The European Association of
Medical devices Notified Bodies

TEAM-NB A.I.S.B.L.
Rue Bawepuce, 20
B – 4140 Sprimont BELGIQUE
Tel.: +32 475 85 40 45

E-mail: schlemmer@team-nb.org
Web: http://www.team-nb.org
Bank : IBAN BE09 3401 5174 8757
VAT : BE 0864.640.677 - RPM Liège

February 5th, 2026

Subject : Team-NB Letter on cybersecurity in medical devices

To whom it may concern,

We as notified bodies appreciate the efforts to increase cybersecurity of medical devices in Europe for the benefit of patients. And we'd like to reiterate our willingness to collaboratively contribute to such efforts. Particularly, we welcome the proposed changes in MDR/IVDR that close an oversight gap in cybersecurity matters by involving ENISA (proposed MDR Art. 87a) and increase clarity of GSPRs with that regard (proposed MDR, Annex I, 17.4). However, it must be ensured that decisions concerning availability of medical devices and safety of patients remain with governance bodies established and defined by MDR/IVDR while ENISA gains full oversight of cybersecurity incidents and activities to support cybersecurity across sectors.
Similarly, we acknowledge the need for revised regulatory guidance and standards, as stated by the draft report of the MDCGs Cybersecurity task-force lead and initiated by Poland in 2025. Particularly, we see MDCG 2019-16 Rev. 1 ('Guidance on Cybersecurity for medical devices') would benefit from an update. Additionally, we expect development of a harmonised standard on medical device cybersecurity would substantially simplify compliance in these matters; such a standard would allow for presumption of conformity with our regulatory framework and make compliance more feasible for all players, especially small and medium-sized enterprises (SMEs) in MedTech. Concrete, we believe IEC 81001-5-1 on 'Health software and health IT systems safety, effectiveness and security' would offer itself as basis for harmonisation. We'd like to offer our full support for any activities to adequately reflect the state-of-the-art in cybersecurity in up-to-date guidance and standards.

Yet, we are concerned about intentions to include more granular cybersecurity requirements in MDR and IVDR. As part of the New Legislative Framework (NLF), both regulations are designed to adapt to innovation and changes of their environment by means of (harmonised) standards, common specifications and regulatory guidance. Technical provisions anchored in 'hard' law hinder and prevent innovation as has been illustrated previously (e.g. EU directives on blood, cell and tissues stopping innovation in that field to some extent). Guidance and standards allow deviation when adequately justified, for example in case of superior or more fitting solutions for distinct use cases. Nevertheless, they increase harmonisation between

different member states, notified bodies and developers of medical device software (MDSW). We fear inflexible legal rules on cybersecurity (and any other technical or scientific matter) will effectively decrease availability of innovative medical devices to European patients without increasing or worse, even hindering, cybersecurity.
Likewise, an extension of the framework provided by the Cyber Resilience Act (CRA) to cover medical devices would – if at all – improve cybersecurity only incrementally while administrative burden would increase disproportionately. Such an additional overlap of governance in the area of medical device software (MDR/IVDR ***&*** AIA ***&*** CRA) is very likely to cause SMEs to further reduce their involvement in the European market and thus reduce competition between manufacturers and availability of medical devices for patients and practitioners. We consider an exchange and crosstalk between regulatory frameworks as proposed by the European Commission in their draft revision of MDR and IVDR (see above) a more practicable and yet satisfactory solution.

Further, we'd like to emphasise that state-of-the-art (SOTA) is by no means a vague or imprecise benchmark while we appreciate this could be the impression to persons not familiar with regulatory compliance of medical devices. SOTA is anchored in the Union's 'Blue Guide' (e.g. section 4.1.2.5) and, consequentially, fundamental to European product regulations under the NLF, incl. MDR and IVDR. It reflects current technical capabilities or clinical practice and is based on consolidated insights from science, technology and practical considerations. This principle was chosen for regulation of medical devices, because its capability to adapt to innovation cycles without regulation falling significantly behind. Cybersecurity means the never-ending competition of defenders with external attackers. Like all such highly competitive environments, this results in very dynamic innovation cycles. Consequently, SOTA as principle might be even more important for cybersecurity than in other less dynamic fields (e.g. clinical practice) because cybersecurity can never be a compliance exercise of simply fulfilling requirements but must be conceived and implemented as a process.
This thought leads to another critical aspect of cybersecurity lying entirely out of reach of regulatory affairs: The (cybersecurity) threat landscape we currently experience is to a good proportion created by nation states attacking and harming infrastructure in other, competing regions. Due to the unlimited resources of such players in comparison to any private or corporate entity, it must also be nation states *actively* defending against these. Passive defensive activities alone as foreseen in cybersecurity cannot succeed in such a competition and must be complemented by coordinated action throughout our Union.

To summarise, we welcome revision and further development of the European cybersecurity framework for medical devices based on guidance and (harmonised) standards and caution against granular technical requirements in our regulations that will be outdated faster than any legislator may update them. The principle of state-of-the-art should remain the guiding principle for this as for all other aspects of development and compliance of medical devices. We deem adjustments as proposed by the Commission in their draft revision of MDR and IVDR sufficient to enable crosstalk between the regulatory frameworks for general cybersecurity and medical devices.

We offer to support and participate in all related activities aimed to improve cybersecurity of medical devices in Europe with our practical experience and expertise.

Hoping for your consideration,

Françoise Schlemmer
Director
Team-NB
Tel +32 475 85 40 45
Web www.team-nb.org

Team-NB, The European Association of Medical Device Notified Bodies, was founded in 2001 and represents 44 members from 20 different countries. We promote high standards and work to harmonise practices among Notified Bodies.