NIS 2 Directive Adoption
Proposal for a Directive on measures for a high common level of Cybersecurity across the Union
2020/0359 (COD)

Final Draft, 17 March 2021

1. Introduction

MedTech Europe **welcomes** the opportunity to provide the comments of the medical technology industry to **the proposed revised Directive on Security of Network and Information Systems** (NIS 2 Directive) [1] with the aim **to strengthen cybersecurity provisions** in Europe. The **digital transformation of society** and the plan to realise a European Health Data Space require trust in the security of digital health tools as well as adapted and innovative responses to **new cybersecurity threats**.

Healthcare organisations and business associates (e.g., vendors, manufacturers in the procurement and supply chain) must implement robust security measures to protect patient data (i.e., Personally Identifiable Information (PII) and Patient Protected Health Information (PHI)) from an increasing number and variety of threats. Vulnerabilities in wireless networks, for instance, may offer an easy entry point for hackers. Yet, these networks are of critical importance to healthcare organisations, as they facilitate access to patient information and optimise the delivery of care. Best practices for healthcare cybersecurity need to keep pace with the evolving threat landscape, addressing threats to privacy and data protection on endpoints and in the cloud, and safeguard health data while in transit, in use or at storage/rest. Achieving security of private and health data requires a harmonised and sophisticated approach. In this regard, the **NIS 2 Directive** lays the groundwork for **coordinated cybersecurity action**, which is fundamental to ensuring a safe digital transformation.

Overall, MedTech Europe welcomes the NIS 2 Directive proposal as an improvement over the current NIS Directive. Relevant guidance on specific elements and other non-legislative measures could promote further harmonisation and clarity. For example, comprehensive sectoral guidance could provide more clarity on how to act when cyber incidents are putting healthcare and patient safety at risk.

The medical technology (“medtech”) industry is at the heart of the health data ecosystem and a critical enabler for the digital transformation of healthcare. The medtech industry is fully committed to delivering products and services that benefit from top-notch cybersecurity provisions, assuring state of the art in information security. Given the high sensitivity of health data, the medtech industry needs to be part of the conversation when new cybersecurity provisions are discussed.

2. Context of the proposal

- **Reasons for and objectives of the proposal**
  MedTech Europe welcomes the intention to give the EU more competences to further improve the

[1] The document is available here for download.

resilience and incident response capacities of the Union in the field of cybersecurity and critical infrastructure protection, especially in response to the COVID-19 crisis and the digital transition of the healthcare sector.

- **Consistency with existing policy provisions in the policy area**
  MedTech Europe welcomes this proposal and its close alignment with the proposal for a Directive on the Resilience of Critical Entities, intending to enhance the resilience of critical entities against physical threats in the healthcare sector. The medtech industry supports a policy framework for enhanced coordination between the competent authorities under this Directive and the Directive on the Resilience of Critical Entities for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

- **Consistency with other EU policies**
  MedTech Europe agrees that a consistent approach to international cooperation is needed and that this Directive shall constitute a reference model to be promoted in the context of the EU's cooperation with third countries, notably when providing external technical assistance. The medtech industry believes that continued support and awareness are necessary to develop a risk-based and outcomes-focused cybersecurity framework that leverages international standards that are relevant across sectors, particularly in healthcare.

3. The legal framework

- **Legal basis**
  The medtech industry believes that the NIS 2 Directive has a robust legal basis, which would establish clear, generally applicable rules on the scope of application of the NIS Directive as well as harmonise the rules applicable around cybersecurity risk management and incident reporting. MedTech Europe would like to add that relevant guidance on specific elements and other non-legislative measures can promote further harmonisation and clarity. For instance, the industry would benefit from a comprehensive guidance on how to act when cyber incidents such as a malware attack (including ransomware, spyware, etc.) are putting at risk the health of patients or the integrity of a manufacturing plant.

- **Subsidiarity (for non-exclusive competence)**
  MedTech fully agrees that cybersecurity resilience across the European Union cannot be effective if approached through national or regional silos. The medtech industry supports an increased EU intervention which goes beyond the rules of the old NIS Directive and is justified by (1) the increasingly cross-border nature of the NIS-related threats and challenges, (2) the potential of EU action to improve and facilitate effective and coordinated national policies, and (3) the contribution of collaborative policy actions to effectively protect data protection and privacy.

- **Proportionality**
  The medtech industry is interested in reducing fragmentation across Member States and implementing more harmonised requirements in the Digital Single Market. Therefore, it supports the enhanced level of protection that would be achieved by the NIS 2 Directive through coordinated

requirements, which are proportionate to the increasingly high cybersecurity risks, including cross-border elements.

