Cybersecurity Act Revision

MedTech Europe's response to the public consultation

MedTech Europe welcomes the opportunity to provide feedback on the Proposal for a revised Cybersecurity Act, which seeks to strengthen the EU's cybersecurity capabilities and resilience while preventing fragmentation across the Digital Single Market. MedTech Europe represents the medical technology sector, whose members develop and deploy innovative digital health solutions, including connected medical devices, diagnostic software, and AI-enabled technologies, within a highly regulated framework designed to ensure patient safety, quality, and trust.

Digital health technologies are transforming healthcare delivery by enabling more connected, efficient, and data-driven care pathways. However, as healthcare systems and providers become increasingly digitalised and interconnected, they are also exposed to a growing and evolving landscape of cybersecurity threats. Cyber incidents affecting medical technologies or healthcare infrastructures can have direct consequences for the continuity of care, patient safety, and public trust, in addition to financial and operational impacts.

In this context, revising the Cybersecurity Act is not only a matter of regulatory compliance. A coherent, proportionate, and well-aligned EU cybersecurity framework plays a fundamental role in ensuring the secure development, deployment, and use of digital medical technologies, supporting the safe and reliable delivery of healthcare services across the EU.

While MedTech Europe supports the overarching objective of strengthening the EU's cybersecurity resilience through this proposed revision, we wish to highlight several key aspects that merit careful consideration to ensure the revised Cybersecurity Act effectively achieves its objectives in practice, while remaining workable for highly regulated sectors such as healthcare.

Proposal for a revised Cybersecurity Act

The proposed revision of the Cybersecurity Act (CSA 2) represents an important and timely initiative to strengthen the EU's cybersecurity framework in light of an increasingly complex and evolving threat landscape. For the medical technology sector, the proposal offers an opportunity to reinforce cybersecurity governance, enhance coordination at the EU level, and further support trust in digital healthcare systems. In this context, MedTech Europe welcomes the strengthening of the mandate of the European Union Agency for Cybersecurity (ENISA) and recognises its central role in promoting a consistent, effective and risk-based approach to cybersecurity implementation across Member States and sectors.

At the same time, given the critical importance of cybersecurity for the safe development, deployment and use of digital medical technologies, MedTech Europe considers that certain aspects of the proposal would benefit from further clarification and refinement. Addressing these points will be essential to ensure that the revised Cybersecurity Act delivers proportionate, coherent and workable solutions in practice, particularly for highly regulated sectors such as healthcare. Our key considerations and recommendations are set out below.

Title II: The European Union Agency for Cybersecurity

1. Ensure clarity and alignment in EU-level vulnerability handling for medical technologies

Recommendation: The revised Cybersecurity Act shall ensure that ENISA's coordination and support role in vulnerability handling is implemented in a way that avoids creating new or parallel vulnerability handling or disclosure requirements for medical technologies and preserves flexibility within existing regulatory and operational frameworks applicable to safety-critical healthcare environments.

The proposed revision strengthens ENISA's role in supporting coordination, information sharing and situational awareness in relation to cybersecurity vulnerabilities at the EU level. MedTech Europe recognises the value of enhanced cooperation and transparency in vulnerability handling to support cybersecurity resilience and address risks with potential cross-border relevance.

At the same time, vulnerability handling in the context of medical technologies involves specific considerations related to patient safety and clinical use. Medical devices (MDs) and in vitro diagnostic medical devices (IVDs) are often deployed in live healthcare environments, where remediation measures such as patching, system changes, or configuration updates may require validation, coordination with healthcare providers, user training, or scheduled maintenance windows. As a result, the timing and manner in which vulnerability-related information is communicated can be critical to ensuring that risk mitigation does not inadvertently disrupt clinical workflows or compromise safe use.

In this context, MedTech Europe considers that the coordination, support and information-sharing functions entrusted to ENISA in the area of vulnerability handling under the revised Cybersecurity Act should be implemented in a manner that does not result, in practice, in the introduction of new or parallel vulnerability handling or disclosure requirements for medical technologies that would cut across existing regulatory and operational processes. EU-level coordination and information-sharing activities should focus on supporting situational awareness and cooperation, while allowing sufficient flexibility for manufacturers and healthcare providers to manage vulnerabilities in accordance with applicable regulatory and operational frameworks and the realities of safety-critical healthcare environments.

