ADVANCING CYBERSECURITY OF HEALTH AND DIGITAL TECHNOLOGIES

MARCH 2019

COCIR SUSTAINABLE COMPETENCE IN ADVANCING **HEALTHCARE**

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

COCIR

As the digitisation of health and care progresses, the number of connected digital health technologies is increasing. This is inevitably accompanied by a growing number of cybersecurity risks. European regulators have responded by introducing cybersecurity requirements for devices, systems and infrastructure in various regulatory frameworks, addressing both the healthcare sector specifically or the industry horizontally.

This document outlines the different requirements, introduced by various legislative frameworks, that now our industry faces. It contains our recommendations for ensuring that medical devices and services in Europe remain secure.

1. EXECUTIVE SUMMARY

The products and services that COCIR members place on the European market have to ensure that not only vendors, but particularly operators (healthcare providers, including hospitals) can comply with all applicable European, national and regional regulations. Medical devices are strictly regulated in Europe; in addition, several EU legislative frameworks have introduced new requirements for the security of connected health technologies.

Security is a shared responsibility. It must be clear to all parties involved that it takes organisational measures to ensure security, which can then be supported by product technology.

A product or service needs to have the necessary security features to allow it to provide the security controls as required - and as far as applicable - under the Medical Devices Regulation (MDR), the Directive on Security of Network and Information Systems (NIS Directive), the General Data Protection Regulation (GDPR) and the forthcoming Cybersecurity Act. In addition, they need to comply with the security requirements from specific laws and regulations that many of the EU Member States have in place at national level.

COCIR remains actively involved in on-going discussions with various regulators. However, we need to broaden the discussions to ensure better harmonisation and alignment to the European and national laws that set security requirements for products and services.

TO SUPPORT SECURE HEALTHCARE IN EUROPE, COCIR HAS DEVELOPED THE FOLLOWING RECOMMENDATIONS FOR CONSIDERATION BY EUROPEAN, NATIONAL AND REGIONAL REGULATORS:

1. **SET UP** a broad European discussion to establish good security practices in all regulatory frameworks, in order to reduce market access limitations, conflicting requirements and unnecessary administrative burden.
2. **PROMOTE** regulatory convergence between EU Member States and industry sectors.
3. **DEVELOP** European guidance that clarifies the concept of shared responsibility, including criteria for determining the device's intended environment.
4. **ADOPT** the new MDS2 form[1] (currently under revision and expected to be adopted in Summer 2019) as a means of documenting and communicating medical device security and privacy features in Europe.
5. **COORDINATE** a European approach to security-related incident reporting, in order to avoid duplication and confusion.
6. **SAFEGUARD** a level playing field by ensuring that consistent and effective market surveillance measures are in place to warrant compliance with the existing regulatory framework.
7. **AVOID** multiple certification schemes for the same technologies and processes.

1 Manufacturer Disclosure Statement for Medical Device Security (MDS2), https://www.himss.org/resourcelibrary/MDS2

2. INTRODUCTION

As an industry, COCIR and its members are very much aware of the technology shift currently underway and the consequentially increasing cybersecurity risk for connected health technologies, both at home and in the cloud. Therefore, COCIR members have long implemented ***'SECURITY BY DESIGN'*** principles in the products and services they offer in the European and global marketplace.

We feel strengthened, but also concerned, by new regulatory developments in cybersecurity in Europe. Strengthened, because these deliver a clear expectation for vendors and operators. Concerned, because there is no harmonised approach towards security.

