New guidance document on cybersecurity for medical devices

Article by Miriam Schuh and Jennifer Thielen

The "Guidance on Cybersecurity for medical devices," published in December 2019 by the MDCG, is designed to serve as an aid for medical devices manufacturers in complying with cybersecurity-specific requirements, particularly those found in Annex I of (new) Regulations (EU) 2017/745 (the MDR) and (EU) 2017/746 (the IVDR).

For the most part, the guidance document presents basic concepts in cybersecurity and makes clear that cybersecurity must be regarded as part of the fundamental requirements for the general safety and effectiveness of medical devices. Accordingly, the document makes reference to the regulatory requirements of the MDR and IVDR which are of relevance for medical devices manufacturers while at the same time offering hints for the implementation of aspects relating to cybersecurity.

The guidance document states that general IT security is of central importance for all aspects of cybersecurity and that it is to be assessed depending on the product's risk, intended use and operating environment. It also notes that the goals of product safety, security and effectiveness are to be kept in mind at all times when designing security mechanisms for medical devices and in-vitro diagnostics.

A significant part of cybersecurity is risk prevention. What this means for medical device manufacturers is that security mechanisms have to be implemented in the product's development phase, and not only in the manufacturing process. Such mechanisms include, above all:

- secure design,
- a security risk management system,
- security capabilities,
- a standardized security risk assessment,
- a security benefit risk analysis,
- minimum IT requirements, and
- validation and verification throughout the product life cycle.

The guidance document also points out that cybersecurity aspects may be of relevance for documentation and in drafting instructions for use. Product documentation must include e.g. security requirements to ensure safety and product effectiveness: this includes cybersecurity! In addition, the instructions for use which are provided with medical devices must include information relating specifically to cybersecurity, such as information relating to product installation or step-by-step instructions for deploying security updates. The specific shape which these requirements take in each case depends on the security risk, the operating environment and the specific product.

In addition to prevention and documentation requirements, medical device manufacturers also have to satisfy post-market surveillance requirements, including continuous monitoring and remediation of cybersecurity vulnerabilities.

The specific (cybersecurity) requirements for each medical device and manufacturer depend on the specific situation in each case, particularly the product's intended use, reasonably foreseeable misuse and operating environment. For this reason, the guidance document notes that manufacturers should include cybersecurity questions in their risk assessments from the very beginning, in other words from the development phase, and should continue to do so throughout the product's life cycle.

As medical devices become increasingly digitized and connected, this guidance document illustrates to manufacturers once again and with particular urgency that cybersecurity is an essential part of product safety and one that may not be neglected at any point during the product's life cycle if the product is to comply with regulations.

Company contact: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E > melanie.schaumann@reuschlaw.de