Position Paper: Medical Technology Industry Perspectives on Digital Legislation in the Netherlands

Executive Summary

Europe's medical technology sector plays a critical role in delivering safe, innovative, and increasingly digital healthcare solutions to patients. However, the sector is currently confronted with a rapidly expanding set of horizontal digital regulations—including the Artificial Intelligence Act (AI Act), cybersecurity legislation, and the Data Act—layered on top of existing, highly developed sectoral frameworks such as the Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR). This risks creating duplicative obligations, legal uncertainty, and unpredictable compliance timelines for medical technology manufacturers. Without careful alignment, this fragmented regulatory environment may delay patient access to innovative technologies, increase compliance costs, and undermine Europe's global competitiveness.

The European Commission's Digital Omnibus initiative represents an important opportunity to simplify and streamline the EU's digital regulatory framework. The Dutch government has also expressed support for reducing unnecessary regulatory burden while safeguarding public interests. NEFEMED welcomes these efforts to simplify the regulatory landscape and call on policymakers to ensure that horizontal digital legislation is fully coherent with MDR and IVDR.

NEFEMED calls on policymakers to ensure that:

1) AI Act requirements for medical devices are coherently integrated into existing MDR/IVDR conformity assessment pathways;
2) Cybersecurity obligations are implemented through harmonized reporting mechanisms that avoid parallel or duplicative requirements; and
3) Data sharing obligations under the Data Act remain voluntary for medical technologies and aligned with sector-specific health data legislation.

These measures are essential to deliver genuine simplification while safeguarding patient safety, innovation, and legal certainty.

Digital legislation should complement, rather than duplicate or contradict, the existing medical device regulatory framework. A coherent, streamlined digital regulatory environment is essential to safeguard innovation, competitiveness, and timely patient access to medical technologies across the Netherlands and the EU.

1. Introduction

Digitalization is transforming healthcare delivery across the EU, with medical technologies at the center of this shift. Medical technology—including connected devices, software as a medical

device (SaMD), and AI-enabled diagnostics and decision-support tools—has become an integral part of modern healthcare systems. These technologies support earlier diagnosis, personalized treatment, and more efficient healthcare delivery, contributing directly to patient outcomes and system sustainability. Ultimately, they contribute to improved patient outcomes and more efficient, resilient healthcare system in the Netherlands as well as the EU.

The medical technology sector already operates under the MDR and IVDR, a comprehensive regulatory framework, which sets high standards for product safety and performance. These regulations are specifically designed to address the risks and benefits associated with medical technologies, including digital and software-based products.

In parallel, the EU has adopted a series of horizontal digital legislation—such as the AI Act, cybersecurity rules and the Data Act—intended to address cross-cutting digital risks across sectors, including medical devices. While these initiatives pursue legitimate policy objectives, insufficient alignment with the existing MDR/IVDR framework risks creating overlapping requirements and legal uncertainty for manufacturers.

In this context, the European Commission has published the Digital Omnibus Package proposal on 19th of November 2025, aiming to simplify the EU's complex digital legislative landscape by addressing overlapping and fragmented compliance requirements. The package includes targeted amendments to several cornerstone digital laws that have a direct impact on businesses operating in Europe, including GDPR, AI Act, the Data Act, and rules governing cybersecurity. Collectively, these initiatives aim to reduce administrative burdens, streamline compliance, and foster innovation while maintaining effective regulatory oversight.

The Netherlands Cabinet has shown its support for the principle of omnibus proposals as a means of reducing regulatory burdens, streamlining legislation and improving feasibility. The Cabinet has also stressed the importance of analyzing the cumulative effects of digital legislation while improving the consistency and coherence of legislation without compromising the protection of fundamental rights.

NEFEMED welcomes initiatives at the EU and national level that seek to streamline and simplify digital regulation and urges policymakers to ensure that horizontal digital legislation remains fully coherent with MDR and IVDR. Digital regulations must complement, not duplicate or contradict, the existing MDR/IVDR framework. To fully realize the benefits of digital medical technologies both in the EU and the Netherlands, the regulatory environment must support digital innovation through legal certainty, predictability and proportionate requirements. Fragmentation risks delaying access to vital technologies, reducing predictability, and undermining Europe's attractiveness for innovation and investment.