Title III: European Cybersecurity Certification Framework

2. Avoid overlapping and duplicative cybersecurity requirements across EU legislation

Recommendation: The revised Cybersecurity Act should ensure that cybersecurity certification remains voluntary, aligned with existing EU and international product regulatory frameworks, and based on a clear presumption of conformity to avoid duplicative cybersecurity assessments, audits, and documentation obligations across EU legislation.

Medical devices and in vitro diagnostic medical devices are already subject to comprehensive and stringent regulatory requirements under the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR). These frameworks establish lifecycle-based obligations covering risk management, design controls, post-market surveillance, and corrective actions, with cybersecurity increasingly embedded as an integral component of safety and performance. In parallel, recent horizontal digital legislation, notably the Cyber Resilience Act, introduces additional cybersecurity requirements applicable to products with digital elements, including certain health and medical technologies.

Against this backdrop, the revision of the Cybersecurity Act must carefully avoid introducing further layers of product-related obligations that overlap with, duplicate, or diverge from existing sectoral requirements. While MedTech Europe welcomes the objective of streamlining the European cybersecurity certification framework, including clearer timelines for certification scheme development and stronger coordination among authorities, cybersecurity certification should not come at the expense of already applicable product legislation or internationally recognised standards. In the current proposal, individual Member States retain the option to introduce national approaches that affect the application of cybersecurity certification schemes. We believe that it is essential that certification schemes remain voluntary and are not applied in a way that undermines regulatory harmonisation across the EU, including in connection with the NIS 2 Directive. Requiring manufacturers to demonstrate compliance multiple times against similar cybersecurity objectives, assessed under different legal acts and procedures, risks creating legal uncertainty, increasing administrative burdens, and placing additional pressure on already constrained conformity-assessment capacity.

For highly regulated products such as medical technologies, it is essential that cybersecurity certification frameworks align with existing regulatory requirements and do not create parallel compliance expectations in practice. Even where cybersecurity certification schemes are formally voluntary, the way they are referenced or relied upon within regulated healthcare environments may significantly shape deployment and use decisions.

Thus, the revised Cybersecurity Act should explicitly prioritise reliance on existing conformity assessment frameworks and international standards. Where equivalent levels of protection are pursued, compliance with relevant harmonised or international standards should give rise to a presumption of conformity under cybersecurity certification schemes, ensuring proportionality, legal coherence, and operational feasibility across the EU regulatory framework.

Without a clear presumption of conformity across legislative frameworks, European cybersecurity certification risks becoming an additional compliance requirement rather than a mechanism to reduce duplication. The revised Cybersecurity Act should therefore ensure that certification schemes are designed and implemented in a way that reduces duplication of cybersecurity assessments, audits, and documentation obligations where equivalent requirements already apply.

3. Ensure sector-specific competence of conformity assessment bodies for health-related cybersecurity schemes

Recommendation: Where cybersecurity certification schemes are applied to medical technologies, conformity assessment bodies should be required to demonstrate health-sector-specific expertise, and relevant evidence generated under MDR/IVDR conformity assessments should be reused wherever possible to ensure high-quality, coherent, and proportionate evaluations.

The proposed revision reinforces the role of conformity assessment bodies in the implementation of European cybersecurity certification schemes, including for products and services deployed in sensitive and safety-critical environments. MedTech Europe recognises the importance of credible and technically sound assessments in supporting trust in cybersecurity requirements, particularly where independent third-party evaluation is foreseen.

However, in the case of medical technologies, the quality and relevance of any cybersecurity-related assessment depend critically on the assessor's understanding of the healthcare context. Medical devices and in vitro diagnostic medical devices operate in clinical environments, interact directly with patients and healthcare professionals, and are subject to strict safety, performance, and post-market obligations under the MDR and IVDR. Assessing cybersecurity aspects without sufficient familiarity with clinical workflows, risk-benefit considerations, lifecycle management, and patient safety requirements risks leading to conclusions that are misaligned with clinical realities, inconsistent with sectoral regulation, or operationally unfeasible.

To ensure that cybersecurity assessments meaningfully contribute to safety and resilience in healthcare, conformity assessment bodies involved in health-related cybersecurity schemes should demonstrate appropriate sector-specific competence, including knowledge of medical device regulation and clinical risk management. In addition, assessment processes should explicitly allow for the reuse of relevant technical documentation, risk-management files, and post-market evidence already generated under MDR/IVDR conformity assessments. This approach would enhance assessment quality, reduce unnecessary duplication, support efficient use of assessment capacity, and ensure that cybersecurity requirements complement existing regulatory frameworks while prioritising patient safety and continuity of care.