4. Clarifications and Comments

- **Subject matter and scope of the proposal (Article 1 and 2):** MedTech Europe would recommend clarifying (1) how the obligations for the Member States to adopt a national cybersecurity strategy are established; (2) whether these obligations are harmonised; (3) whether information sharing is mandatory; (3) the potential consequences, should there be a lack of trust in the recipient of the information; (4) whether medtech manufacturing plants or devices, if attacked, are considered to represent a disruption of public health; and (5) who determines what confidential information should be shared, be it the Member States, ENISA, the Competent Authorities of a specific sector, or Law Enforcement Authorities. MedTech Europe also calls for harmonisation across the lists of entities that Member States shall establish and submit to the Commission.
- **Definitions (Article 4):** MedTech Europe would recommend clarifying whether public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded from the NIS 2 directive obligations and, should it be the case, how these entities are controlled.
- **Coordinated national cybersecurity frameworks (Articles 5 to 11)** and, particularly, the requirement for Member States to designate one or more national competent supervisory authorities on cybersecurity and a national Single Point Of Contact on cybersecurity (SPOC): MedTech Europe notes that many competent authorities may create more bureaucracy, which may increase costs to the Member States as well as create a burden for the companies impacted as important or essential entities. In addition, given the total amount of policies (189 = seven for each Member State) and guidelines (27 = one for each Member State) impacting the different sectors and required as part of the national cybersecurity strategy, the medtech industry believes that harmonised policies, where Member States may have their own deviations tailored to their countries specificities, would be beneficial. Moreover, the industry fully supports the **voluntary** nature of information sharing.
- **Coordinated vulnerability disclosure and a European vulnerability registry (Article 6)** developed and maintained by ENISA: the medtech industry believes that in this case ENISA should implement a mechanism to establish the good faith of the 'interested' parties on the vulnerability information, as there may be reasons for which the manufacturers may not want to share this sort of information with parties that may use the information for malicious purposes.
- **National cybersecurity crisis management frameworks (Article 7)**, according to which each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises: the medtech industry believes this may create an unnecessary economic burden to Member States.
- **National competent authorities and Single Points of Contact (Article 9)**, according to which each Member State shall make public their designation and the Commission shall publish the list of the designated SPOC. The medtech industry would recommend clarifications about when and where the list will be published and whether the European Commission or ENISA will announce it.
- **Computer Security Incident Response Teams (CSIRTs) (Article 9):** MedTech Europe would recommend clarifying whether the CSIRTs, designated by the original NIS Directive, will be confirmed and/or whether new CSIRTs will be created, especially for those new sectors/entities,

added under the scope of the NIS 2 Directive (in the lists in Annex I and II). In addition, the medtech industry would suggest specifying where CSIRTs will provide dynamic risk and incident analysis as well as situational awareness regarding cybersecurity and whether it would be possible for manufacturers to be informed about which interested parties the information concerning their vulnerabilities will be shared with.

- **Cooperation at national level (Article 11),** according to which where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20. The medtech industry suggests clarifying whether it would be possible for Member States to decide that only the Competent Authorities from the different sectors will receive the notifications, instead of the CSIRT.
- **Cooperation (Articles 12 to 16):** the medtech industry believes that a biennial report on the state of Cybersecurity in the Union issued by ENISA in cooperation with the Commission would help to have an overview of the cybersecurity health of critical networks.
- **Cybersecurity risk management and reporting obligations (Articles 17 to 23),** according to which Member States are required to provide that management bodies of all entities, under the scope, approve the cybersecurity risk management measures taken by the respective entities and follow specific cybersecurity-related training. The medtech industry recommends further clarifications regarding which training, and established by whom, entities should follow. Member States are also required to ensure that entities notify the national competent authorities or the CSIRTs of any cybersecurity incident having a significant impact on the provision of the service they provide. The medtech industry would recommend clarifying whether an identified vulnerability in, or attempt to attack, entities' products and services, with no ultimate impact, can fall under the definition of 'significant impact'.
- **Cybersecurity risk management measures (Article 18)**, according to which the Commission is empowered to adopt delegated acts to take account of new cyber threats, technological developments, or sectorial specificities. MedTech Europe would suggest clarifying whether these acts will be horizontal or vertical (sectoral).
- **Use of European cybersecurity certification schemes (Article 21),** MedTech Europe opposes a cybersecurity certification scheme in our sector. We note that manufacturers of Medical Device (MD) and *in vitro* Diagnostic (IVD) already have their own certification provisions under MDR[2]/IVDR[3], which are clarified by the MDGC Guidance on Cybersecurity[4]for medical devices (including medical device software). These provisions are valid for both important and essential entities.
- **Cybersecurity information-sharing arrangements (Article 26):** the medtech industry welcomes the requirements laid down to improve cybersecurity information sharing, as long as this is realised among trusted partners and with proper sharing agreements.
- **Supervision and enforcement of essential entities (Article 29):** MedTech Europe would suggest clarifying who determines the tasks of the monitoring officer as per Art. 29.4.(g), be it through the competent authorities or ENISA guidance.
- **Supervision and enforcement for important entities (Article 31)**, according to which there are two components of fines: one concrete and with a fixed limit (10m) and one flexible and uncertain (2