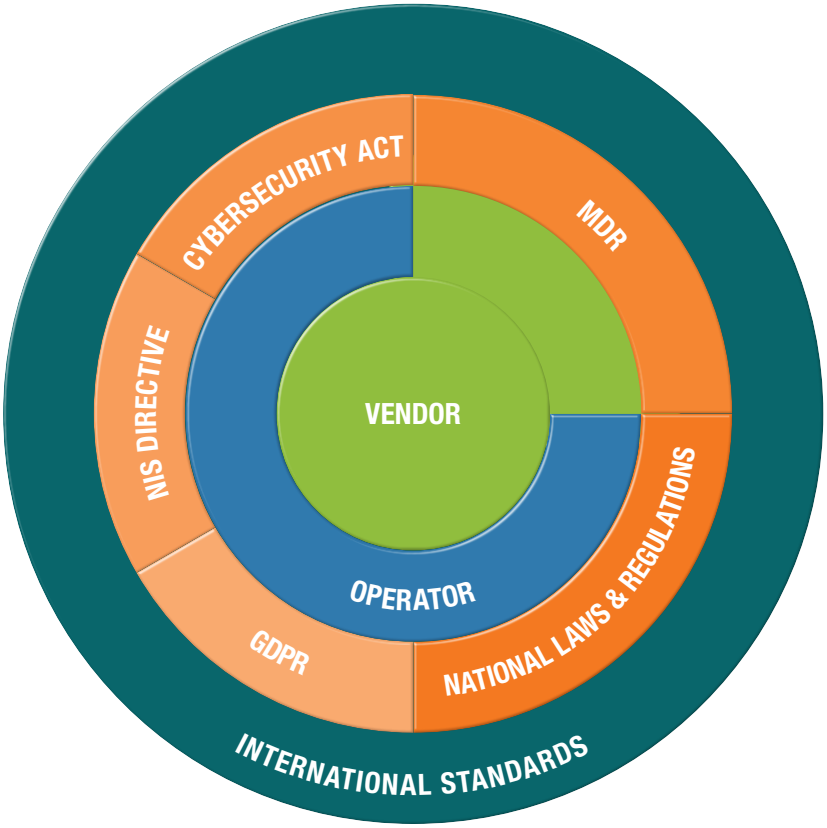


Figure 1: Overview of the framework for cybersecurity in Europe's health sector

This document outlines the different requirements introduced by the various legislative frameworks and the challenges these pose to the industry, as well as our recommendations to ensure that digital health technologies in Europe remain secure.

3. MEDICAL DEVICE REGULATION

The new Medical Device Regulation[2] (MDR) that enters into force on 26 May 2020 introduces new General and Safety Performance Requirements for the security of devices (see Annex I). COCIR, together with regulators, is currently contributing to developing EU guidance on how to interpret these requirements and support industry in implementing the Regulation.

As the MDR is the first CE-marking legislation to introduce security requirements, the medical device sector will likely serve as an example for other industry sectors. It is therefore important to set the right example, while at the same time acknowledging the specific needs of medical devices, i.e. that safety risks should always outweigh security risks.

In general, any further guidance on cybersecurity should draw on both the current state-of-the-art as expressed in international standards (see dedicated section below) and existing guidance documents, such as the German Cyber Security Requirements for Network-connected Medical Devices[3]. The minimum requirements for industry should be based on a range of well-established security frameworks to ensure the appropriate level of security required by the intended use in design and in operation.

4. DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS

The Directive on Security of Network and Information Systems[4] (NIS) entered into force in August 2016 and had to be transposed into national law of the Member States by May 2018. The NIS Directive provides legal measures to boost the overall cybersecurity levels in the EU by ensuring:

1. Member States establish a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
2. All Member States cooperate in order to support and facilitate strategic cooperation and to exchange security information;
3. A culture of security across sectors which are vital for our economy and society, relying heavily on ICT.

Operators of Essential Services (critical infrastructures) and Digital Service Providers need to adopt risk management practices and notify significant security incidents to the national competent authorities. The specific operators who are in scope and the concrete security requirements are identified at the national level.

There have been considerable delays in transposing the NIS Directive into national legislation. In addition, several Member States have yet to identify their operators of essential services. It is crucial that national implementation is finalised as early as possible to provide legal certainty for operators. The European Commission and ENISA play an important role in coordinating the implementation and facilitating convergence between Member States as much as possible to avoid requirements diverging.

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745
3 German Federal Office for Information Security, Cyber Security Requirements for Network-Connected Medical Devices, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.pdf?__blob=publicationFile&v=5
4 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

5. GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) entered into force on 25 May 2018. This introduced stricter rules on the processing and transfer of individuals' personal data in the EU. The GDPR also contains specific provisions on the security of personal data. Whereas technical and organisational measures for ensuring a level of security should be appropriate to the risks linked to the processing activities, there are more prescriptive provisions on timing, communication and responsibilities concerning data breaches.

In the event of a data breach, the data controller is obliged to inform the supervisory authority for data protection within 72 hours after becoming aware of the issue. They are also obliged to document all information relating to this breach, including facts, effects and remedial actions. In severe cases, they are also obliged to communicate the data breach to all data subjects involved without undue delay.

