MedTech Europe's vision for cybersecurity in the medical technology ecosystem

May 2023

POSITION PAPER

MedTech Europe
from diagnosis to cure

Contents

Executive Summary

The digital ecosystem has dramatically changed the way in which healthcare is delivered to patients. Nowadays, medical technology companies concentrate not only on ensuring the safety and security of MDs and IVDs, but also on the protection of patients' and users' confidential data. As such, medical device manufacturers invest substantial resources in guaranteeing state of the art cybersecurity for all their products and services, ensuring the resilience of the digital health ecosystem.

In this position paper, MedTech Europe outlines three key areas of discussion for regulators, medical device manufacturers, healthcare systems and society-at-large.

Firstly, that the security of medical technologies continues to be regulated under sectoral legislation. The Medical Devices Regulation and the *In Vitro* Diagnostic Medical Devices Regulation ('MDR' and 'IVDR') lay out essential requirements for digital medical technologies and services, including Medical Device Software (MDSW) placed on the EU market. In addition, MDCG 2019-16 rev.1 guidance on cybersecurity, provides medical technology manufacturers with the necessary guidance on fulfilling the relevant General Safety and Performance Requirements of MDR and IVDR respectively, with regards to cybersecurity. It also provides guidance on how to comply with both the Network and Information Security Directive ('NIS1'), and the General Data Protection Regulation ('GDPR'), both of which apply to medical technology manufacturers.

Secondly, the paper underlines MedTech Europe's commitment against ransomware, and other malicious interference with healthcare delivery in Europe. MedTech Europe welcomes legislative interventions aimed at reinforcing existing cybersecurity responsibilities and curbing tactics employed by potential cyber-attackers and cyber-criminals. The ongoing digital transformation of society and the lagging digitalisation of healthcare institutions and healthcare delivery continue to lead to healthcare being prime target for malign actors. MedTech Europe welcomed the revision of the Network and Information Security Directive (known as 'NIS2'), as a means of reinforcing the digital resilience of states and businesses, while ensuring that they increase their investments in cybersecurity. While we welcome such legislative intervention, we believe that it should be combined with tangible investments in organisations' security postures, resilience of digital tools and processes, and the investment in people and the skills necessary to deliver on such legislation.

Finally, the paper highlights MedTech Europe's support for measures aimed at improving the level of overall digital literacy, and particularly, cybersecurity skills. The evolving cybersecurity threat landscape coupled with a significant European cybersecurity skills shortage is an untenable situation, and must be addressed. MedTech Europe supports a public-private partnership approach to confront these issues. We also applaud the European Commission's efforts to improve the situation, particularly through the European Skills Agenda Digital Education Action Plan, as well as the recently published communication for a Cybersecurity Skills Academy.

Introduction

Medical devices (MDs) and *In Vitro* Diagnostic (IVDs) medical devices offer the promises of innovation, improved access and streamlined delivery of healthcare to patients and support to healthcare professionals. Using state of the art security for digital medical technologies and services to keep users and patients safe is a bedrock principle of the medical technology industry and sectoral regulation.

The digital ecosystem has fundamentally changed the nature and delivery of healthcare. Nowadays, medical technology companies concentrate not only on ensuring the safety and security of MDs and IVDs, but also on the protection of patients' and users' confidential data, as linked for example to personalised software-driven diagnoses and treatments. Hence, medical device manufacturers continue to invest significant resources in guaranteeing state of the art cybersecurity for all their products and services, while ensuring the resilience and integrity of the digital health ecosystem as a whole.

The medical technology industry is called to engage fully in national, European and global conversations on cybersecurity. MedTech Europe, as the association representing the medical technology industry to the European Union, commits fully to these conversations. Our sector engages directly with stakeholders from the Medical Devices Coordination Group (MDCG), the Stakeholder Cybersecurity Certification Group (SCCG), the EU Agency for Cybersecurity (ENISA) and its eHealth Security Experts Group, and the European Commission, as well as other relevant EU actors, including Standard Development Organisations. On a global level, MedTech Europe, via its members, continues to actively contribute to the work of the International Medical Device Regulators Forum (IMDRF), including to its Cybersecurity Working Group.

