vice versa.
  - disrupted operation of the device due to electromagnetic disturbance (refer to electromagnetic compatibility standards - European Directive 2014/30/EU)
  - capture or modification of the data exchanged between the medical device and the HIS.

Examples of attacks

In recent years, a number of French healthcare facilities have been targeted by large-scale cyberattacks. In 2015, the IT system of the Valence radiotherapy department was hacked, allowing access to the patient data held on the medical devices. Radiotherapy treatments were suspended for 24 hours[4].
In 2016, a number of faults on connected medical devices were identified. An insulin pump with a Wi-Fi function was withdrawn from the market by Johnson & Johnson due to a security vulnerability that made it possible to hack into the device[5].
That same year, security vulnerabilities were identified in connected implantable MDs manufactured by St Jude Medical. The security vulnerabilities, if exploited, allowed an authorised person to access the device and to modify the pacemaker programming commands by rapidly depleting the battery of the

[4] "Cyberattaques : les établissements de santé tentent de se protéger", Marion Guérin, 23/10/2015
[5] https://www.jnj.com/innovation/johnson-and-johnson-leading-fight-to-prevent-cyberattacks

implanted device or by administering inappropriate shocks that could cause patient death. A software update was ordered by the FDA[6].

Medical devices have undergone tremendous technological progress over recent years, with the development of data exchange, monitoring, risk prediction and control software. These developments have been rapidly incorporated in day-to-day medical practice without the associated risks being fully controlled. Even though manufacturers are able to guarantee product safety in terms of biological safety and clinical efficiency, there is still a lack of any specific culture relating to cybersecurity.

The European Regulations now introduce security and performance requirements specific to MDIS. The Regulations do not explicitly refer to or elaborate on the notion of cybersecurity, but application of these new rules, alongside the continuing development of technology and connectivity, do pave the way for the introduction of a new approach to risk management and system security on the part of manufacturers. These provisions can be taken into consideration at an early stage and set as a requirement in the product specifications.

[6] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

CYBERSECURITY APPLIED TO MDIS

Information system security (ISS)

Cybersecurity is understood to mean "*The full set of technical or organisational measures set up to ensure the integrity and availability of a MD and the confidentiality of the information held on or output by this MD against the risk of targeted attacks*"[Fig.1].

Figure 1. Priority criteria for cybersecurity

DEFINITION OF CRITERIA

Availability is the ability of a system to deliver a service (for example, access to information or resources) under predefined conditions of operation and maintenance, within the constraints of performance and response times. Attacks on system availability are generally categorised as denial of service attacks. Resilience is the ability of a system to continue to operate (by operating in failsafe mode, where relevant) under adverse conditions, and to return to normal operation after an incident.

Confidentiality is the property of information to be known only to those individuals, entities or processes duly authorised to have knowledge of it: restricted read-only access.

Integrity is the property of a system or of information to prevent unauthorised modification, alteration or deletion. Where data integrity cannot be guaranteed (for example, during transfer via an untrusted data channel), it must be possible to detect the integrity defect.

According to the French General Security Framework (RGS), the criteria of availability, integrity and confidentiality are the baseline objectives to be fulfilled in terms of security.

There is one additional criterion termed **auditability**[7]. This is the ability of a system to keep records of the operations performed on the protected assets (for example, access or attempted access to information) and to ensure the operability of these records for monitoring or investigation purposes, i.e. recording actions by date in a log file.

CLARIFICATION REGARDING DATA PROTECTION AND CONFIDENTIALITY

Data confidentiality within the sense of "protection of privacy" must be a central focus for manufacturers of medical devices. A number of guidelines cover the protection of data confidentiality.

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

Manufacturers will be able to refer in particular to the French **General Security Framework** (RGS) which includes an appendix setting out the requirements relating to the security activity "confidentiality"[8].

By way of example, the guidelines state that "all connected devices must have an onboard data encryption mechanism in order to guarantee the confidentiality of personal medical data when being stored or transferred". The General Data Protection Regulation (GDPR), which entered into effect on 24 May 2016 and came in application on 25 May 2018, provides a clear definition of personal data and lays down provisions to protect it. As confidentiality and data protection are already tightly regulated by the GDPR, the issue will not be covered further within this document.

Confidentiality and data protection in the context of privacy protection are already largely regulated by the GDPR, so this issue will not be discussed further in this document. On the other hand, the notion of confidentiality in the sense of protecting read data against unauthorized disclosure and protecting access to technical elements will be developed in this document.

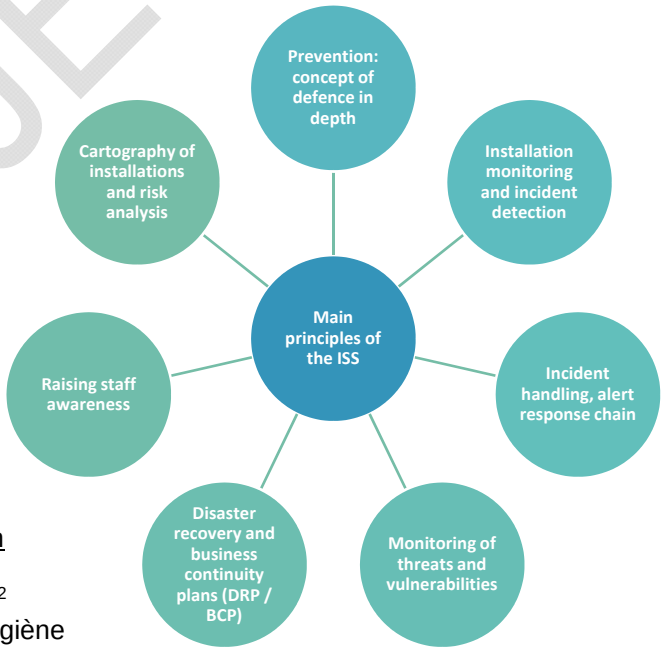
The ANSM recommendations will focus mainly on the availability and integrity of MDIS, where a malicious attack could have harmful repercussions on patient health.

Management of risks in terms of information technology (IT)

Information system security (ISS) is based on a number of key principles. It entails preventing the unauthorised use, misuse, modification, silent copying or hijacking of the information system [↳Fig. 2].

In France, the **National Cybersecurity Agency** (ANSSI)[9] is responsible for protecting national information systems and for verifying the application of relevant measures.
The ANSSI provides a set of good practice guidelines and recommendations[10] intended for information security professionals and the general public in order to raise awareness of the different methodologies for digital security.

Examples of guidelines available:
-Recommendations for choosing controlled firewalls in Internet-exposed areas[11]
-Recommendations for setting up system partitioning[12]
-Cartography of the information system-Guide hygiène informatique.[13]



↳*Figure 2.* Main principles of ISS

RISKS ANALYSIS METHODS

[8] 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
[9] https://www.ssi.gouv.fr/en/
[10] Link: https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[11] https://www.ssi.gouv.fr/guide/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-a-internet/ (in French)
[12] https://www.ssi.gouv.fr/uploads/2017/12/guide_cloisonnement_systeme_anssi_pg_040_v1.pdf (in French)
[13] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

There are several methods of ISS risk analysis (MEHARI, EBIOS), based on identifying the **critical assets to be protected**. These assets are the elements which could, if attacked, have consequences for assets or persons.

The ANSSI has developed a methodology for analysing and managing risk known as **EBIOS**[14] [Fig. 3]. It is used to evaluate risks, to assist with risk handling by specifying security requirements to be implemented, to prepare the security records required for risk acceptance and to provide all information as relevant for communication regarding risk.

This method is also applicable to medical devices.

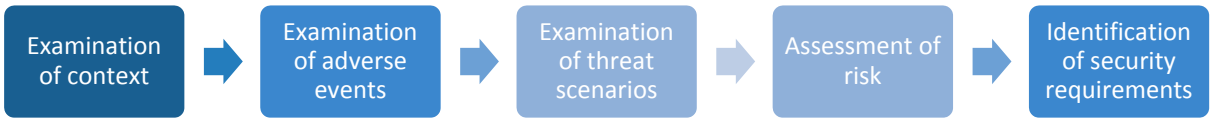


Figure 3. Different stages of the EBIOS method

The various documents and tools provided by ANSSI are also applicable to MDIS. They were used as a source of reference for drafting this document

Risk management in terms of medical devices

Application of risk management to medical devices is defined in **ISO standard 14971 (BS EN ISO 14971:2013)** published in January 2013 and developed specifically for manufacturers of medical devices.

