PROREGIA

Digitalization and Cybersecurity

QUAREGIA

Quality & Regulatory Compliance

Digitalization and Cybersecurity in Lifescience Quality & Regulatory

QUAREGIA and PROREGIA, SMT 23.03.2021

QUAREGIA GmbH & PROREGIA AG

QUAREGIA GmbH, Qualitymanagement and Regulatory Affairs Services for Medical Devices, In Vitro Diagnostic Devices, Combination Products, Medical Device Software, Cybersecurity, Artificial Intelligence.

Web: www.quaregia.com, Phone: +41 76 741 61 62

PROREGIA AG, Protect Your Digital Territory, Digitalization Services, Cybersecurity Concepts, End-2-End Secure Platforms, Cybersecurity Verification and Validation, Cybersecurity Post-Market Surveillance, Artificial Intelligence, Interoperability Concepts- and Solutions

Web: www.proregia.com, Phone: +41 44 586 24 00

Cybersecurity Regulations and Guidelines (non exhaustive list)

QUAREGIA
Quality & Regulatory Compliance

- **Europe: GDPR, MDD/AIMDD/MDR, IVDD/IVDR (MDR: 10 hits for “security” related to IT/Software, MDD: 0 hits, IVDR: 5 hits for “security” related to IT/Software, IVDD: 1 hit for “security”**
- **USA: 21 CFR Part 820, FDA Cybersecurity Guidelines, HIPAA**
- **Health Canada Cybersecurity Guideline**
- **Australian Government – Department of Health – Therapeutic Goods Administration, Cybersecurity Guidelines**

GDPR: General Data Protection Regulation, MDD: Medical Device Directive, AIMDD: Active Implantable Medical Device Directive, MDR: Medical Device Regulation, IVDD: In-vitro Diagnostic Device Directive, IVDR: In-vitro Diagnostic Device Regulation, FDA: Food and Drug Administration, CFR: Code Federal Regulations, HIPAA: Health Insurance Portability and Accountability Act

§

QUAREGIA
Quality & Regulatory Compliance

- **Example MDR, Annex I: General safety and performance requirements:**
  - 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.

- **Example MDR, Annex I, Chapter II, Section 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.

In order to be compliant with regulations and guidelines, not only a safety concept but also a security concept must be established for medical device software.

Cybersecurity Guidelines (USA)

QUAREGIA
Quality & Regulatory Compliance

USA (FDA):

- **Content of premarket submissions for management of cybersecurity in medical devices, Draft guidance V2.0 (update of 2014 version) – consultation from Oct. 2018 until March 18th 2019, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf**

Postmarket Management of Cybersecurity in Medical Devices, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

- **Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM077823.pdf**

Cybersecurity Guidelines (Canada, Australia) (non exhaustive list)

QUAREGIA
Quality & Regulatory Compliance

Government of Canada, Health Canada:

- **Pre-market requirements for medical device cybersecurity, Draft guidance V1.0 – consultation from Dec. 2018 until Feb. 5th 2019, https://www.canada.ca/en/health-canada/services/drugs-health-products/public-involvement-consultations/medical-devices/consutation-premarket-cybersecurity-profile/draft-guidance-premarket-cybersecurity.html**

Australian Government, Department of Health:

- **Medical device cybersecurity, Draft guidance V1.0 – consultation from Dec. 2018 until Feb. 14th 2019, https://www.tga.gov.au/sites/default/files/consultation-medical-device-cyber-security.pdf**

Cybersecurity Standards and Guidelines (EU, USA, CAN, AUS, non exhaustive list)

QUAREGIA
Quality & Regulatory Compliance

Standard	Scope
ISO 14971	Medical devices - Application of risk management to medical devices
ISO 13485	Medical devices - Quality management systems
IEC 62304	Medical devices - Software lifecycle requirements
IEC 60601-1	Safety and essential performance of medical electrical equipment
IEC TR 60601-4-5	Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications
IEC 82304	Health software - Part 1: General requirements for product safety
IEC 80001 series	Application of risk management for IT-networks incorporating medical devices
IEC 80002 series	Medical device software standards (guidance on the application of ISO 14971 to medical device software)
AAMI TIR57	Principles for medical device security - Risk management.
IEC 62443 series	Security for industrial automation and control systems
UL 2900-1	Software Cybersecurity for Network-Connectable Products - Part 1: General Requirements
UL 2900-2-1	Software Cybersecurity for Network-Connectable Products - Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems
NIST Framework	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 – April 2018, https://nist.gov/cyberframework/framework
ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure
ISO/IEC 30111	Information technology - Security techniques - Vulnerability handling processes
MDCG 2019-16	Guidance on Cybersecurity for medical devices

Cybersecurity Standards, Guidelines, etc.

QUAREGIA

Quality & Regulatory Compliance

There are hundreds of standards and guidelines out there, some are better and more helpful than others….

However, no matter what, in order to get cybersecurity control and be compliant with whatever standards and guidelines - companies must define security concepts and in there develop threat models that consider attacks from outside the organization as well as from inside the organization

Copyright Information

PROREGIA
Digitalization and Cybersecurity

QUAREGIA
Quality & Regulatory Compliance

QUAREGIA GmbH & PROREGIA AG
Kirchbannstrasse 18
4703 Kestenholz
Switzerland

www.quaregia.com / www.proregia.com
info@quaregia.com / office@proregia.ch
+41 76 741 61 62 / +41 76 586 24 00