2. Artificial Intelligence (AI) Act

AI-enabled medical technologies have long been regulated under the EU MDR and IVDR, which apply to all medical technologies, including software irrespective of whether they use AI/ML techniques or traditional algorithms. While the AI Act was introduced with the goal of ensuring legal certainty for AI development and use in Europe, early implementation challenges have exposed the limits of applying horizontal rules to well-established sectoral frameworks without

sufficient integration mechanisms. New requirements related to AI-enabled medical technologies should build and complement existing frameworks for medical technologies, through targeted adaptation and ongoing dialogue between EU policy makers, regulators and manufacturers. The Artificial Intelligence Digital Omnibus represents an important and timely update to support the effective implementation of the AI Act.

In this context, NEFEMED welcomes the Commission's proposal to pause the application of high-risk AI obligations until key implementation prerequisites are in place, including the availability of harmonized standards and sufficient notified body capacity. Applying obligations before these foundational elements are operational would create legal uncertainty and uneven implementation across Member States. The timing of application should be strictly contingent upon notified bodies' readiness, completion of harmonized standards, and the system being declared formally ready by the European Commission.

At the same time, NEFEMED emphasizes the importance of ensuring a clear and predictable integration of AI Act requirements into the MDR/IVDR framework for AI-enabled medical devices. NEFEMED supports the application of high-risk AI requirements to medical devices, provided these requirements are operationalized through existing MDR/IVDR conformity-assessment mechanisms, rather than creating parallel compliance layers under the AI Act. This allows manufacturers to rely on a single, integrated conformity-assessment pathway for AI-enabled medical devices. Alignment should be limited to the horizontal requirements applicable to high-risk AI systems, as set out in Chapter III, Section 2 of the AI Act, and integrated in a way that ensures consistency with the MDR's general safety and performance requirements, avoids duplication, and preserves the integrity of existing conformity assessment procedures. As a key simplification measure, NEFEMED calls on the European Commission to formally map Chapter III, Section 2 requirements of the AI Act to existing MDR/IVDR obligations, including Annex I General Safety and Performance Requirements, Quality Management System elements, post-market surveillance and cybersecurity documentation. This would provide legal clarity, ensure predictability of requirements, and enable a single, integrated conformity assessment pathway for AI-enabled medical devices. This approach provides predictability of requirements and safeguards legal certainty and reflects the risk-based lifecycle oversight already embedded in the MDR/IVDR.

Finally, clarity and alignment of key definitions are essential. Concepts such as "substantial modification" and "significant change" are central to both the AI Act and MDR/IVDR. The definitions for these concepts must be aligned across laws to avoid parallel interpretations and reduce uncertainty. Clear, aligned guidance is needed on "substantial modification", ensuring that change-control processes for adaptive or continuously learning AI systems follow one predictable and coherent regulatory pathway under MDR/IVDR, rather than parallel regimes under the AI Act.

3. Cybersecurity

Cybersecurity is a critical component of patient safety and system resilience, particularly for connected and networked medical technologies. NEFEMED supports strong, consistent cybersecurity requirements across the EU but stresses the importance of harmonized implementation across the Member States to avoid internal market fragmentation.

In the Netherlands, national transposition of EU cybersecurity legislation—such as the Cyberbeveiligingswet under Network and Information Security Directive II (NIS2)—should be closely aligned with other Member States to ensure a level playing field. Divergent national interpretations risk increasing compliance complexity for manufacturers operating across borders and could place Dutch based companies at a competitive disadvantage within the internal market. Increased harmonization of national transpositions and reporting obligations under the NIS2 and the Cybersecurity Act is essential to prevent further fragmentation of the internal market and to ensure that critical medical technologies remain safe, interoperable and accessible across the EU. As industry, we support the objectives of the Cyberbeveiligingswet of strengthening cybersecurity in healthcare, while recommending targeted refinements to ensure the framework remains workable and proportionate in practice.

With respect to the scope of the Cyberbeveiligingswet, we encourage a clear distinction between healthcare organizations and medical technology manufacturers to ensure proportionality. Hospitals face immediate patient-safety risks from even short outages, while manufacturers can often mitigate short-term disruption through inventory buffers and continuity planning.

We further recommend a flexible, context-based approach to incident reporting that allows for contextual assessment and consideration of the activity and impact on the entity and natural persons. Furthermore, we call for a risk-based framework that considers:

(1) the nature of the service being affected (e.g., direct patient care versus manufacturing).