It covers risk management processes focussed mainly on the patient, but also the operator and other persons and equipment, as well as the environment of use. Risk analysis is performed at the different stages in the life cycle of the medical device [Fig. 4].

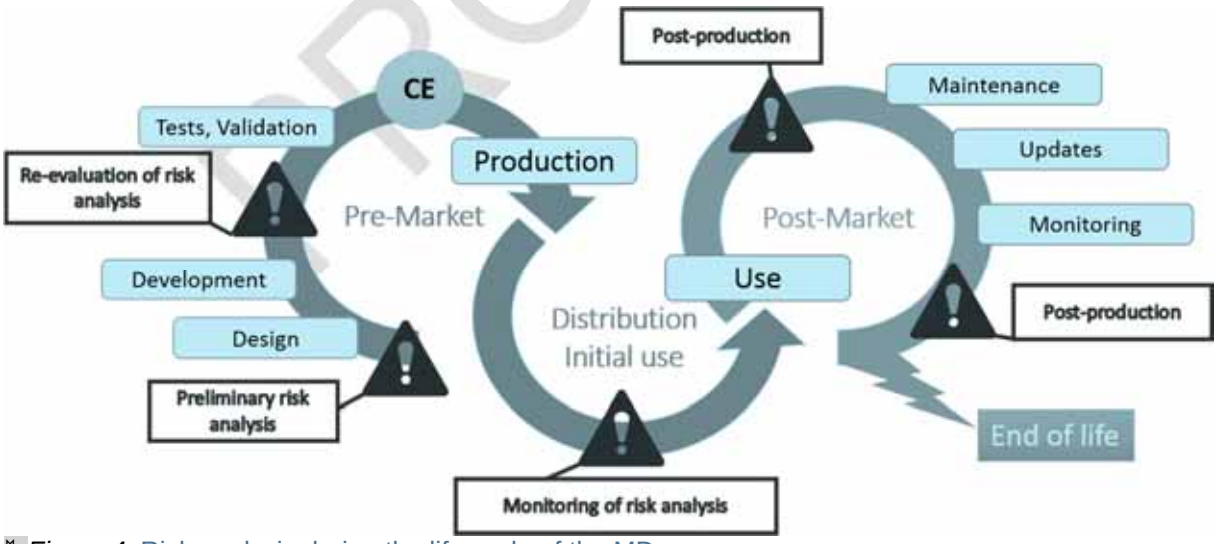


Figure 4. Risk analysis during the life cycle of the MD

According to **ISO standard 14971**, the manufacturers must, for a given medical device, within a context of use as defined by the manufacturer itself, assess the vulnerabilities that are present and determine the potential impact that could result. This covers vulnerabilities in both hardware and software, loopholes in procedures and also issues related to human aspects.

[14] https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite (in French)

Once an event is identified, they determine the **acceptable level of risk** by defining the risk tolerance threshold.
Acceptance of risk is analysed in respect of the risk-benefit ratio. A risk is acceptable if:

- it is controlled as far as is possible,
- reduction of the risk does not alter the overall risk-benefit ratio
- it presents a favourable risk-benefit ratio, and
- post-market surveillance measures are provided for.

For example:

☒ Death – irreversible harm ⇒ *unacceptable,*
☒ Reversible harm ⇒ *possible acceptability if the medical benefits outweigh the overall residual risk,*
☒ Damage to brand image, financial loss ⇒ *acceptable if below a set threshold*

Next, they plan the measures to be introduced in order to minimise the resulting potential impact. The introduction of measures serves to ensure the continuity of functionality at an acceptable level.
The definition of risk reduction measures is documented in a risk management plan and a software security report.

- The Risk Prevention plan is formulated as follows:
  - Assess the vulnerabilities of the MD Software throughout the life cycle:
  - Assess the threats relating to Confidentiality/Availability/Integrity in line with the vulnerabilities and critical functions assessed.
  - State the requirements for counter-measures and security for all threats assessed.
  - Align with the Software Development Plan and the Risk Management Plan.
  - Serve to formulate the Software Security Report verifying the inclusion of security requirements.

- The Software Security Report must:
  - Assess the activities relating to the security of the software.
  - Assess whether the security requirements set out in the Threat Prevention Plan have been taken into account.
  - Determine and provide an opinion on the security of the software

Align the two approaches of MDs and IT

PRINCIPLE

In order for the risk analysis and management methodology used for information systems to be applied specifically to MDIS, we need to establish a common language. Effectively, there is a difference in culture between the world of MDs and the world of information system security that needs to be taken into account when formulating a security system.

- In the world of ISS, the risk is a combination of a threat and the consequential losses that could result. The threat is a feasible scenario and the losses are estimated in terms of damage to basic needs/assets.
- In the world of MDs, the manufacturer must prove that the potential risks associated with the use of the medical device are acceptable in terms of the benefit to individual patients.

In order to integrate the risks associated with cybersecurity, the idea is to recommend that manufacturers perform a risk analysis that combines both approaches: risk analysis in ISS and ISO 14971 [↳Fig. 5].

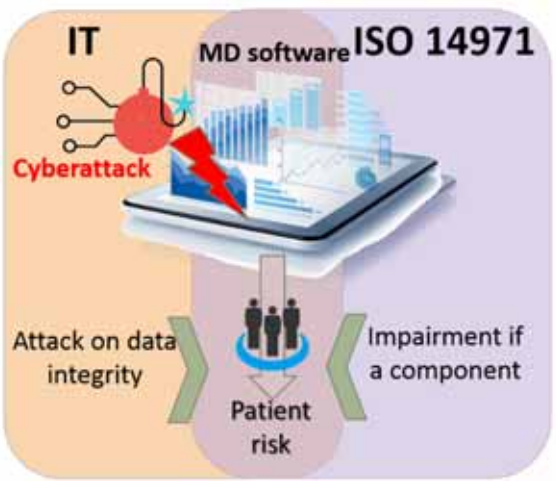


Figure 5. Combination of SSI and ISO 14971 approaches for MDIS

More precisely,

- To fully comply with the specifications for CE marking, **the manufacturer must guarantee that its medical device meets the general requirements** for security and performance throughout its life cycle, from the design phase right through to disposal.
- In order to think in terms of cybersecurity, the manufacturer must identify the critical assets to be protected and ensure their integrity, availability, confidentiality and auditability.

Formulating a risk analysis that combines both approaches will involve creating the "standard" risk analysis and then introducing "cyber" security criteria throughout the life cycle of the medical device. The aim is to set out measures as adequate to cover the identified threats.

In its approach, the manufacturer will need to take account of differences in risk according to the types of MDs in question and to adapt the design of the MD accordingly. It will also have to take into account the specificities related to the topology and the environment in which DMIL is used.

For example:

- Medical devices that are implanted or worn by the patient (e.g. pacemakers, insulin pumps, etc.)

⇒ *Risk to patient health*

- Medical devices connected to the hospital network of a more "diagnostic" nature

⇒ *Main risk: vector of attack on the network*

- Medical devices connected to the hospital network for healthcare purposes

⇒ *Risks for the patient and the network*

As systems become increasingly interlinked/interconnected, it is too limiting to perform a risk analysis on a per-system basis. This assessment framework seems inadequate for complex architectures, such as a hospital IT network.
When the MD is integrated within a HIS, it can provide a vector for propagating a potential attack. The recommendation must then be to perform a risk analysis on the entire system, the difficulty there being that manufacturers will not generally be familiar with the overall IS in which the MDIS will be used. A helpful suggestion would be for the manufacturer to assess the risk of propagating threats within the system in the event of an attack and to strengthen it against system failures.

There are a number of computer-based tools that use modelling systems to facilitate this process, such as those developed in the aeronautics sector. However, considering current practices, this type of approach is more of a long-term objective.

