Product Service

Add value.
Inspire trust.

Med-Info

International expert information
for the medical device industry

Cybersecurity for medical devices

Background

The steadily increasing number of cyberattacks affect more and more often also medical devices, which consequently leads to a growing importance of cybersecurity in the medical device field.

There are many definitions of the term cybersecurity. They usually revolve around the protection of assets from attacks or the managing of risks associated with information technology. No matter what definition you look at, a key concept in cybersecurity is the so-called CIA triad:

- Confidentiality (protection of private data from unauthorised access)
- Integrity (protection of data from unauthorised change)
- Availability (ability to access data when needed)

This Med-Info focuses on the requirements applicable to medical device manufacturers when demonstrating the confidentiality, integrity and availability of data involved with the medical device.

When is cybersecurity applicable to a medical device?

Cybersecurity is applicable for medical devices as soon as either application security (focus on patient safety) or data security (focus on data privacy) becomes relevant.

Application security is relevant if

- the device could be accessed by unauthorised persons (remotely or locally).
- the manipulation of program code, configuration data, parameters, etc.
- could result in patient injury.

Data security is relevant if

- the device could be accessed by unauthorised persons (remotely or locally)
- and the device handles information assets (e.g. personally identifiable health information).

Why medical device manufacturers need to address cybersecurity

Apart from the obvious benefits of protecting one's assets, there are also legal requirements for manufacturers to address cybersecurity. The MDR includes several clauses which address security, e.g.:

- **Annex I, chapter II, item 17.2:** 'For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.'

- **Annex I, chapter II, item 17.4:** 'Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.'
- **Annex I, chapter II, item 18.8:** 'Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended.'

There are other legislations aside from the MDR which require cybersecurity measures, e.g. the Regulation (EU) 2016/678 (General Data Protection Regulation). A failure to meet the data protection requirements of this regulation can lead to high penalties.

What does this mean for you as a medical device manufacturer?

Since cybersecurity is mandatory for medical device manufacturers at least since the introduction of the MDR, the topic will be addressed in more detail during audits, technical documentation assessments and product testing.

Medical device manufacturers should therefore be able to answer the following questions:

- Is there a systematic process for cybersecurity risk management?
- Are cybersecurity risks considered? (confidentiality, integrity including safety, availability)
- Are adequate measures defined?
- Have they been verified?
- Are relevant sources regarding cybersecurity vulnerabilities and threats observed?

How TÜV SÜD Product Service can support you

TÜV SÜD Product Service and its partners offer a variety of assessment and training services for cybersecurity:

- Concept assessment early in the development phase (based on applicable regulations and/or standards including IEC 62443-4-2 and UL 2900-2-1)
- Vulnerability scans conducted by our service partners
- Cybersecurity assessment based on IEC 62443-4-2 or UL 2900-2-1 including in-depth vulnerability scans and penetration tests based on OWASP IoT
- Training by the TÜV SÜD Akademie

Your contact partner at TÜV SÜD Product Service can provide further information.

Dr. Andreas Purde
Phone: +49 89 5008-4203
Email: andreas.purde@tuev-sued.de

Olaf Teichert
Phone: +49 89 5008-4156
Email: olaf.teichert@tuev-sued.de

TÜV SÜD Product Service GmbH, Medical and Health Services, Ridlerstr. 65, 80339 Munich
www.tuev-sued.com/medinfo

2019 © TÜV SÜD Product Service GmbH | PS-MKG/MHS/medinfo/1.5/en/DE