4. Support international recognition of voluntary cybersecurity certification schemes to avoid supply-chain disruption

Recommendation: Where cybersecurity certification schemes are used on a voluntary basis, the revised Cybersecurity Act should prioritise international mutual recognition, particularly for components and services integrated into globally marketed medical technologies. Central EU-level publication and the progressive sunsetting of national schemes should be leveraged to reduce fragmentation and avoid duplicative assessments.

MedTech Europe welcomes the efforts to improve transparency and coherence in the EU cybersecurity certification landscape, including through centralised publication of European schemes and the reduction of overlapping national approaches. These measures can help limit internal market fragmentation and provide greater legal certainty for manufacturers operating across multiple Member States.

However, medical technologies rely on complex, globally integrated supply chains, including hardware components, software modules, and digital services that are developed, certified, and maintained across multiple jurisdictions. In the absence of international mutual recognition, certification requirements, even where formally voluntary, may in practice lead to duplicative testing, parallel assurance expectations, or

re-assessment of identical components or services. This can introduce inefficiencies, increase costs, and delay supply-chain operations, with potential knock-on effects on the availability, maintenance, or updating of medical technologies used in healthcare settings.

To mitigate these risks, the revised Cybersecurity Act should place greater emphasis on international cooperation and mutual recognition with trusted third countries, notably for cybersecurity assurances applicable to components and services used in globally marketed medical technologies. Recognising equivalent international certifications and standards would support supply-chain resilience, reduce unnecessary duplication, and help ensure that cybersecurity objectives are achieved without disrupting patient access to safe, effective, and secure medical technologies.

5. Strengthen structured stakeholder involvement in the development of cybersecurity certification schemes

Recommendation: While welcoming the establishment of the European Cybersecurity Certification Assembly as a strategic coordination forum, the revised Cybersecurity Act should ensure that it is complemented by a permanent expert-level mechanism enabling continuous and meaningful stakeholder input throughout the lifecycle of cybersecurity certification schemes.

The current proposal foresees the establishment of a European Cybersecurity Certification Assembly to facilitate dialogue on cybersecurity certification priorities and to support strategic exchanges among EU institutions, Member States, and stakeholders. MedTech Europe welcomes such initiatives that promote coordination and information-sharing across the EU and recognises the value of structured high-level discussions on emerging cybersecurity challenges and policy developments.

At the same time, a strategic forum such as the European Cybersecurity Certification Assembly, meeting on a limited basis, is not designed to support hands-on engagement in the technical development, implementation, and maintenance of cybersecurity certification schemes. Meaningful stakeholder input is particularly important to ensure that certification schemes are technically robust, aligned with existing regulatory frameworks, and workable in real-world deployment environments, notably for highly regulated and safety-critical sectors.

To enhance the quality, relevance, and effectiveness of cybersecurity certification schemes, MedTech Europe believes the governance framework would benefit from being complemented by a permanent expert-level mechanism to enable ongoing stakeholder engagement. A useful reference can be found in the Medical Device Coordination Group (MDCG), which has demonstrated the value of sustained expert collaboration in developing practical and coherent guidance. Establishing a comparable approach would help ensure that cybersecurity certification schemes benefit from sector-specific expertise, support regulatory coherence, and facilitate effective implementation across the EU.

Title IV: Security of ICT Supply Chains

6. Ensure scope clarity for medical technologies under the trusted ICT supply chain framework

Recommendation: The revised Cybersecurity Act shall ensure clear scope delineation for medical technologies by avoiding overlapping or conflicting requirements under the trusted ICT supply chain framework and by addressing non-technical supply chain risks in a proportionate manner that preserves regulatory coherence under the MDR and IVDR.

MedTech Europe supports the proposed distinction between technical cybersecurity risks, to be addressed through cybersecurity certification schemes, and non-technical security risks, to be addressed under the trusted ICT supply chain framework. A coordinated, European approach to structural non-technical risks to supply chain security is preferable to fragmented, national rules.

At the same time, the current proposal includes all sectors covered by the NIS 2 Directive, including manufacturers of medical devices, within the potential scope of measures under the trusted ICT supply chain framework. Medical technologies are regulated within a highly specialised and mature legal framework under the MDR/IVDR, which already establishes clear responsibilities, oversight mechanisms, and risk management obligations. In this context, the revised Cybersecurity Act should avoid introducing parallel or conflicting requirements for medical technologies that could blur regulatory responsibilities or lead to overlapping supervision.