METHODOLOGY

Compliance with security requirements is part of the general framework of **a standard quality management system (BS ISO 13485: 2016**), with the following elements in addition:

1. **Identify the assets and property/goods to be protected**
   in other words, draw up a list of critical assets to be protected and set out the security objectives for these assets.
   - In the case of an MD as the target of an attack, these are the assets which, if attacked, can have a negative impact on patient care.
   - In the case of an MD as a point of entry, these are the assets which will cause impairment to the operation of the infrastructure.
   -

The assets to be protected are, as a minimum:

- Firmware
- Medical configuration: *for example*, in terms of the control process for the injection sensor, this is the rule which measures the quantity to be injected / calculates the flow rate, etc.
- Cryptographic keys
- Event logs
- Patient data

2. **Define a security objective for each of the assets** in terms of integrity, confidentiality, availability and traceability and **the security functions to be implemented in order to reach this security objective**.

Once the critical assets have been identified, the manufacturer must define the potential vulnerabilities, dangers and associated risks (impact analysis on priority criteria). This step provides an overall picture of the full set of protection measures to be put in place.

The approach will proceed as follows:

There are a number of existing approaches to guarantee integrity, availability, confidentiality and auditability:

- **prevent**: avoid the existence or emergence of vulnerabilities;
- **block**: stop an attack from reaching sensitive or vulnerable elements;
- **limit**: minimise the consequences of an attack;
- **detect**: identify an intrusion in order to provide an attack response (traceability);
- **repair**: have the means to return the system to normal operation following an attack (notion of resilience).

For example

Assets to be protected	*Security objectives*	*Protection systems*
Medical configuration	*Integrity and confidentiality*	- ***Limit*** Data signature - ***Block*** Memory encryption - ***Limit*** Management of permissions (initialisation / first use / modification)
Firmware (operating software, system software)	*Ensuring integrity within the context of an update, for example*	- ***Block*** Secure boot sequence for the MD linked to a verification process for the firmware's cryptographic signature
Cryptographic keys	*Integrity, confidentiality and traceability*	- ***Prevent*** Protect the secrecy of keys, do not move them
Event log	*Integrity, confidentiality and traceability*	- ***Limit*** Regular backups, troubleshooting, troubleshooting
Patient data	*Integrity and confidentiality*	- ***Block Encryption*** - ***Limit*** Collect only essential data

The aim of these recommendations is to guide manufacturers in their approach to cybersecurity of medical device software, from initial development through to introduction to the market, usage and post-market monitoring.

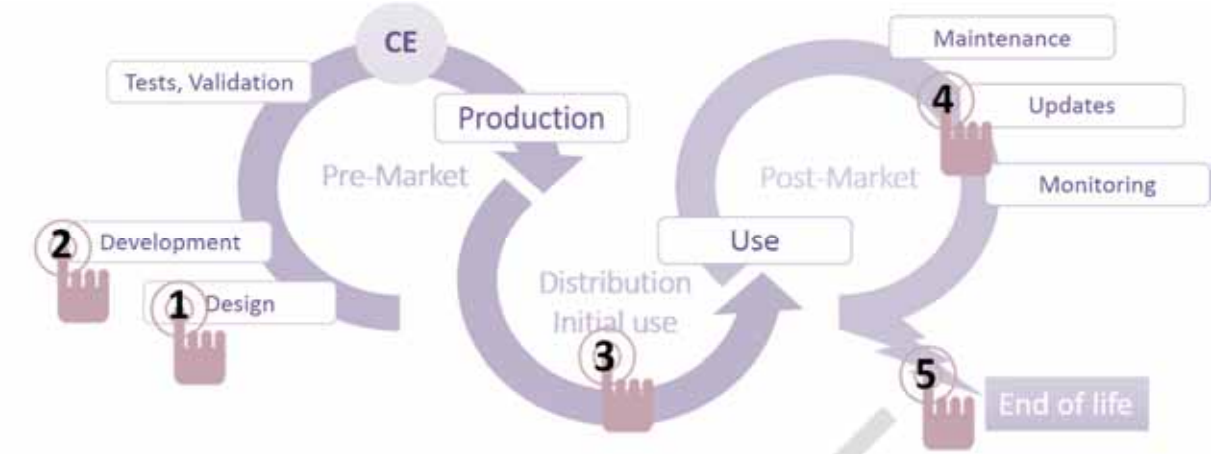
They seek to set out the key principles without expanding on the technical details, which would otherwise quickly render this document obsolete given the rate at which both medical devices and attacks can develop.

Based on the elements set out earlier, the document focuses on the analysis and risk methodologies developed in the world of MDs and the world of ISS. The key issue is to reach a minimum acceptable level of risk.

These provisions are part of an approach to implementing a quality management system (QMS). The specific points relating to cybersecurity should be specified.

RECOMMENTATIONS ARISING FROM THE RISK ANALYSIS

The recommendations are divided into five key areas based on the software life cycle:



Given the diverse range of products and usages, this is a standard list of general recommendations for all MDIS: MDs, IVDs and AIMDs. However, certain recommendations may not be applicable. The recommendations are summarised in appendix A3.

1 Software design activity

GENERAL PROVISIONS

[R1] Risk analysis
This is fundamental. The risk analysis will be the basis used to determine and justify all subsequent measures set up to ensure the protection of the MD and its environment. It is the first and foremost of all the recommendations. All the other recommendations will stem from the risk analysis (see section II).

[R2] It is recommended to ban security by obscurity
The security of a system should not rely on the secrecy of its design or implementation. It must be assumed that an attacker can always gain access to the internal operation of a medical device, particularly to its source code (*e.g. using reverse engineering techniques*), its algorithm secret or protocol.

[R3] It is recommended to minimise the data used by retaining only those software components that are strictly necessary for the correct operation of the medical device. Deleting unnecessary components is one way to reduce the surface of vulnerability exposed by the medical device.
It is also recommended that the manufacturer makes the security aspect of the MDIS less complex. For this, the software can be segmented into critical zone and non-critical zone. Only those zones identified as critical will need to meet the minimisation requirements.

[R4] It is advisable to establish a policy for managing purchasing, software components and subcontracting (Acceptance Check). *For example, for SOUP-type software, the usage must be justified and a security assessment must be performed and taken into consideration.*

[R5] It is suggested to provide for remedial action (return to secure operation) from as early as the product design phase. *For example*, update firmware and secrecy (cryptographic keys).

[R6] It is proposed to apply the principle of least privilege to all active components of the medical device. Endeavour to restrict privileged processes to an absolute minimum.

For example:
- Access to a device via an authentication badge defining the associated rights and privileges.
- Limit access to the administrator account

DEFINE THE CONTEXT OF USE OF THE MD

[R7] The intended usage is a key element to consider at the statement of requirements stage. It is recommended to find a balance between the user authentication process and the context of use.
For example, MD software used in an emergency context need not require the same authentication process as software used in a non-emergency context.

[R8] It is suggested to take into consideration the environment of use from as early as the design phase in order to identify appropriate control systems.
For example, the requirements for accessibility will not be the same for software used at home and software used within a healthcare facility.

ACCES CONTROL

[R9] It is recommended to clearly define the roles and privileges of stakeholders/users: users must not all have the same access permissions. Access will depend on their user roles.

i. The privileges granted to users can be restricted to the minimum level required to fulfil the functions of their specific role
ii. User access permissions can be organised according to roles/profiles (administration, maintenance, etc.)
iii. Access to the data export functions on the connected medical device may be restricted to duly authorised persons.
iv. Access to the software update functions or modification of sensitive parameters may require strong authentication. Any validation tasks within these contexts may require two-step confirmation
v. A connected medical device could include a user authentication function based on named accounts. User workstations may need to be protected for confidentiality and integrity.
   Depending on the features and usage of the MDIS, a hardware (badges, chips) or multi-factor authentication policy could be introduced:
   a. Physical media (badge, smart card)
   b. Fingerprint (biometric information)
   c. Login/Password

Stringent precautions may be taken when using a password system. The password may be strong (minimum number of characters, special characters, regular password change, etc.) and secure (monitor the number of failed attempts, limited renewal period, inability to reuse old passwords, etc.).