(2) the criticality of the specific system or process,

(3) mitigation measures already in place that can reduce the significance of the incident, and

(4) actual harm to persons and degree of disruption to business operations.

NEFEMED recommends that implementation of the Cyberbeveiligingswet be supported by clear and timely guidance on registration obligations and compliance timelines to minimize uncertainty and avoid unnecessary costs. We further advocate a phased rollout that recognizes ongoing NIS2-related program improvements and allows organizations to prioritize the most critical measures first. Finally, early and structured stakeholder engagement is essential to ensure requirements are practicable, consistently interpreted, and effectively adopted across the sector.

NEFEMED welcomes the commitment, as reflected in the Digital Omnibus, to establish a single-entry point for cybersecurity incident reporting via ENISA. This approach represents a significant step towards reducing administrative burden and fragmentation. At the same time, incidents that have direct patient safety implications and qualify as MDR vigilance events should continue to be reported through established medical device vigilance pathways.

Clear delineation between cybersecurity reporting and MDR vigilance is essential as it preserves patient safety oversight while avoiding duplicative reporting and legal uncertainty. In contrast, routing cybersecurity notifications through EUDAMED, as envisaged in the MDR/IVDR review, would risk reintroducing fragmentation. If EUDAMED is to maintain any involvement in

cybersecurity-related notifications, it is essential that robust interoperability and data exchange protocols are established between systems. This will support a genuine "no wrong door" policy, avoiding inconsistent or duplicate reporting. As a result, public-facing data will remain reliable for stakeholders such as health institutions, and manufacturers' security professionals will have access to a unified and harmonized process for reporting vulnerabilities—applicable across MDR/IVDR as well as non-MDR/IVDR contexts, should they choose to do so.

4. Data Act

The Data Act introduces horizontal rules on data access and sharing that may affect medical technology manufacturers. From an industry perspective, it is essential to confirm that data-sharing obligations under the Data Act remain voluntary for the medical technology sector.

Health-related data is already subject to strict sector-specific rules, including data protection legislation and, in the future, the European Health Data Space (EHDS). The EHDS should remain the primary and tailored framework governing access to and use of health data, reflecting the sensitivity of such data and the specific safeguards required.

Applying mandatory data-sharing obligations under the Data Act to medical technologies risks creating legal uncertainty, undermining investment incentives, and conflicting with existing health data governance frameworks. For example, mandatory disclosure of device-generated data could expose validated algorithm parameters, cybersecurity architectures or safety-critical performance characteristics, thereby undermining safeguards assessed and approved under MDR/IVDR and potentially impacting patient safety.

NEFEMED supports the proposed reinforcement of trade secret protections under the Data Act, allowing refusal of data sharing where there is a high risk of unlawful disclosure to third countries.

NEFEMED would like to see this protection reinforced further. As such, NEFEMED recommends that trade secrets be recognized as a legitimate ground to withhold data access where disclosure could lead to the loss of valuable proprietary know-how. This recognition would provide data holders with the necessary legal certainty to safeguard innovation.

It is also essential that data holders can limit access to data when sharing as it could undermine product performance, compromise security, or jeopardize patient safety. These safeguards are particularly critical in the context of medical technologies, where the integrity and safety of products directly impact patient outcomes.

5. Conclusion

Digital technologies are transforming healthcare, and NEFEMED welcomes the commitment of the European Commission and the Netherlands national authorities to simplifying digital legislation through the Digital Omnibus. However, without careful clarification and alignment, horizontal digital legislation risks creating legal and operational uncertainty, delaying access to innovative medical technologies, and weakening Europe's innovation ecosystem.

NEFEMED therefore calls on policymakers to:

- Ensure full coherence between horizontal digital legislation and MDR/IVDR;
- Avoid parallel conformity assessment, reporting, or enforcement mechanisms for medical technologies;
- Engage early and systematically with notified bodies and industry during implementation; and,
- Ensure that national implementation choices, including in the Netherlands, support regulatory predictability and a level playing field.

A digital policy environment that is aligned with existing medical device legislation, proportionate to risk, and tailored to the realities of medical technology development is essential to safeguard innovation, ensure timely patient access, and preserve innovation and competitiveness in the Netherlands and across Europe.

NEFEMED stands ready to engage with Dutch and EU authorities to support practical, risk-based implementation of digital legislation that reinforces patient safety while enabling innovation in medical technologies.