

Medical Device Software

New IEC Guidance for Networked Medical Devices IEC 80001

By David Walker

How can patient safety be assured when a medical device is connected to an IT network?

Although there are regulations and standards that address the manufacture of medical devices and use by clinical staff, there are currently no standards to addresses how medical devices may be connected to general-purpose IT networks to achieve safe and secure delivery of health care.

A new proposed international standard, International Electrotechnical Commission (IEC) 80001 - Application of Risk Management for IT-Networks Incorporating Medical Devices, outlines requirements of both manufacturers of medical devices and organizations responsible for the operation of the IT network over its entire life cycle. According to the standard, the manufacturer of a medical device that is intended to be incorporated into an IT network is responsible for providing information about the medical device sufficient to allow the medical facility to manage risk when incorporating the device into an IT network.

The AAMI (Association for the Advancement of Medical Instrumentation) Medical Device Software Standards Committee is currently providing US comment on the draft of this standard. Although distribution of the draft standard is prohibited, this short report uses the outlines of IEC 80001 to provide a narration of its content.

Scope

1.1 Purpose

1.2 Field of application

Generally, the standard applies to medical device manufacturers and responsible organizations, but not to a single manufacturer that specifies a complete medical device that includes its own network. But the standard would apply to modifications to the specified configuration of a medical device that includes its own network.

2 Terms and Definitions

3 Roles and responsibilities

3.1 RESPONSIBLE ORGANIZATION

3.2 TOP MANAGEMENT

3.3 MEDICAL IT-NETWORK RISK MANAGER

3.4 MEDICAL IT-NETWORK MAINTAINER

3.5 MEDICAL DEVICE MANUFACTURER(S)

3.6 Other providers of Information Technology

3.7 RISK MANAGEMENT team

The responsible organization (organization accountable for the use and maintenance of the medical IT network) is required to apply risk management to the planning, installation, connection, operation, maintenance, and disconnection of the medical device IT network. The medical device manufacturer is required to provide, as part of the device specifications, instructions for implementing such connection, including but not limited to:

- Intended use of the medical device's connection to an IT network
- Required characteristics of the IT network incorporating the medical device
- Required configuration of the IT network incorporating the medical device
- Constraints governing the extent to which the IT network incorporating the medical device may be extended or modified after installation
- Technical specifications of the network connection of the medical device such as functional security specifications
- Intended information flow between the medical device and the IT network and, if relevant to the key properties (safety, effectiveness, data and system security, interoperability), the intended routing through the IT network

Also discussed are non medical devices used on the network. The responsible organization is required to maintain agreements where possible for providers of active non medical devices or related services. The agreements specify documentation requirements.

4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS

4.1 Overview

4.2 POLICY FOR RISK MANAGEMENT for INCORPORATING MEDICAL DEVICES

4.3 RISK MANAGEMENT PROCESS

4.4 Project Planning and Documentation

4.5 RISK ANALYSIS

4.6 RISK EVALUATION

4.7 RISK CONTROL

4.8 RESIDUAL RISK EVALUATION

4.9 Reporting and approval

4.10 CHANGE MANAGEMENT

4.11 Monitoring

Section 4 provides a valuable discussion of the application of risk management principles to medical device networks based on ISO 14971 Application of risk management to medical devices.

5 Document control

5.1 Document control procedure

5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE

Section 5 has no surprises. The responsible organization must maintain a secure risk management file.

Annex A (Informative) Overview of RISK MANAGEMENT relationships

Annex B (Informative) Guidance on field of application

Annex C (Informative) Maintaining an IEC 80001 compliant network

Annex D (Informative) Causes of HAZARDS associated with MEDICAL IT-NETWORKS

Annex E (Informative) Use of wireless technologies in medical networks

Annex F (Informative) MEDICAL IT-NETWORK RISK MANAGEMENT template

Annex G (Informative) MEDICAL IT-NETWORK security

Annex H (Informative) References

Bibliography

This report is intended to announce the new IEC 80001 and share some key elements of its content. More information regarding this new standard and its status will be published in future ASQ Software Division newsletter articles.

David Walker is the immediate past chair of the ASQ Software Division. He represents ASQ's interests in medical device software standards development through membership on the AAMI Medical Device Software Standards Committee.