AUTHENTIFICATION MANAGEMENT

[R10] It is recommended to regulate access to data and system components through prior authentication: authentication of users on the system, authentication of software, authentication of a message sent to or received by the MD, etc.
For example: authenticate before accessing a DMIL at the hospital

[R11] An authentication process can be established in accordance with the context of use of the MD.
For example: reduce the authentication of DMILs used in an emergency context

The recommendations set out below may be followed when setting up authentication mechanisms.

i. Access to the connected medical device system may require prior authentication depending on the MD usage

ii. The date of last login to the connected medical device system could be shown during the user login process

HOSTING

[R12] Hosting should be addressed as a measure of risk control. There is a minimum requirement level to be reached for data security.
The manufacturer can therefore set minimum conditions for hosting the MDIS (service proposal or subcontracting). Its recommendations for hosting the MD software in accordance with the risk analysis should be stated to users and made clear in its documentation. For example:

- Either the MD software communicates with **local** or shared servers

e.g. a healthcare facility can host the application locally and provide other healthcare facilities with access to it

- The MD software uses external servers, passing through data hosting providers that offer this specific service (e.g. OVH, Amazon etc.).

The hosting sector is tightly regulated. Manufacturers may need to refer to the regulation on certification of Health Data Hosting Providers (HDS)[15].
The DGOS (French Directorate-General for Care Provision) has published a handbook on cybersecurity for use by directors of healthcare facilities[16]. The NIS[17] Directive published in the Official Journal on 19 July 2016 seeks to "improve the ability to resist cyber-attacks" for organisations providing "essential services" or operators of essential services such as healthcare settings.

For example: if a manufacturer wishes to store data in the cloud, it should be vigilant about how the data is stored and refer to relevant regulations or to documents that set out the cloud safety.
If a manufacturer sells a set of services related to an MD, it may comply with the regulations relevant to those services; for provision of a health data hosting service, the manufacturer should comply with the HDS Regulation.

ENVIRONNEMENT OF USE

[R13] The intended environment of the MDIS is understood to mean the software elements in which it operates and with which it interacts (operating systems, healthcare facility network, etc.).
It is recommended that the MD be as autonomous as possible in terms of its security. To achieve this, the number of hypotheses within the environment should be kept to a minimum (general safety and performance requirement 17.4. of Annex I of the DM and DMDIV Regulations).

The manufacturer should state the hypotheses within the environment for secure operation of its device. These security hypotheses should be satisfied by the operating environment of the MD. They can not be excessive, however. The manufacturer cannot base the safety of his DMIL exclusively on the safety of the environment. It should research the intended environment of its MD and recommend a minimum requirement in terms of compatibility.
For example: during updates, it should have a process in place to verify the authenticity and integrity of the firmware

[R14] The correct operation of the MDIS cannot hinder or impede the application of security requirements within the MD software's operating environment (e.g. prevent the hospital from updating its IT equipment to Windows 10 on the pretext that a MD software only operates under an obsolete version of Windows XP).

15 L.1111-8 of the French Public Health Code
Link: esante.gouv.fr > Labels et Certifications heading > Hébergement des données de santé (in French)
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.0_niveau_essentiel.pdf
https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante
16 Link: https://solidarites-sante.gouv.fr/IMG/pdf/dgos_memento_ssi_131117.pdf (page 18)
17 Directive (EU) 2016/1148 of the European Parliament and Council of 6 July 2016

[R15] In accordance with the requirements relating to the quality management system[18], the manufacturer is also encouraged to determine the compatibilities between software and hardware. To reiterate, such incompatibilities should at least be managed and controlled and at best be kept to an absolute minimum. An incompatibility is effectively a potential hindrance to security.
For example,
If correct operation under a new version is not guaranteed, this is not acceptable.

[R16] The environment should be made physically and logically secure depending on the medical devices (computer-type workstations, command consoles, medical device at patient home / outpatient setting, mobile MD) through the use of protective measures such as:

- Encryption of sensitive data (identified by prior risk analysis)
- Providing for the possibility of network partitioning to counter any digital attack from the outside
- Having regulated and secure access (badge, login/password, etc.)
- Recommending a stable environment: the medical device must be relatively autonomous in terms of security (secure network access)
- Using anti-virus (this will be dependent on the MDIS in question); effectively, the use of anti-virus is not systematically recommended in all contexts).

[R17] Depending on the nature of the MDIS and the relevant level of security to be achieved, the user workstations for connected devices must provide security that can detect and respond to potential attacks using malicious code. In this sense, software used specifically for managing connected devices installed on user workstations must be compatible with security solutions that counter malicious code.

[R18] Depending on the nature of the MDIS, a set up operating system hardening in order to block or hinder any attempts to execute arbitrary code or illegitimate programmes on the MDIS can be implemented or proposed (dedicated memory segments, mutually exclusive permissions for modification and execution, protective mechanisms for the process execution stack, layout randomisation for memory storage, etc.).

[R19] Depending on the MD type and the degree to which it is integrated within a more complex system, it is recommended to propose partitioning mechanisms. For example, in the event of a successful attack on the MDIS, a software integrity check should be performed and measures must have been foreseen to prevent the attack propagating to the entire system.
-partitioning between the graphical interface and critical data, partitioning between the DMIL software and the rest of the network

PHYSICAL SECURITY

[R20] It is suggested to set up measures to ensure the physical security of the device (physical access). The physical elements in which the device operates and with which it interacts (e.g. access to a service port on a medical device) should be protected and be usable by authorised persons only, etc. This will depend on the type of medical device.
Example: lock protecting access to the connected medical device, premises, systems

MD CONNECTED TO A NETWORK

[R21] The documentation for the connected medical device should contain an exhaustive matrix of the network data streams (protocol types, origin/destination of data streams, addressing scheme, etc.).

[R22] The connected devices may include security measures for filtering the data exchanged on the networks (protocol types, origin/destination of data streams, etc.). Accordingly, the software installed on workstations used specifically to manage the connected devices should be compatible with the security solutions for network filtering such as personal firewall.

18 ISO Standard 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes

[R23] When implementing wireless communications, for example, the connected medical device should be compliant with current good practice requirements. For details regarding Wi-Fi mode, refer to the relevant reference documents available on the ANSSI website: Good practice: securing Wi-Fi access[19].

[R24] From as early as the design phase, and depending on the medical purpose, it is recommended to provide for the option of isolating the MD software from the network or from all communication channels in the event of an attack or threat. This provision should not affect the availability of the MD.

[R25] It is suggested the option of using a virtual private network (VPN) to safeguard the logical security that exists within a local network. This is not applicable to all types of MDIS.
For example, in the case of a DMIL used in a patient's home, use of a VPN between the DMIL at home and the hospital to protect the data exchanged.

Reference could be made to the details of standard BS EN 50159 on Safety-related communication in transmission systems, which recommends the following defences:

i. Sequence number (anti-replay)
ii. Time-stamping (anti-replay)
iii. Time-out
iv. Source and destination identifiers (= authentication)
v. Return message (integrity)
vi. Identification procedure
vii. Security code
viii. Cryptographic techniques[20].

[R26] All communications may be secure. To achieve this, mechanisms should be defined to ensure:

i. Baseline criteria: integrity, confidentiality (e.g. use of encryption key)
ii. Non-rejection of communications (depends on the MD and the context of use)
iii. Authenticity of communications
iv. Data exchanges between the connected medical device and the environment. The latter must be compliant with the security requirements set by the Shared Health Information Systems Agency (ASIP) in its guidelines on interoperability of Health Information Systems (HIS).

TRACEABILITY AND LOGS

[R27] The connected medical device could include a local logging function that can trace all access to the connected medical device and all events, particularly those that could have a critical impact on its operation.

[R28] It is proposed that the manufacturer indicate in his documentation the procedures for implementing logging, particularly the medical device's log storage capacity and the recommendations for backing up and using the logs.
These elements should be protected in terms of integrity.

