DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

KMDIA Virtual Seminar

Advancement of Global Medical Device Regulation: Cybersecurity

An update on International Standards

Ben Kokx

Chair of COCIR Cybersecurity FG

Thursday 29, July 2021

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA Medical Imaging & Technology Alliance · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · KMDIA Korea Medical Devices Industry Association · ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Cybersecurity standards

Security requirements must be:

- balanced against safety and performance;
- fit the intended use and intended operating environment
- fit for the technologies used;
- address the entire life-cycle;
- be applied in all environments, e.g. the manufacturers development, manufacturing and enterprise as well in the end-user's infrastructure;
- Applied to people, products, services & organizations.

As a result, we have many different security standards developed by different TC's for specific purposes

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Recently published security related healthcare specific standards

- **IEC/TR 60601-4-5 (:2021-01) - 1st edition**
  Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices
- **ISO/TR 11633-2 (:2021-02) – 2nd edition**
  Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 2: Implementation of an information security management system (ISMS)
- **ISO/TR 21332 (:2021-03) – 1st edition**
  Health informatics — Cloud computing considerations for the security and privacy of health information systems
- **ISO 81001-1 (:2021-03) - 1st edition**
  Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

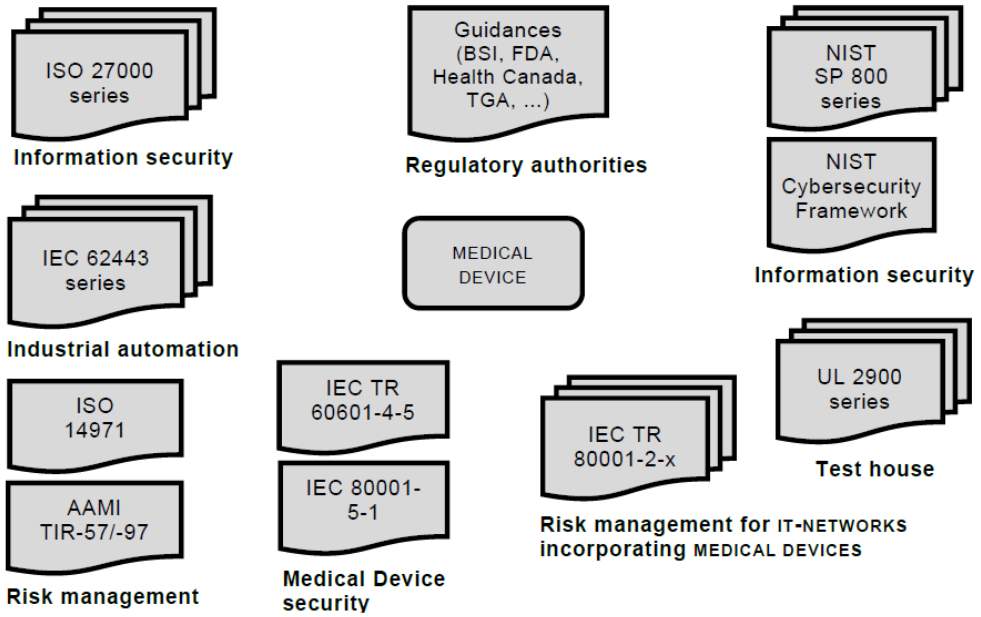
Focus on IEC/TR 60601-4-5

Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

➔ Application of IEC 62443-4-2 (Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components) for medical devices

906 **A.4 Correlation to existing regulations, standards and technical specifications**

907 The sheer number of cybersecurity frameworks, standards and guidance documents may seem
908 overwhelming to the MEDICAL DEVICE MANUFACTURER. The following illustration shows an
909 overview of the most commonly used frameworks, standards and guidance used for MEDICAL
910 DEVICES.



911

912 **Figure A.7 – Selection of IT security related documents**

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Nearing publication security related healthcare specific standards

- **ISO/TS 82304-2 (:2021-08) - 1st edition**
  Health informatics —Quality and reliability criteria for health and wellness apps
- **IEC 80001-1 (:2021-07) - 2nd edition**
  Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
- **IEC 81001-5-1 (:2021-11) - 1st edition**
  Health informatics — Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Activities in the Product Lifecycle

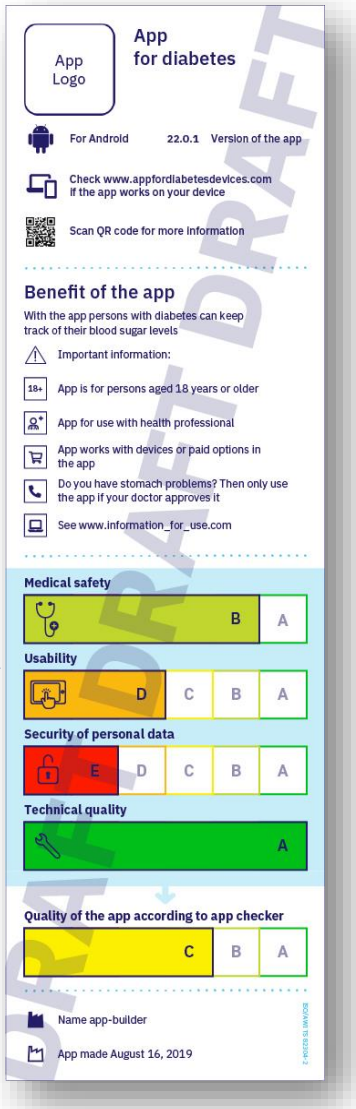
DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Focus on draft ISO/TS 82304-2

Health Software — Part 2: Quality and reliability criteria for health and wellness apps

Started as a CEN/TC 251 based on BSI PAS 277, with three main parts:

1. A walkthrough of relevant international Health Software product and process standards
2. defines the evidence that an app manufacturer should provide to show that their app conforms to the specification (Product information, Privacy, Safety and Security, Clinical Assurance, Usability (and Accessibility) and technical assurance
3. Annexes covering a range of topics such as a mapping between the product and process requirements, ethical considerations, relevant security and privacy considerations



DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Focus on draft IEC 81001-5-1

Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Security - Activities in the Product Lifecycle

This standard uses a well established secure by design process standard from the Industrial Control Systems IEC 62443 series developed by ISA99/IEC TC65:

> IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

To increase acceptability and ease of implementation ISO/IEC 81001-5-1 restructured IEC 62443-4-1 to align with IEC 62304 and describes the additional process activities to be executed as part of the 62304 processes to adequately address cybersecurity.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

In development security related healthcare specific standards

- **IEC/TR 80001-2-2 (:2023-12) – 2nd edition**
  Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- **IEC/TR 80001-2-8 (:2023-12) – 2nd edition**
  Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
- **ISO/TS 81001-2-1 (:2023-02) – 1st edition**
  Health software and health IT systems safety, effectiveness and security - Part 2-1: Coordination - Guidance for the use of assurance cases for safety and security
- **ISO/TS 14441 – 2nd edition**
  Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment
- **ISO/DTR 24306 – 1st edition**
  Health informatics - Guidance on Security for Gateways Used in Personal Health Care Systems

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

Thank you!

ben.kokx@philips.com

www.globalditta.org

Follow us onr @DITTA_online

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA Medical Imaging & Technology Alliance · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · KMDIA Korea Medical Devices Industry Association · ITAC Information Technology Association of Canada