MEDTECH INSIGHT
CITELINE COMMERCIAL

31 Jan 2024 | **News**

# Cybersecurity Update: NIS2 Directive, Cyber Resilience Act And Cyber Solidarity Act

by Natasha Barrow

Healthcare digitalization opens the industry up to cyber-attack, the EU Cybersecurity Strategy aims to combat this. However, further work is needed to address interplay between cybersecurity legislation and the MDR, says academic expert.

The European cybersecurity policy framework is quickly evolving under the EU Cybersecurity Strategy, with the introduction of vertical legislation such as the NIS2 Directive on cybersecurity, the proposed Cyber Resilience Act, and the proposed Cyber Solidarity Act.

*MedTech Insight* spoke to academic expert Elisabetta Biasin, cybersecurity doctoral researcher at KU Leuven, and Pilar Arzuaga, senior associate at McDermott Will & Emery, to get the update on the EU's cybersecurity framework and how this interacts with sector-specific cybersecurity under the MDR and IVDR.

Cybersecurity of medical devices is regulated both by vertical cybersecurity legislation that operates across all sectors, and by sector-specific cybersecurity-related requirements, horizontal regulations, and guidance under the MDR and IVDR.

While the MDR does not explicitly refer to "cybersecurity," it calls for the "appropriate means to be adopted to reduce risks or impairment of the performance."

Therefore, the MDR and IVDR is supplemented by the *Medical Device Coordination Group 2019-16 Guidance (MDGC) on Cybersecurity for medical devices*, to provide guidance on how to fulfil all the relevant essential requirements with regards to cybersecurity.

## *More Guidance Needed To Understand When MDR Prevails Over NIS2 Directive*

In one important step, the NIS2 proposal stated sector-specific rules should take priority if the overlapping requirements "are at least equivalent in effect to the obligations laid down" in the new directive. (Also see "*Cybersecurity In The EU: How Overlapping Regulations Could Harm Medtech*" - Medtech Insight, 7 Oct, 2022.)

But that's not enough, Biasin said. "Medtech would surely benefit from further indications by MDCG to understand whether and when the MDR prevails over the NIS2," Biasin noted, adding that NIS2 provides another opportunity for further medical device cybersecurity guidance. For example, the document could address the topic of incident notifications and other practical questions in more detail.

*NIS2 Directive entered into force January 16, 2023*. Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October.

The NIS2's approved text added further clarifications to the former proposal text for EU sector-specific texts, said Biasin. It added a specific article to suggest when specific law should prevail, but also defined "at least equivalent.", to detail that sector-specific requirements should correspond or go beyond the requirements of the NIS2 Directive, with the understanding that sector-specific provision may be more granular in detail.

## *Medical Devices Could Be Included In Cyber Resilience Act*

The proposed Cyber Resilience Act (CRA) specifically excluded certain digital products and services subject to sectoral legislation, including medical devices. (Also see "*Cybersecurity In The EU: How Overlapping Regulations Could Harm Medtech*" - Medtech Insight, 7 Oct, 2022.)

Yet, Biasin noted, the European Data Protection Supervisor, who monitor and assure European institutions respect the right to data protection and privacy, *released an opinion* suggesting that medical devices should be included.

It remains to be seen whether the latest version of the proposals, agreed in December 2023, has considered this recommendation.

The CRA sets out a range of obligations for manufacturers and importers of "product with digital elements," including hardware and software.

The final text has not yet been published, but the regulation is expected to come into force early this year. After this, manufacturers will have 36 months to apply the rules.

## *Uncertain Impact Under Cyber Solidarity Act*

The proposed Cyber Solidarity Act creates a regulatory framework for the detection, preparation, and response to cybersecurity threats. Including methods such as the *European Cybersecurity Shield and Cyber Emergency Mechanism*.

As the Cyber Solidarity Act is still in the proposal stages, it is difficult to ascertain its impact. It could have impact on entities operating in the healthcare industry. However, in contrast to the NIS directive, the act does not clearly delineate which organizations are within its scope, Arzuaga told *Medtech Insight*.

## *NIS2 Background*

The NIS2 Directive replaces the original NIS Directive and expands its scope. Its principal aim is to create a high common level of cybersecurity across the EU. Further, it intends to harmonize cybersecurity requirements in the European Union to strengthen security against cyberattacks.

The NIS Directive concerns the security of network and information systems, creating a point of distinction with the General Data Protection Regulation, which concerns personal data.

As reported by *Medtech Insight*, medical device companies are not directly included within the scope of the NIS Directive however they are "tangentially touched." (Also see "*Cybersecurity In The EU: How Overlapping Regulations Could Harm Medtech*" - Medtech Insight, 7 Oct, 2022.)

Under the NIS2 Directive, medical device companies are considered "essential entities" or "important entities."

Essential entities cover sectors including healthcare and energy, while important entities cover sectors including digital providers and manufacturers of critical products. Both are obligated to follow notification requirements for reporting of security incidents.