PROVIDE FOR MONITORING DURING THE MD OPERATION

[R29] The connected medical device should include a self-monitoring function (integrity check) and a local alert function used to monitor correct operation and to flag any event that could have a critical impact on its operation.

For example: Verification at startup that the code has not been modified, verification of the signature at startup

[19] https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/
[20] https://www.ssi.gouv.fr/guide/cryptographie-les-regles-du-rgs/ (in French only)

[R30] The operating systems used within certain MDs should be kept up to date, so that they cannot propagate viruses that exploit weaknesses in obsolete versions of these operating systems (as in the case of Mirai21, ransomware, worms, etc.)

[R31] In the case of integration within another IS, it is suggested that the MD include an alert function based on standard mechanisms that allow the HIS to monitor the correct operation of the MD, connections to the device, and any event that could have a critical impact on its operation (software update, modification of critical parameter, etc.).
In the case of MDs connected to a network in a healthcare setting, there is a need to evaluate the risk that the MD represents in terms of the HIS and conversely in terms of introducing a threat/vulnerability. The ASIP has developed a practical guide for connected devices in an HIS setting that lists the relevant security requirements[22].

[R32] Data recovery solutions used to restore data, for example when swapping out equipment, may be proposed.

OPERATION IN FAILSAFE MODE

[R33] Certain connected medical devices can have a (secure) failsafe mode to provide a data recovery function when resuming normal operation. Failsafe mode could be triggered when an attack is detected or when the effect of an attack is detected
For certain types of MD, continuity of service could be a requirement, particularly for devices that are worn or implanted (Pace maker for example). Mechanisms that guarantee the availability of critical functions can be put in place even when security is compromised or when a threat to integrity is identified.

[R34] The product documentation issued or made available to customers may include procedures for using the product in failsafe mode, particularly:
- the functional scope in failsafe mode
- any performance restrictions
- the procedure for implementing failsafe mode
- the procedure for resuming normal mode.

There is scope to adapt these procedures to fit with the customer context.

It is suggested to plan:
- How to enter failsafe mode, i.e. what triggers this mode following a security alert or incorrect operation.
- How to exit failsafe mode (via strong authentication of an authorised person, to be defined by the manufacturer)

21 Biggs, John, “Hackers release source code for a powerful DDoS app called Mirai”
22 http://esante.gouv.fr/sites/default/files/Guide_Pratique_Dispositif_Connecte.pdf (in French only)

2 MD software development activity

CHOICE OF PROGRAMMING LANGUAGE

[R35] If the choice of programming language is at the manufacturer's initiative, it should be justified and the coding rules should be specified in the developer's quality system and correspond to good practices in terms of quality and safety through the use of a validation system and regression testing.

For example, a language that has a strong data typing mechanism helps to avoid some errors.

The MD software development will need to comply with encoding rules that are checked automatically by way of continuous in-service inspection. This allows for automation of vulnerability detection. The aim is to produce software that is “secure by construction”. Open source, proprietary or customised tools can be used. These tools should be able to check the properties described in recognised standards such as MISRA C/C++, CWE, SANS Top 25, CERT, OWASP, and so on.

VALIDATION METHODS

[R36] It is recommended that the designer of the DM software specify the expected software functions. It could develop procedures and types of tests associated with each function (Requirement Based Testing, Code Analysis).

When running the tests, it is proposed to measure the structural coverage of the code, and justification must be provided for all lines of code not covered by the tests. Dead code (code that is not specified and not testable) should be deleted.

SECURE STARTUP AND INTEGRITY MEMORIES AND SENSITIVE DATA

[R37] The connected medical devices should have a function that can check the integrity and authenticity of the device's software and sensitive data both at startup and during its operation. The medical device should have a function to display the latest version of the software being used and the sensitive data. This also applies during the update process.

[R38] It is recommended that the connected medical device system provide an interface used to supply the configuration of the connected medical device system and its operating status. The devices broadcast information on the network about their own configuration in line with the SNMP standard (simple network management protocol). This is a communication protocol used by network administrators to manage the devices on the network, and to monitor and diagnose hardware and network problems remotely. This is, however, advisable to use a recent secure version of the SNMP protocol (the use of older versions is likely to introduce serious vulnerabilities).

MD PROTECTION MECHANISM

[R39] MD self-monitoring includes setting up a self-test mechanism that is run at startup and during medical device operation. The principle would be to provide for integrity checks at the appropriate time and as often as possible, which will depend on the type of DMIL concerned.

Example:
- Firmware integrity checks (Secure boot) performed at startup
- Memory integrity check during each access to permanent storage (NVM, mass storage)
- Self-monitoring of the integrity of the software produced at each start or activation, for example
- Self-monitoring of hardware integrity performed at startup
- Auto monitoring of the DM battery

[R40] The use of attack sensors (light, temperature change, etc.) will detect anomalies in the event of an attack. If an anomaly is detected, the MD automatically switches from standard operating mode to a safe failsafe mode.
For example: secure integrated circuits equipped with driver sensors with degraded mode in case of alert

DOCUMENTATION

[R41] The documentation may cover the technical properties of all hardware and software components (versions, operating system) that make up the medical device. This information should be accessible either via an online user area or in paper format.

According to the MDIS, it must specify in particular:
- the properties of the administration workstation for the connected medical device: hardware properties, operating system versions, middleware and drivers, peripheral devices, etc.
- the properties of the workstations intended for user operations: hardware features, operating system versions, middleware and drivers, peripheral devices, etc.
- the specifications of the software, source code, executables and testing procedures and results.

Note: These recommendations are applicable to each phase of the MDIS life cycle.

SOFTWARE VERIFICATION / VALIDATION

[R42] It is recommended to apply appropriate verification methods and tools to ensure that there are no vulnerabilities in the software (secure memory management: library or primitive OS or HW, etc.). and to minimize the risk of anomalies appearing and ensure that the software complies with the specifications. (attack simulation, analysis tools)

[R43] The manufacturer is encouraged to submit his DM to a safety assessment process (e. g. CSPN or and ANSSI: Common criteria as proposed by ANSSI[23]). This evaluation must be carried out before the medical device is placed on the market and then updated each time the medical device is overhauled.

PRODUCTION LAUCH AND VALIDATION PROCESS

[R44] It is suggested to the manufacturer to provide a production launch checklist. It supplied system integrators with guidelines on security recommendations and requirements relating to integration of the DM within a health information system. This document is to be updated with each major release of the MD.
It is proposed that the supplier and/or manufacturer undertakes to install only those software programmes that are necessary for the operation of the connected medical device. The supplier and/or manufacturer undertakes to enable only those services that are necessary for the operation of the connected medical device.

[R45] An acceptance check system should have been put in place ahead of the integration of outsourced services (subcontractors, purchasing management, incorporation of SOUPs). To achieve this, the specifications should have been defined in advance and the integration of a new element will only be validated after verifying that it fully satisfies the specifications. It is suggested not to integrate external elements without carrying out the proper checks beforehand.
For example, HSS libraries: identifying vulnerabilities in certain versions of HSS libraries, using tried and tested libraries for the integration of a SOUP.

[R46] As it is not feasible to ban data imports outright, certain actions may be implemented in order to manage the process. This also involves an acceptance check type approach. Data imports could:

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

- be an integral part of the manufacturer's risk analysis. *For example*, carrying out a risk assessment related to the use of physical media that could destroy the system (USB Killer)
- be controlled: the manufacturer must provide for a filtering system for data imported onto the MD (safety of data imported onto the MD). *For example*, if using a USB key on a workstation connected to an MRI device, the data will need to be encrypted or a malicious code detection system will need to be put in place.

Initialisation – First use

MANAGEMENT OF INITIAL PARAMETERS AND CONFIGURATIONS

[R47] It is proposed that the initial setup and configuration stages be planned and be consistent with the overall risk analysis performed at an earlier stage.

- The default passwords should be changed during the installation or at first login and should be user specific.
- Widespread use of cryptographic keys should be provided for as appropriate to the environment of use. From as early as the design phase, simply apply the basic principle “one key, one use”.
- It is possible to set up antivirus solutions provided that these do not hinder the correct operation of the MD (provision is not applicable to AIMDs, for example).
- Updates must be planned as often as possible, particularly during the installation/initialisation phase. An initial update must be planned for MDs that might have been in storage for a long period between delivery and use.