As the GDPR introduces a one-stop-shop principle in terms of activities, the data controller normally only interacts with a single lead supervisory authority. This is different from other regulations, where organisations may need to work with the supervisory authorities in each individual country. Furthermore, the GDPR permits Member States derogations in many different areas, undermining a uniform approach to data protection throughout the EU.

An appropriate way to handle the security requirements under the GDPR from a sector perspective is to work according to an approved code of conduct. As such codes of conduct would require approval from the European Data Protection Board, there are however limits as to what the code of conduct can describe.

Furthermore, the code of conduct should be able to describe procedures specific to the sector, rather than defining additional measures over and above the existing legal requirements under the GDPR.

6. CYBERSECURITY ACT

The forthcoming Cybersecurity Act provides for a European cybersecurity certification scheme. An overarching European Cybersecurity Certification Group will be established and each country will need to appoint a certification supervisory authority. Creating these structures may cause additional fragmentation of, and/or overlaps with, existing security policies.

Whereas the cybersecurity certification in principle is voluntary, this can be overruled by any Union or Member State law. As a consequence, a patchwork of regulatory requirements may appear, as Member States introduce their own requirements for cybersecurity certification.

COCIR calls upon the Commission, ENISA and EU Member States to ensure a harmonised European approach to the scope and obligations of the cybersecurity certification mechanism.

We understand that policy makers have decided that wherever a specific regulated framework applies, then security will be managed through that framework. A specific certification scheme for medical devices is therefore not necessary, as the MDR introduces security requirements that will become part of the certification for receiving the CE mark. For other connected technologies and processes in the healthcare setting, these need to comply with the basic security requirements as set out by self-assessment schemes to be developed under the Cybersecurity Act.

7. INTERNATIONAL STANDARDS

There are a large number of security standards from (Inter)national Standards Development Organisations and many other bodies. There are security elements in several medical device standards (e.g. IEC 60601-1 Ed 3.1) but there are no specific security standards that directly apply to medical devices or medical software. Only a few standards focus on healthcare security, but these primarily address the health delivery organisations. New work items focus on how to apply established base security standards within the healthcare domain.

Certain products may benefit more from a specific security standard. For example, developing a cloud-based distributed clinical decision support solution may benefit from using a different security standard to that for developing the security controls for an ICD (implantable cardioverter defibrillator).

At a high level, all security standards overlap. However, on a more granular level, the specific security controls, level of assurances and product or organisational scope are what make the difference. Security standards applied to a product are based on the type of product and its intended use, the market and customer demand.

The European Union needs to recognise the different well-established horizontal security frameworks to ensure the appropriate level of security by design and in operation. In the medical domain, these should of course be accompanied by healthcare-related standards. A first overview of applicable (healthcare) security standards is provided in Annex II.

8. CONCLUSIONS

COCIR remains actively involved in on-going discussions with various regulators. However, we need to broaden the discussions to ensure better harmonisation and alignment to the European and national laws that set security requirements for products and services.

We must recognise that a single medical device will need to implement security features that originate from multiple regulatory frameworks (MDR, GDPR, NIS etc.). As such, security cannot be addressed from an isolated viewpoint.

RECOMMENDATION 1: **SET UP** a broad European discussion for establishing good security practice in all regulatory frameworks to reduce market access limitations, conflicting requirements and unnecessary administrative burdens.

Cybersecurity threats are usually not restricted by country borders. Nor do they recognise the application of a system; they attack the vulnerabilities in the technology used by a system. Furthermore, many security practices and standards are not sector-specific.

RECOMMENDATION 2: **PROMOTE** the regulatory convergence between EU Member States and industry sectors

Healthcare delivery organisations rely on safe, effective and secure systems as business-critical factors. Ineffective management in implementing and using connected systems can threaten the capacity to deliver health services. Therefore, security management needs to be an important part in the in-depth security strategies of both the vendor and healthcare delivery organisation. Everyone recognises that security is a shared responsibility, but there is no clear guidance on how this should be established and where certain responsibilities cross from one to the other party.

RECOMMENDATION 3: **DEVELOP** European guidance to clarify the concept of shared responsibility, including criteria for the determination of the device's intended environment.

Information sharing is an area that requires a standardised approach. The MDS2 form is a well-recognised industry best practice that is undergoing a major update to satisfy the changing needs of the industry. Currently under cooperation of both healthcare delivery organisations and medical device vendors, the form has been extended with more detailed information on items such as patch management, network environment and software bill of materials. It is advisable to use this form to ensure a consistent approach to sharing information on security and privacy features between medical device vendors and healthcare delivery organisations.