[2] Regulation 745/2017 on Medical Devices
[3] Regulation 746/2017 on *in vitro* Diagnostic Medical Devices
[4] MDCG 2019-16 Guidance on Cybersecurity for medical devices

per cent of worldwide annual turnover). The medtech industry would recommend specifying whether this is based on the annual statements from the entities and, in the case of essential services/products, whether it might be only the 2 per cent of the total worldwide of that service/product (that is considered essential) or the overall economic turnover of the manufacturer. Furthermore, this article mentions "worldwide", which exceeds the Directive's scope and jurisdiction, and which could be considered punitive rather than effective, proportionate, and dissuasive. Therefore, transparency on the criteria or mitigation factors when setting fines is crucial.

- **Penalties (Article 33):** MedTech Europe would recommend having only one set of penalty rules applicable/endorsed in/by all Member States, rather than 27 different penalty rules, to avoid fragmentation.
- **Mutual assistance (Article 34)**, according to which a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30: the medtech industry would recommend clarifying if this is implying delegation of authority to another competent authority and based on what the delegation would take place.

5. Recommendations

- An adequate level of cybersecurity in healthcare is essential for ensuring the provision of medical care, patient safety and the protection of health data. Beyond protecting confidentiality, security of healthcare systems will advance the trust in the use of innovative and cutting-edge healthcare solutions. The medtech industry is committed to delivering products and services that meet requirements that contribute to these goals.
- We acknowledge the references to Medical Device (MD) and *in vitro* Diagnostic (IVD) manufacturers in Annex I, point 5 (Essential Entities) and Annex II, point 5 (Important Entities) and the supervisory measures for Essential Entities and Important Entities, e.g., ex-ante and ex-post regime versus ex-post regime. Nevertheless, we want to highlight that the medical technology industry is already under rigorous supervisory, auditing and post-market surveillance regimes that include cybersecurity requirements under the new Medical Devices Regulations (MDR and IVDR) [5] and accompanying guidance [6] (including software as medical device and IT systems). We welcome strengthened coordination between the national Single Points Of Contact on cybersecurity (SPOC) and the national competent authorities responsible for medical devices and *in vitro* diagnostics. However, in the interest of legal consistency and respect for the Lex Specialis principle, we would strongly urge against any creation of duplicative or parallel certification requirements that would exist on top of the existing cybersecurity provisions of the MDR and IVDR.
- We emphasise the high importance of consulting with the industry in drafting the list for "medical devices as critical during a public health emergency", which would classify the manufacturers as Essential Entities.
- We also note that the classification of medical devices' manufacturers as "critical during a public health emergency" and "non-critical" in other circumstances could lead to two supervisory regimes under the current proposal for a given manufacturing facility.

[5] Regulation 745/2017 on Medical Devices; Regulation 746/2017 on *in vitro* Diagnostic Medical Devices
[6] MDCG 2019-16 Guidance on Cybersecurity for medical devices

- The medtech industry stresses the importance of uniform implementation of the NIS 2 Directive across the EU Member States to avoid fragmented regulatory and procurement requirements, as laid down in Article 5.2.(b), when operating in more than one EU Member State. Additionally, after the entry into force of this Directive, it will be necessary to clarify which ENISA channels will be employed to receive the information required to maintain the registry for Essential and Important Entities (as per Article 25).
- Cybersecurity is a shared responsibility of medical device manufacturers, healthcare providers, vendors, and patients. Accordingly, the scope of this Directive should consider the risks involved, and apply the same provisions, on all players in the supply chain, to ensure a fair and balanced approach. We therefore encourage efforts to improve cybersecurity awareness through programmes initiated by the Member States' competent authorities under the proposed Directive. We encourage training for both healthcare professionals and all citizens in basic cyber skills (including digital literacy, setting up secure networks and identifying threats) with the aim to prevent data breaches and protect private and public networks.
- We support the risk management approach for both Essential Entities and Important Entities under the proposal but emphasise the leverage of current (sectoral) risk management standards and best practices that have international consensus.
- We disagree with setting fines based on "worldwide" annual turnover, which exceeds the scope and jurisdiction of the Directive, and which is considered punitive rather than effective, proportionate, and dissuasive.
- We welcome the requirements laid down in article 26 to improve cybersecurity information sharing, as long as this is realised among trusted partners and with proper sharing agreements.

MedTech Europe looks forward to working with the Commission, ENISA and all stakeholders to advance cybersecurity in healthcare.

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.

Contact: Michael Strübin, Director Digital Health, m.strubin@medtecheurope.org