MD INTEGRITY PROTECTION DEVICE

[R48] It is recommended to the manufacturer to provide the user with a list of precautions to take during the startup phase, depending on the type of installation and the type of MD in question. These precautions will be dependent on the number of connected systems, their usage, the network tree structure.
For example, the precautions will be different for a single medical device connected to the IS network, as opposed to a medical device connected by server to a sub-network of the IS used to control the hardware remotely, which itself is connected by the Internet to the remote maintenance system.

[R49] The MD should feature a mechanism to run integrity checks at startup and during updates as a minimum (e. g. Verification of update signatures).

INCLUDE SUITABILITY OF USE / CONSIDER THE END USER

[R50] It is suggested to the manufacturer to put measures in place to counter threats and to include these in its development plan for suitability of use. The security measures may be adapted to suit users who are not security-aware.

[R51] Negligence and misuse are not the result of malicious acts, and yet the resulting impact can be similar to that of an attack. They can create vulnerabilities open to exploitation by hackers or simply affect the system availability.
Examples

- Unintentionally modifying the settings for alarms and warning messages can have disastrous consequences on the quality of products, delivered services, the environment, the health or safety of individuals.
- Using a USB key to transfer data between isolated systems can lead to system unavailability if this key is carrying a virus.

In both these cases, borne of real experience, the individuals involved did not intend to cause harm. And yet there was a clearly tangible impact on the system architecture.
Such examples of negligence can be due to a lack of staff training and a lack of information on the relevant issues. It is therefore recommended to involve users in the security process. The software should be designed in terms of accessibility and ergonomics. There should then be an appropriate training plan.

[R52] The manufacturer is advisable to consider the use of the MD in emergency situations, even in the event of a threat.

[R53] The service provisions necessary for the correct implementation of the device should be specified: user requirements in terms of training, installation, production launch, system operation support, assistance with drafting documents and setup support.

Several user types can be recognised:

- The maintenance technician, who is not the end user, or a healthcare professional, or the manufacturer.
- The end users of the MD who will be using the equipment on a daily basis
- The user(s) with greater permissions who will be responsible for first-level support where the manufacturer is not present on site and will monitor any qualified changes (hardware or software). In practice, it is usually the onsite biomedical engineer who takes on this role. It is up to the manufacturer to provide for suitable, user-specific training.

4 Monitoring – post-market management

With technology advancing at a pace, it is not possible to identify from the outset all the vulnerabilities that a medical device may present during its life cycle. Post-market monitoring to identify new weaknesses is a vital proactive approach towards being able to react and to reduce patient risk.

MANAGING INCIDENTS AND CORRECTIVE ACTIONS

To recap, there are several ways of reporting IT security incidents in France.

Portal	Incidents	Individual	Link
ANSM	Reporting incidents involving medical devices and *in vitro* diagnostic medical devices	Patient Healthcare professional Patient Healthcare professional Manufacturer / distributor	materiovigilance@ansm.sante.fr
French Ministry of Health and Solidarity	Reporting of adverse health events relating to healthcare products, everyday products and care procedures	Patient consumers or users	signalement-sante.gouv.fr
ASIP Santé (Shared Health Information Systems Agency)	Security incidents relating to IT or new technologies	Users	https://www.cyberveille-sante.gouv.fr/
ANSSI	Reporting a security flaw or vulnerability	Users	https://www.ssi.gouv.fr/en/

In addition, the Cybersecurity Act explicitly requires manufacturers to set up a vulnerability monitoring system. In addition, as part of the certification of medical devices, each manufacturer must propose a vulnerability registration system.

[R54] The new MD and IVDMD regulations set out the prerogatives for the reporting of serious incidents and field safety corrective actions. The following is detailed:
"Manufacturers of devices made available on the Union market [...] shall report to the relevant competent authorities [...] the following respectively in Articles 87 and 82 of the DM and DMDIV Regulations:

a) Any serious incident involving devices made available on the Union market, except expected side-effects which are clearly documented in the product information and quantified in the technical documentation and are subject to trend reporting pursuant to Article 88;
b) Any field safety corrective action in respect of devices made available on the Union market, including any field safety corrective action undertaken in a third country in relation to a device which is also legally made available on the Union market, if the reason for the field safety corrective action is not limited to the device made available in the third country. "

Manufacturers must therefore notify the ANSM of any incident or risk of incident concerning a medical device or *in vitro* diagnostic medical device. All details required to investigate the case also need to be provided: responses to additional questions within the given timeframe, and final report within 60 days. The report must contain an analysis that provides proof that the measures taken are appropriate or to justify the absence of such measures (causal analysis, frequency, etc.).

The reporting forms and procedures (MEDDEV) are available on the ANSM website[24]. This entails a continual process of gathering, recording, identifying, processing, assessing and investigating incidents or adverse effects relating to the use of healthcare products. The aim is to provide oversight of the safe use of these products and to prevent all risks relating to their use through implementation of corrective and/or preventive actions.

[R55] Analyse all incidents involving the medical device that are reported by users.

24 https://www.ansm.sante.fr/Declarer-un-effet-indesirable/Votre-declaration-concerne-un-dispositif-medical/Votre-declaration-concerne-un-dispositif-medical/(offset)/0 (in French only)

[R56] Provide permanent and prospective monitoring of vulnerabilities related to the technologies embedded in the products. All incidents must be catalogued. This monitoring is needed in order to set up corrective actions.

[R57] When the manufacturer is aware of a risk of incident (identification of a vulnerability and/or threat), there is always a risk that this vulnerability can be exploited. Using a monitoring system to anticipate this risk seems essential.

Manufacturers should be aware of all identified vulnerabilities and implement corrective measures without delay.

For example, a process for managing anomalies in SOUPs must be effective in order to rectify the vulnerabilities published by the SOUP editors (standard 62304).

METHODS FOR SOFTWARE UPDATES / MAINTENANCE

[R58] It is recommended to set up a secure update function for the software that will ensure its authenticity and integrity. The individuals involved in the update procedures should be clearly identified. Their roles are defined. Strong authentication during the update process is strongly recommended.

WHAT TO DO IN THE EVENT OF A SECUTITY ALERT

In the event of an attack, the user will be the first to act. However, the manufacturer is advisable to provide a documented action plan so that the user knows how to respond to an alert message.

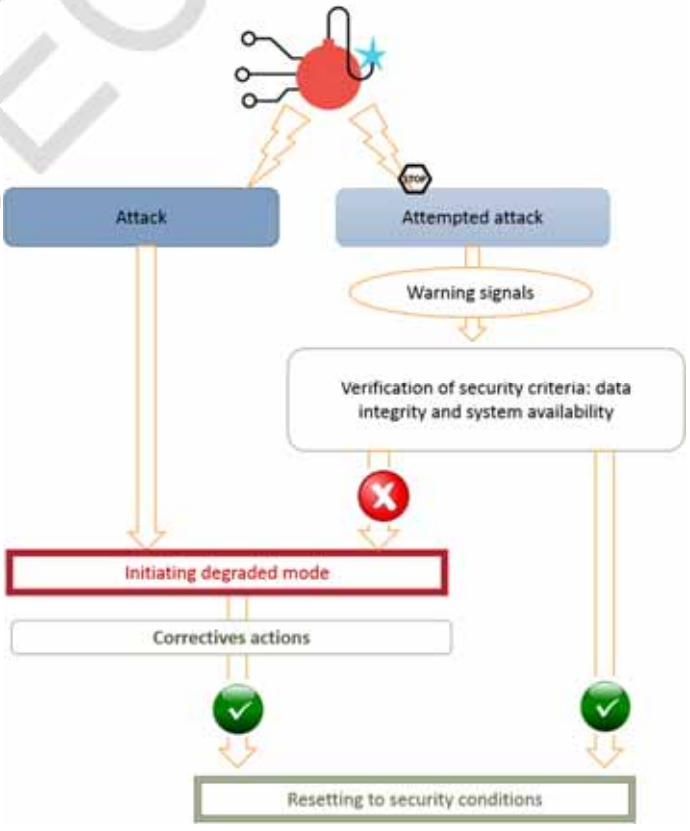
[R59] Following an attack or attempted attack, the MD must fulfil the safety criteria. Four aspects should be taken into consideration:

1. Ensure the safe operation of the MD for the patient (or for the healthcare facility's IS)
2. Ensure the availability of the MD; this involves setting up a failsafe mode or isolating the system.
3. Check the integrity and confidentiality of the MD data (verifying pre/post-attack consistency ensures that data integrity is maintained).
4. Inform the user

Triggering a warning signal will in turn trigger the failsafe mode. This is a minimal mode of operation that guarantees patient security. Failsafe mode continues to operate until corrective actions can be implemented, after which the device can return to secure operation.