RECOMMENDATION 4: ADOPT the new MDS2 form (currently under revision and expected to be adopted in Summer 2019) as a means to document and communicate medical device security and privacy features in Europe.

Incident reporting is another area where we see increasing numbers of organisations that need to be informed about a single security incident. In some examples, multiple competent authorities in a single country, e.g. for privacy (GDPR), critical infrastructures (NIS), medical device (MDR) have to be informed. A more centralised approach could expedite this process and reduce the administrative burden. There should be clear guidance on how national and European Computer Emergency Response Teams (CERT) work with each other. In addition, it should be clarified whether vendors need to communicate with every national CERT when a product has been brought onto the market or, to reduce the administrative burden, a single report to one CERT will suffice instead.

RECOMMENDATION 5: **COORDINATE** a European approach to security-related incident reporting to avoid duplication and confusion.

Laws and regulations are most effective where they are supported by strong market surveillance activities by the relevant authorities. This is also the case for cybersecurity, where regular checks are crucial. To make this a reality, national authorities and agencies need to have the right tools and resources.

RECOMMENDATION 6: **SAFEGUARD** a level playing field by ensuring consistent and effective market surveillance measures are in place to ensure compliance with the existing regulatory framework.

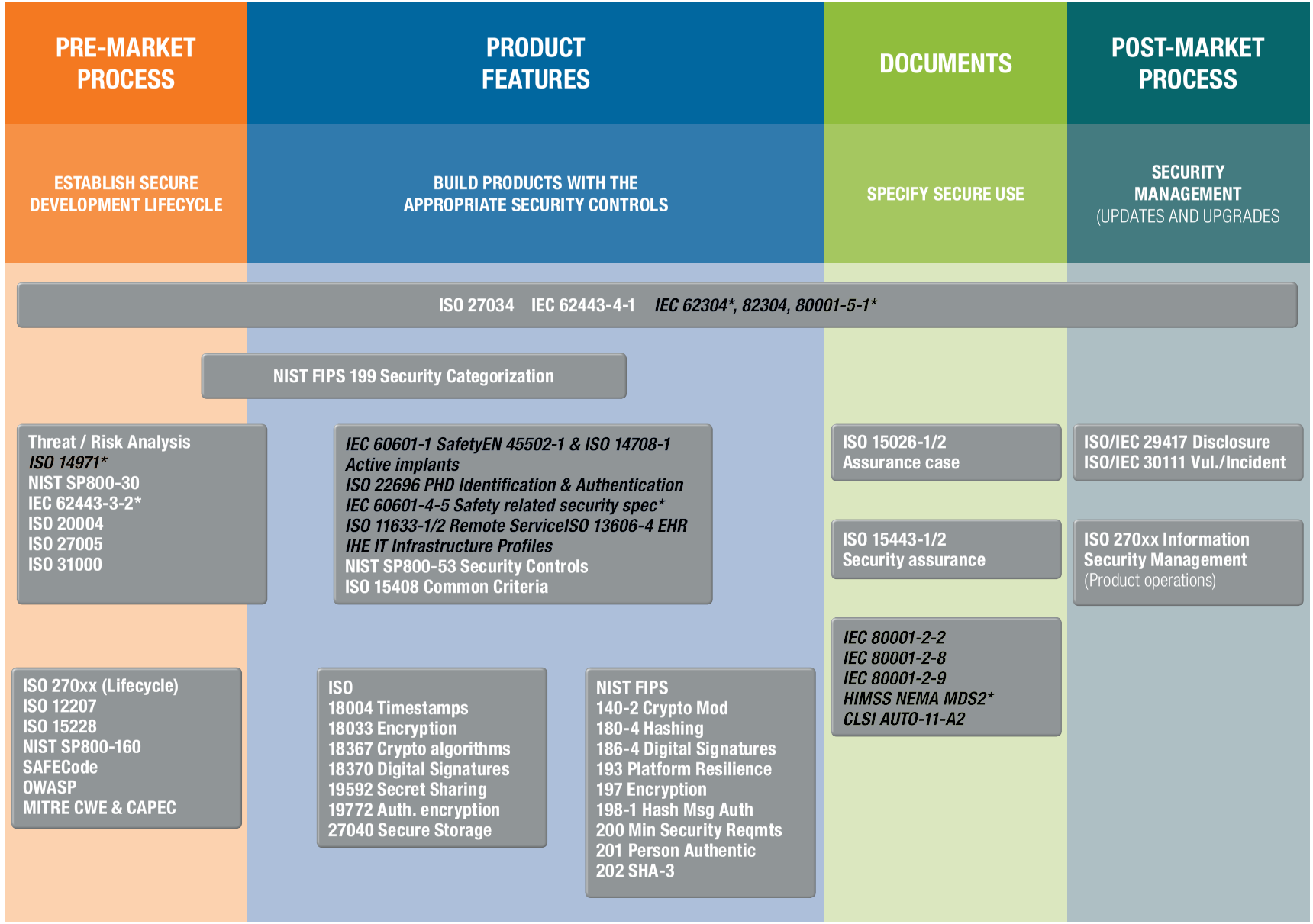
Certificates, and particularly product certificates, are seen by many regulators as one of the solutions to the issue of cybersecurity. However, we must not underestimate the complexity of the problem. Only the combination of technical and organisational measures can achieve cybersecurity. Rather than introducing further product certificates that may create a false sense of security in both vendors and users, it would be better to audit an organisation's capability to detect, respond and recover from new vulnerabilities and risks through well-established lifecycle processes.