Furthermore, by defining the scope of the trusted ICT supply chain framework through the NIS 2 Directive, any measures introduced under the proposed framework would be limited to EU legal entities. As a result, MDs and IVDs manufactured outside the EU by entities not subject to NIS 2, but placed on the EU market, would fall outside the scope of the framework. This may create an uneven playing field for EU-based manufacturers without necessarily improving overall supply chain security outcomes. Against this backdrop, the inclusion of medical device manufacturing, as listed in Annex II, 5 of the NIS 2 Directive, within the scope of the trusted ICT supply chain framework should be carefully reconsidered. Where relevant, non-technical risks linked to the procurement and use of medical technologies from high-risk suppliers could instead be addressed through proportionate obligations placed on healthcare providers who remain within the scope of NIS 2.

7. Safeguard patient safety and continuity of care in the context of supply-chain risk mitigation measures

Recommendation: Measures adopted under Title IV should be strictly technically grounded and risk-based, proportionate to both cybersecurity risk and clinical impact and designed with clear and transparent governance to safeguard patient safety and continuity of care. Where significant technical or operational adaptations are required, appropriate funding support should accompany implementation to enable effective mitigation without disrupting healthcare delivery.

Title IV of the proposed revision introduces a set of far-reaching measures to address cybersecurity risks linked to ICT supply chains, including potential restrictions, mitigation measures, and obligations related to high-risk suppliers. MedTech Europe recognises the rationale behind these provisions and supports the objective of strengthening the Union's resilience to supply-chain-related cybersecurity threats. However, when applied to medical technologies, such measures may have unintended consequences that go beyond economic or operational impacts and directly affect patient safety and the continuity of healthcare delivery.

Medical devices and in vitro diagnostic medical devices are often integral to diagnosis, treatment, monitoring, and life-sustaining care. Restrictions affecting components, software, updates, maintenance, or supplier relationships may impair device availability or performance, particularly in hospital environments where technologies are embedded in complex clinical workflows. Abrupt supply-chain measures or immediate withdrawal obligations, if not carefully calibrated, risk disrupting healthcare services, delaying treatments, or forcing the substitution of technologies without adequate clinical validation.

In this context, it is essential that any mitigation measures introduced under Title IV are strictly technically grounded and risk-based and applied through clear, transparent criteria and governance. Measures should be proportionate not only to the cybersecurity risk identified but also to the potential clinical impact, ensuring

that actions taken to address supply-chain risks do not inadvertently compromise patient safety or continuity of care.

Furthermore, the revised Cybersecurity Act should avoid the introduction of non-technical or geopolitical risk criteria that could lead to de facto origin-based restrictions, reduce legal certainty, or disrupt globally integrated healthcare supply chains without demonstrable cybersecurity benefit. Ensuring proportionality, predictability, and transparency in the design and application of supply-chain measures is essential to enable manufacturers and healthcare providers to plan and implement mitigation actions effectively.

Where compliance with supply-chain risk mitigation measures requires substantial technical or operational changes, appropriate funding support should be made available to affected entities. Such support could be provided, for example, through national and regional partnership plans under the next Multiannual Financial Framework, as part of broader investment in hospitals and in the implementation of the EU Action Plan on the cybersecurity of hospitals and healthcare providers.

Conclusion

The proposed revision of the Cybersecurity Act represents an important opportunity to strengthen the EU's cybersecurity framework in response to an evolving threat landscape, including in the healthcare sector. For medical technologies, cybersecurity is closely linked to patient safety, continuity of care, and trust in digital health solutions. MedTech Europe supports the overarching objective of enhancing EU-level coordination and resilience, including through ENISA's role, and underlines the importance of a risk-based and proportionate approach that takes into account the specificities of highly regulated sectors such as medical technologies.

MedTech Europe and its members stand ready to continue engaging constructively with EU policymakers to support the development of a coherent, workable, and patient-centred cybersecurity framework for Europe.

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 that research, develop, manufacture, distribute and supply health-related technologies, services and solutions.
www.medtecheurope.org.

For more information, please contact:
Alexander Olbrechts
Director Digital Health & Medtech Value
a.olbrechts@medtecheurope.org