The manufacturer should set out a business continuity plan (BCP) to ensure that information remains available regardless of what issues are encountered. It should also provide for a disaster recovery plan following an incident.

For example: insulin pumps in case of an attack, activation of an autonomous operating mode (pre-programmed flow rate) with an alert.



5 End of life for the MD software

Different situations can bring about the end of life of a software programme:

- The software is no longer intended for use (statement of requirements)
- Migration of data to another media or another MD is necessary; migration to a more efficient or more recent system
- The software and/or hardware becomes obsolete in terms of upgrade options, capacity, settings, automated modifications, etc.

If the software of the MDIS is obsolete, i.e. it cannot be replaced or updated, the entire MD is deemed to be obsolete.

END OF LIFE OF THIRD-PARTY COMPONENTS OF THE MD (OPERATING SYSTEMS, DATABASES, COTS, ETC.)

[R60] The end of "life" of the software and physical components of the MD should be considered as early as the design phase. This involves end-of-medium management for the third-party software (COTS) used in the MD. The manufacturer is advisable to guarantee its media in the long term.

MD manufacturers should anticipate an end-of-medium approach for the third-party software used within their products.

For example, if the operating system providing for use of the medical device software is Windows XP, there should have been a plan in place, from as early as the design phase, for when Windows XP becomes obsolete. Given that the average lifetime of an operating system is six to eight years (creation, maintenance, end of maintenance), the issue of updating the operating system will need to be addressed if the MDs have an expected lifetime of ten years.

MANAGING THE END OF LIFE OF THE MD DATA

[R61] Before erasing any data, and depending on the type of MD and its usage, it may be necessary to transfer the data off of the MD and recover it for storage or for reuse. The procedure for extracting the data to another system should be secure. In accordance with the GDPR[25], the right to data portability is a baseline principle.
Data transfer (virtual or onto hardware) is a potential point of vulnerability. It should therefore be carried out in secure conditions. This calls for the implementation of a procedure for data portability and for good practice in terms of cryptography.

[R62] When using a DM, sensitive data can be stored on different hardware media (e.g. hard disks, magnetic tapes, USB keys, CD, DVD, etc.) or on a remote server.

It is suggested to the supplier to implement functions for secure data erasure in accordance with current good practice requirements (For example: Full encryption of storage media).

The deletion of data from a medium poses difficulties in its implementation. Full encryption of storage media enhances the security of this type of procedure. In the short term, it is sufficient to "forget" the key used to encrypt the data on the storage medium, which represents only a few bytes. To protect against longer-term cryptographic advances, the usual overload erasure procedures will still be applied," seems clearer to me.

25 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

[R63] Compliance with Article L1111-8 of the Public Health Code, relating to data hosts, is a mandatory basis. In addition, if necessary, the manufacturer could rely on the SecNumCloud [26].

HARDWARE

[R64] Once the data held on the MD has been managed, in other words once it has been erased or transferred, the next step is the secure recycling of the hardware.

The French National Cybersecurity Agency (ANSSI) has also published recommendations for the erasure of magnetic (hard disks or magnetic tapes) and non-magnetic storage media (such as USB keys or SD cards) that previously contained sensitive information (references nº 1 and 2):

- Recommendation: “Erasure of mass storage media”
- Guide: “TECHNICAL GUIDE for the confidentiality of data stored on hard disk drives for recycling or export”

26 L.1111-8 of the French Public Health Code; esante.gouv.fr > Services heading > Hébergement des données de santé (in French)

BIBLIOGRAPHY

- 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, ASIP SANTE. Guide pratique regles pour les dispositifs medicaux connectes d'un systeme d'information de sante. Novembre 2013.
- PGSSIS, ASIP 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, ASIP. Guide pratique specifique a la destruction de donnees lors du transfert de materiels informatiques des Systemes d'Information de Sante (SIS)
- Sante, ASIP Politique Generale de Securite des Systemes d'Information de Sante (PGSSIS) Decembre 2014 V1.0. 2014.
- Sante, ASIP. Regles pour les interventions a distance sur les systemes d'information de sante. Decembre 2014 V1.0.

ANNEXE 1

List of 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/
- ASIP SANTE : AGENCE FRANÇAISE DE LA SANTE NUMERIQUE
  - 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

ANNEXE 2

Standards and regulatory texts

	France	Europe / International
Non-MD	PGSSIS: Rules for the remote maintenance of health information systems PGSSIS - Guide to management of mobile terminals French National Authority for Health (HAS) Guidelines on Connected Objects (GT28) Cybersecurity France label? French decree no. 2016-1214 (duty to report serious incidents regarding IS security) ANSSI: Cybersecurity requirements for industrial system integration and maintenance service providers (March 2016) ANSSI: Controlling IS security for industrial systems (June 2012) ANSSI: Référentiel Général sur la Sécurité (General Security Framework) ASIP Santé: Référentiel Qualité Hôpital Numérique (Digital Hospital Quality Guidelines)	ITU (International Telecommunication Union) Global Cybersecurity Agenda (GCA) Framework for Improving Critical Infrastructure Cybersecurity – NIST (National Institute of Standards and Technology) ISO 27032: Information Technology - Security Techniques - Guidelines for cybersecurity ISO/IEC 27000: Information Technology - Security Techniques - Information security management systems - Overview and vocabulary ISO/IEC 27005: Information Technology - Security Techniques - Information security risk management ISO 27001: Information security management (system, not product) ISO 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ENISA **BS EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems** ISO/IEC 15802: Information technology - Telecommunications and information exchange between systems. Local and metropolitan area networks. Common specifications - Part 3: Media access control (MAC) bridges **Access control: Protocol IEEE 802.1X - Port-Based Network Access Control**
MD	**PGSSIS - Guide to connected devices within a Health Information System** *(but in a hospital context, excluding outpatients, and cybersecurity forms part of the scope, but not uniquely)* **IS security requirements for biomedical equipment in healthcare establishments (collective of IS security managers and biomedical engineers in healthcare establishments)** *(addressed to healthcare establishments, recommendations for cooperation between IS security managers and Biomedical Engineers)* **Study on the security of MD software:** analysis of the regulatory completeness of standard BS EN 62304 and ANSM Recommendations for reinforcing the *security* aspects of this standard *(aspects not currently included in the 62304 standard)*	**MD Regulation EU 2017/745** ISO/TR 11633: Health informatics - Information security management for remote maintenance of medical devices and medical information systems **BS EN ISO 14971: Application of risk management to medical devices** **ISO 62366 – Application of usability engineering to medical devices** BS EN 60601-1 (requirements for incorporation of an MD into an IT network) Art 14:13 IMDRF SaMD **FDA: Guidance for the content of Premarket submissions for management of Cybersecurity in medical devices Oct 2nd, 2014.** **FDA: Postmarket Management of Cybersecurity in Medical Devices** **FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (2005)** IEEE Canada: Building Code for Medical Devices of the 21st Century – CyberLex / Recos de Société Savante **BS EN 62304: Medical device software - Software life-cycle processes** **BS EN 80001: Application of risk management for IT networks incorporating medical devices** **Building code for MD software security – IEEE (Institute of Electrical and Electronic Engineers)**