RECOMMENDATION 7: **AVOID** multiple certification schemes for the same technologies and processes.

ANNEX 1.
SECURITY REQUIREMENTS IN MEDICAL DEVICE REGULATION

ORGANIZATION: **STATE OF THE ART INFORMATION SECURITY MANUFACTURING** ANNEX I.17.2					
Device: **ENVIRONMENT** Annex I.14.2(d)	Device: **REPEATABILITY** Annex I.17.1	Device: **RELIABILITY** Annex I.17.1	Device: **PERFORMANCE** Annex I.17.1	Device: **ACCESS CONTROL** Annex I.17.4 Annex I.18.8	Labeling: **SECURITY MEASURES & NETWORK CHARACTERISTICS** Annex I.17.4 Annex I.23.4(ab)

ANNEX 2. OVERVIEW OF APPLICABLE SECURITY STANDARDS



Black italic = Healthcare specific
***** = New or being revised

GENERAL INFORMATION ABOUT COCIR

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries.

Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007. COCIR is unique as it brings together the healthcare, IT and telecommunications industries.

Our focus is to open markets for COCIR members in Europe and beyond. We provide a range of services in the areas of regulatory, technical, market intelligence, environmental, standardisation, international and legal affairs.

COCIR is also a founding member of DITTA, the Global Diagnostic Imaging, Healthcare IT and Radiation Therapy Trade Association (*www.globalditta.org*).

COCIR COMPANY MEMBERS:

Abbott 雅培 · ACCURAY · AGFA HealthCare · AGFA · Alcon A Novartis Division · alert · align · BAYER · Canon CANON MEDICAL · Carestream · CHANGE HEALTHCARE · Elekta · EOS imaging · Epic · esaote · FUJIFILM · GE · HITACHI Inspire the Next · HOLOGIC The Science of Sure · iba · IBM · 强生(中国)医疗器材有限公司 Johnson & Johnson Medical (China) Ltd. · KONICA MINOLTA · Medtronic 美敦力 · nova motum SERVICES & CONSULTING · PHILIPS · SAMSUNG · SIEMENS Healthineers · varian · WeHealth by SERVIER · ZEISS

NATIONAL TRADE ASSOCIATIONS MEMBERS:

AGORIA BELGIUM	snitem creating the tools for medical progress FRANCE	bvitg GERMANY	ZVEI: GERMANY
ETOSZ ASSOCIATION OF HEALTH TECHNOLOGY SUPPLIERS AND MEDICAL DEVICE MANUFACTURERS HUNGARY	ASSOBIOMEDICA ITALY	apormed PORTUGAL	FHI MEDICAL TECHNOLOGY THE NETHERLANDS
fenin federación española de empresas de TECNOLOGÍA SANITARIA SPAIN	SWEDISH Medtech SWEDEN	TIP GÖR DER TURKEY	AXREM UNITED KINGDOM

COCIR HOW TO JOIN US
COCIR aisbl | Bluepoint Building | Boulevard A. Reyerslaan 80 | 1030 Brussels | Belgium
Tel +32 (0)2 706 89 60 | Email info@cocir.org | www.cocir.org | @COCIR