With this position paper, MedTech Europe seeks to outline that:

- Sectoral regulation (the Medical Devices Regulation and the *In Vitro* Diagnostic Medical Devices Regulation) should remain the primary avenue to providing state of the art cybersecurity of digital medical technologies and services and the safety and security of patients and users;
- The medical technology industry has an integral role to play in creating a more resilient shared healthcare ecosystem, aiming to prevent potential cyberattacks, such as malwares or more specifically, ransomware attacks;

Public-private partnerships and the investment in education, awareness and infrastructure should be paramount to the delivery of cybersecurity in the healthcare ecosystem.

The three pillars of a cyber resilient medical technology ecosystem

In this paper, MedTech Europe outlines three key areas of discussion for regulators, medical device manufacturers, healthcare systems and society-at-large. These areas are important to have in order to create

a more cyber resilient healthcare ecosystem, and building a system that works for users and patients, health-supporting infrastructures and medical technology manufacturers.

MDR/IVDR: Ensuring safety and security for patients and users

The safety and security of patients and healthcare professionals is of the utmost importance to medical technology manufacturers. State of the art medical technologies tend to have digital components, or a connection to sensitive assets, such as health data or a hospital network. For example, medical devices, personalised IVDs, and precision treatments require a full data lifecycle management to be designed and maintained correctly, in order to protect confidential patient data. Therefore, as industry, we believe that medical technologies must be protected from malicious actors. These actors may seek to do harm to the well-being of patients, the functioning of hospitals, and the integrity of the healthcare ecosystem, often with the purpose of satisfying criminal economic and disruptive activities. With this in mind, the medical technology industry firmly adheres to a range of cybersecurity, data protection, and sectoral product legislation in the EU, including the Medical Devices Regulations (MDR/IVDR).

The security of medical technologies continues to be regulated under sectoral legislation. Specifically, the Medical Devices Regulation[1] and the *In Vitro* Diagnostic Medical Devices Regulation[2] ('MDR' and 'IVDR') lay out comprehensive, essential requirements for digital medical technologies and services, including Medical Device Software (MDSW) placed on the EU market. In terms of cybersecurity provisions, these and other sectoral requirements include:

- pre- and post-market requirements covering a device's design process, directly relating to risks associated with any potentially negative interaction between a MDSW and the IT environment within which it operates;
- requirements to perform structured mandatory third-party conformity assessment for the vast majority of connected medical technologies and services, in order to obtain a CE ("*conformité européenne"*) marking;
- requirements to lay out an effective Quality Management System (QMS), ensuring continued incident reporting following a device being placed on the market throughout its entire lifecycle;
- requirements to adhere to strict Post-Market Surveillance (PMS) systems for devices, including software, as well as maintain continuous vigilance for a possible malfunctioning of a device (including those which might be caused by cyberattacks);
- And, with respect to Medical Device Software (MDSW), both MDR and IVDR also provide that a device integrating software or medical device software itself is *"developed and manufactured in accordance with the state of the art taking into account the principles of development lifecycle, risk management, including information security, verification and validation"*[3].

[1] Medical Devices Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745
[2] *In Vitro* Diagnostic Medical Devices Regulation https://eur-lex.europa.eu/eli/reg/2017/746/oj
[3] Medical Devices Regulation, Annex I on General safety and performance requirements, Chapter I, 17.2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

Thus, MDR/IVDR wholly account for cybersecurity throughout a medical device's lifecycle. MDCG 2019-16 rev.1 guidance on cybersecurity[4], was developed by regulators, notified bodies, hospital associations and medical device industry associations, as part of the Medical Devices Coordination Group (MDCG), the MDR/IVDR-established body. This provides medical device manufacturers with additional guidance on fulfilling the relevant General Safety and Performance Requirements of Annex I MDR and IVDR respectively, with regards to cybersecurity. Given the inherent complexity of MD/IVD supply chains and the role played by many operators therein, additional expectations from other stakeholders (aside from manufacturers) are provided in the guidance. Cybersecurity requirements listed in Annex I MDR/IVDR, which address both pre- and post-market aspects are also clarified in the guidance.