ANNEXE 3

Summary table - Recommendations

Risk analysis dentify **Critical assets to be protected** As a minimum: firmware, medical configuration, cryptographic keys, event log, patient data	**INDEX** **[R1]**	Define **vulnerabilities and associated risks** **Confidentiality = C** **Availability = D** **Integrity = I** **Auditability = A**	**RECOMMENDATIONS** > Propose **protection systems**	**Examples References** ⇓ (UE) 2017/745 (UE) 2017/746 ISO NF 14971:2013

⇓ ⇓ ⇓

Recommendations	Nb	Security objectives	Measures		Examples References
GENERAL PROVISIONS	[R2]	DIC	PREVENT	Ban security by obscurity Security must not rely on the key or the source code being secret	E.g. Transparency in terms of process and design of cryptographic primitives
	[R3]	DI	PREVENT LIMIT	Process of segmenting the software and making the security aspect of the MDIS less complex:	
	[R4]	I	PREVENT LIMIT	Establish a policy for managing purchasing and software components Validation process: Acceptance check	Justify the use of a SOUP and perform validation texts prior to incorporation
	[R5]	I	BLOCK REPARER	Retain the setup of successive versions Plan remedial action	Firmware update
	[R6]	CDIA	PREVENT BLOCK	Apply the principle of least privilege	Access to a device via an authentication badge defining the associated rights and privileges.
CONTEXT OF USE OF THE MD	[R7]	CDIA	PREVENT	Plan the intended usage	MDIS used in an emergency situation
	[R8]	CDIA	PREVENT	Plan the environment of use	e.g. MDIS used at the patient's home
ACCESS CONTROL	[R9]	CDIA	PREVENT BLOCK LIMIT	Define the roles and permissions of stakeholders / users	Set up user profiles Ref. CNIL, PGSSI -Identify who is able to access the system
MANAGING AUTHENTICATIONS	[R10]	CDIA	LIMIT	Restrict access using authentication	Authentication of a sent or received message
	[R11]	CDIA	PREVENT	Provide for authentication according to the context of use	Pre-authentication
HOSTING	[R12]	CDI	PREVENT	Set out minimum requirements for hosting	See HDS regulations, NIS Directive
ENVIRONMENT OF USE	[R13]	DI	LIMIT	Minimise the number of hypotheses within the environment	Process for checking the authenticity and integrity of the firmware during updates
	[R14]	DI	PREVENT	Do not hinder or impede the application of security requirements within the MD software's operating environment	

	[R15]	CDI	PREVENT LIMIT BLOCK	Define compatibilities between software and hardware	Unsecured operation on a new version is not acceptable
	[R16]	CDI	PREVENT	Safeguard the interface with the environment of use	Physical access, data encryption, network partitioning, anti-virus
	[R17]	I	PREVENT	Use of security systems that are able to detect threats	
	[R18]	I	PREVENT	Use of security systems that are able to block threats	Dedicated memory segments
	[R19]	DI	PREVENT LIMIT	Use of partitioning mechanism – Block chains	Establish a cartography of data streams; filter the data streams using a firewall
PHYSICAL SECURITY	[R20]	DI	PREVENT	Introduce measures to guarantee the physical security of the device	Protection of access to a maintenance port for medical equipment
MD CONNECTED TO A NETWORK	[R21]	DIC	PREVENT	Have an exhaustive matrix of network data streams	
	[R22]	DIC	PREVENT	Provide for security measures to filter the data exchanged on the networks	
	[R23]	DIC	PREVENT	Secure the Wi-Fi access	
	[R24]	DI	PREVENT	Provide for the possibility of isolating the network system	
	[R25]	ICP	PREVENT	Maintain security via a VPN	In the case of a DMIL used in a patient's home, use of a VPN between the DMIL at home and the data exchanged with the hospital
	[R26]	DIC	PREVENT	Provide for secure communications	
TRACEABILITY AND LOGS	[R27]	A	PREVENT	Provide for a local event log function	
	[R28]	DI	PREVENT	Document the implementation methods for the log function	
PROVIDE FOR MONITORING DURING THE MD OPERATION	[R29]	DI	PREVENT	Provide for a self-monitoring function	Verification of the signature at startup
	[R30]	DI	PREVENT	Plan to update the operating system	
	[R31]	DI	PREVENT	Provide for a local alert function	
	[R32]	DI	PREVENT	Provide for data recovery solutions	
OPERATION IN FAILSAFE MODE	[R33]	DI	PREVENT	Develop a secure failsafe mode	
	[R34]	DI	PREVENT	Document the procedure for using the MDIS in failsafe mode	
CHOICE OF PROGRAMMING LANGUAGE	[R35]	DI	PREVENT	Justify the choice of language (set up a quality system)	
	[R36]	DI	PREVENT	Provide for validation testing procedures	Code analysis
SECURE STARTUP AND INTEGRITY OF MEMORIES AND SENSITIVE DATA	[R37]	DI	PREVENT LIMIT BLOCK	Provide for a system check process at startup and during operation	
	[R38]	DI	PREVENT	Provide for an interface specifying the system configuration	
MD PROTECTION MECHANISM	[R39]	DI	PREVENT LIMIT BLOCK	Provide for a self-test process at startup and during operation	Firmware integrity checks (Secure boot) performed at startup
	[R40]	DI	PREVENT	Use of attack detection sensors	
DOCUMENTATION	[R41]	DI	PREVENT	Identify the full technical properties of the MDIS	
SOFTWARE VERIFICATION/ VALIDATION	[R42]	DIA	PREVENT	Set up a verification system	Attack simulation
	[R43]	DI	PREVENT LIMIT BLOCK	Provide for an interface specifying the system configuration	
PRODUCTION LAUNCH AND VALIDATION PROCESS	[R44]	DI	PREVENT	Provide for a self-test process at startup and during operation	Firmware integrity checks (Secure boot) performed at startup

	[R45]	DI	PREVENT LIMIT BLOCK	Use of attack detection sensors	
	[R46]	DI	PREVENT LIMIT BLOCK	Identify the full technical properties of the MDIS	
MANAGE INITIAL PARAMETERS AND CONFIGURATIONS	[R47]	ICA	LIMIT BLOCK	Set up a verification system	Attack simulation
MD INTEGRITY PROTECTION DEVICE	[R48]	CDIA	PREVENT LIMIT BLOCK	Provide for an interface specifying the system configuration	
	[R49]	DIC	PREVENT LIMIT	Provide for a self-test process at startup and during operation	Firmware integrity checks (Secure boot) performed at startup
INCLUDE SUITABILITY OF USE	[R50]	CDIA	PREVENT LIMIT BLOCK	Use of attack detection sensors	
	[R51]	DI	PREVENT LIMIT BLOCK	Anticipate user negligence	
	[R52]	DI	PREVENT LIMIT BLOCK	Provide the use of the MDIS in emergency situations	
	[R53]	CDIA	PREVENT	Set up service provisions that guarantee compliant usage of the MDIS	
MANAGING INCIDENTS AND CORRECTIVE ACTIONS	[R54]	DIA	PREVENT	Set up an incident reporting system	
	[R55]	DIA	PREVENT	Provide for an incident analysis unit	
	[R56]	DIA	PREVENT	Ensure permanent and prospective monitoring of vulnerabilities related to the technologies embedded in the products	
	[R57]	DIA	PREVENT	Set up a monitoring system	
METHODS FOR SOFTWARE UPDATES / MAINTENANCE	[R58]	DCIA	PREVENT LIMIT BLOCK	Set up a secure update function for the software	
WHAT TO DO IN THE EVENT OF A SECURITY ALERT	[R59]	DCIA	PREVENT LIMIT BLOCK	Provide for a response procedure in the event of an attack	
END OF LIFE OF THIRD-PARTY COMPONENTS OF THE MD	[R60]	DI	PREVENT LIMIT BLOCK	Anticipate the end-of-medium approach for the third-party software	
END OF LIFE OF MD DATA	[R61]	ICP	PREVENT	Provide for a procedure for extracting the data to another system	
	[R62]	C	PREVENT	Implement security functions for erasing the data	Full encryption of storage media
	[R63]	DIC	PREVENT	Meet the requirements applicable to cloud service providers	
HARDWARE	[R64]	C	PREVENT	Provide for a hardware recycling process	

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

ansm.sante.fr