The medical technology industry implements and complies with other EU legislation, including the Cybersecurity Act[5], the General Data Protection Regulation[6], the Network and Information Security (NIS1)[7] and international standards and regulations on cybersecurity. The new NIS2 Directive, which replaced NIS1, further emphasises the importance and responsibilities of the medical technology manufacturers in the supply chain to achieve a higher level of security in healthcare. These provisions provide a basis for medical device manufacturers to comprehend and implement the range of cybersecurity and data protection requirements across the entirety of a medical device's lifecycle. As such, the framework helps to ensure cybersecurity of a medical device from their inception, design, and development to the end of life and decommissioning of the device.

Finally, medical technology manufacturers ensure that third parties involved in device manufacturing and operation (e.g., hosting) have measures in place from a security and/or internal controls perspective and support continuous improvement in information security through periodic assessments and certifications by independent external experts.

A Multistakeholder Approach to Ransomware

Ransomware is a form of malicious cyber activity in which a cybercriminal illegally enters a system via one of several attack vectors (i.e., depicts a type of malware like viruses, trojans, etc.). The threat actor then deploys malware that encrypts and potentially exfiltrates or corrupts an organisation's IT applications and data, effectively holding it hostage, as the victims cannot partially or fully use the data stored on it until a 'ransom' is paid. Ransomware has grown in depth and impact to become one of the most prevalent methods of malicious cyber activity affecting hospitals and healthcare organisations. With healthcare systems widely considered as critical infrastructure by EU Member States, healthcare organisations may often be faced with a difficult choice between either 'paying' a ransom to cyber-criminals or risk impacting the well-being of patients under their care. IBM Security's 'Cost of a Data Breach Report 2022' is a stark reminder of this,

[4] MDCG 2019-16 rev.1 guidance on cybersecurity https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native
[5] Cybersecurity Act https://eur-lex.europa.eu/eli/reg/2019/881/oj
[6] General Data Protection Regulation https://eur-lex.europa.eu/eli/reg/2016/679/oj
[7] Network and Information Security Directive https://eur-lex.europa.eu/eli/dir/2016/1148/oj

indicating that healthcare continues to incur the highest costs from a ransomware attack.[8] More broadly, in 2022, the EU cybersecurity agency, ENISA, published its annual Threat Landscape report, which reported that ten terabytes of data were stolen by cyber-criminals each month of 2022 as a result of ransomware attacks.[9] ENISA also reported that approximately 60% of all organisations targeted by ransomware may have paid the ransom demands. In its Communication for a Cybersecurity Skills Academy, the European Commission noted that "ransomware threat actors are routinely inflicting considerable damage, both financially and reputationally, to entities."[10]

A cybersecurity breach in a hospital or healthcare facility can result in major difficulties. In May 2021, the Health Service Executive HSE (the Irish public healthcare system) was the victim of a major ransomware attack,[11] suffering an immediate loss of access to all HSE provided IT systems, including patient information systems, clinical care systems and laboratory systems. It also caused major disruption to the delivery of healthcare services across the country. Non-clinical systems such as financial systems, payroll and procurement systems were also lost.[12] This significant cyber breach resulted simply from the opening of a malicious MS Excel file via a phishing email. A separate ransomware attack taking place in France in August 2022, targeting the Centre Hospitalier Sud Francilien, resulted in 11GB of personal and medical data, including staff-related data, being compromised and later published by the threat attacker.[13]

MedTech Europe and the medical technology industry are committed to exploring methods to address criminal interference and interruption to healthcare delivery in Europe. We applaud legislative intervention aimed at reinforcing shared cybersecurity responsibilities and curbing emerging and expanding vectors of attack used by potential cyber-attackers and cyber-criminals. That said, the ongoing digital transformation of society coupled with a lagging digitalisation of healthcare institutions and healthcare delivery, continues to position healthcare as a prime target for malign actors. MedTech Europe welcomed the revised Network and Information Security Directive (NIS2)[14] as a means of reinforcing the digital resilience of states and businesses, while ensuring that they increase their investments in cybersecurity. While we welcome such legislative intervention, the legislation should be combined with tangible investments in organisations' security postures, resilience of digital tools and processes, and the investment in people and the skills necessary to deliver on such legislation.

Investment in Education and Training in Cybersecurity

In addition to legislative measures, effective European, national, and organisational cybersecurity strategies require sound actions to improve digital literacy, and in particular, cybersecurity skills. Such actions can take

[8] IBM Security 'Cost of a Data Breach Report 2022' https://www.ibm.com/downloads/cas/3R8N1DZJ
[9] 'ENISA Threat Landscape 2022' https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[10] Cybersecurity Skills Academy https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy
[11] Irish Times: 'Opening of email attachment led to HSE cyber attack, report finds' https://www.irishtimes.com/news/crime-and-law/opening-of-email-attachment-led-to-hse-cyber-attack-report-finds-1.4752043
[12] Conti cyber attack on the HSE: Independent Post Incident Review https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
[13] PANORAMA DE LA CYBERMENACE 2022 https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
[14] Revised Network and Information Security Directive (NIS2) https://eur-lex.europa.eu/eli/dir/2022/2555

many forms, such as investments in cybersecurity education and training at EU Member State's national curricular level (secondary and/or tertiary), as well as extra-curricular certificates and continuing professional development and life-long learning activities for relevant staff. Public-private partnerships are more important than ever to achieve these goals. Leveraging the combined expertise of industry, EU Member States, academia, and civil society will be paramount, in order to respond to prolific cybersecurity incidents in the digital space. However, recent investments have not yet reached that ambition, and there still remains a global shortage of a sufficiently educated cybersecurity workforce trained to withstand and respond to the malign cyber activity of today. According to the European Commission's own statistics on tackling the existing European digital skills gap, more than 70% of businesses say that "the lack of staff with adequate digital skills is an obstacle to investment."[15] All stakeholders share a collective interest in addressing this gap.

To counter this shortfall, the European Commission has set out ambitious goals through the European Skills Agenda and the Digital Education Action Plan, to provide 70% of European adults with basic digital training and skills by 2025.[16] The two European initiatives also hope to reduce the level of 13–14-year-olds underperforming in computing and digital literacy by 50% by 2030. Specifically in healthcare, stakeholders from across the ecosystem have identified cyber-resilience as a crucial necessity over the coming years. The healthcare sector might draw inspiration from a recent Horizon 2020-funded project, PANACEA[17], which developed a toolkit to reinforce overall cybersecurity for hospitals and the delivery of healthcare. In addition, in April 2023, the European Commission published a Communication on a Cybersecurity Skills Academy.[18] The Cybersecurity Skills Academy lays out plans at bringing together existing European initiatives on cybersecurity skills and improving their coordination, with the goal of closing the cybersecurity skills gap, and thus, reinforcing the EU's competitiveness, growth and resilience.

Finally, MedTech Europe encourages EU and national policymakers, and other stakeholders, to support an increased patient and public awareness of the different types of risks associated with cybersecurity in healthcare. Most importantly, this should be done through the development of basic education on data security standards to improve fundamental awareness of cybersecurity risks for all types of end users (including healthcare professionals and patients).

The medical technology industry acknowledges its role in the EU regulatory environment in the prevention of cybersecurity incidents. Cybersecurity is a shared responsibility, with all actors across the healthcare and digital ecosystem having a part to play. MedTech Europe supports a policy and investment environment which recognises this shared responsibility. We are eager to explore how we can engage actively to provide our input to design and develop solutions to address the ongoing investments in digital and cybersecurity skills gap, and to reinforce the resilience of healthcare systems. Through this, MedTech Europe is confident that Europe can encourage and foster the delivery of innovative, secure, safe and sustainable healthcare to patients.

[15] Digital skills and jobs, European Commission https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs
[16] European Skills Agenda, European Commission https://ec.europa.eu/social/main.jsp?catId=1223
[17] PANACEA https://cordis.europa.eu/project/id/826293
[18] Cybersecurity Skills Academy https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.
www.medtecheurope.org.

For more information, please contact: Benjamin Meany, Manager Digital Health – Medical Device Software Regulation