TECHNICAL REPORT

ISO/TR 80001-2-6

First edition
2014-12-01

Application of risk management for IT-networks incorporating medical device —

Part 2-6: Application guidance — Guidance for responsibility agreements

Application de la gestion des risques pour les réseaux intégrant appareils médicaux —

Partie 2-6: Application guidage — Orientation des accords de responsabilité

Reference number
ISO/TR 80001-2-6:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO TR 80001-2-6 was prepared by Technical Committee ISO/TC 215, *Health informatics*, jointly with IEC Subcommittee IEC/SC 62A.

ISO/IEC TR 80001 consists of the following parts, under the general title *Application of risk management for IT-networks incorporating medical devices.*

— *Part 1: Roles, responsibilities and activities*

— *Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples*

— *Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*

— *Part 2-3: Guidance for wireless networks*

— *Part 2-4: Application guidance – General implementation guidance for Healthcare Delivery Organizations*

— *Part 2-5: Application guidance – Guidance on distributed alarm systems* (in development)

— *Part 2-6: Application guidance – Guidance for responsibility agreements*

— *Part 2-7: IT-networks incorporating medical devices - Part 2-7: Application Guidance - Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1* (in development)

— *Part 2-8: 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 80001-2-2* (in development)

Introduction

0.1 Background

IEC 80001-1 was developed to meet the need to managing RISKS associated with the increasing prevalence of MEDICAL DEVICES being connected to general purpose IT-NETWORKS. The standard introduces the notion of a RESPONSIBILITY AGREEMENT covering roles and responsibilities of the stakeholders. This Technical Report provides practical guidance to RESPONSIBLE ORGANIZATIONS on establishing a RESPONSIBILITY AGREEMENT among all stakeholders involved, namely the RESPONSIBLE ORGANIZATION, the MEDICAL DEVICE manufacturer(s) and the IT supplier(s).

Examples of situations where a RESPONSIBILITY AGREEMENT could prove useful when an IT-NETWORK incorporates MEDICAL DEVICES. The benefits of the RESPONSIBILITY AGREEMENT include:

a) The roles and responsibilities of the stakeholders are identified and communicated in written form.

   It is essential to have a clear understanding of the clinical dependencies on the network and to identify the roles and responsibilities of the stakeholders, including clinical staff and the MEDICAL DEVICE manufacturers.

   The organization or department responsible for configurations control and maintenance of the IT-NETWORK should have, or establish if necessary, change control procedures to manage the RISKS to services supported by the network arising from the implementation of changes to network (e.g. software upgrade to network components).

   EXAMPLE 1 Common examples include software upgrades for antivirus software or bug fixes in networking switches and routers. Before upgrading hard/soft/firmware on infrastructure supporting MEDICAL DEVICES and medical systems, it is important that MEDICAL DEVICES that can be impacted are identified through an impact assessment. To undertake such an assessment requires either detailed engineering knowledge of each component and its dependencies or for example, the co-operation of the respective manufacturer. Whichever party takes responsibility for this should then review and validate their systems on the new hard/soft/firmware. It is also important to ensure that whenever practicable, there is a back-out/regression plan which has also been tested. In this scenario, the RESPONSIBILITY AGREEMENT would set out the responsibilities of each party, e.g., How such activities would be initiated, who would notify whom, when, with what information and how would they be expected to respond. There have already been documented instances where MEDICAL DEVICES have been adversely affected from such changes and this was one reason for US FDA's "Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software." See:

   http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

b) A clinical user of a MEDICAL DEVICE can desire to connect the MEDICAL DEVICE to a general purpose IT-NETWORK. Having a PROCESS in place to inform and involve relevant stakeholders early in the planning stage (i.e., prior to go live) could help avert uninformed decision making and implementation that could adversely impact other clinical systems that rely on the IT-NETWORK.

   EXAMPLE 2 Demand already exists for this capability, e.g., delivery of MEDICAL DEVICE alarms via wireless communications devices carried by PATIENT care staff, automated/remote programming of infusion therapy pumps and Admit/Discharge/Transfer data feeds to medical monitoring systems. When doing so requires multiple otherwise independent stakeholders to be responsible for aspects of the system's development, implementation and operation, and maintenance, it is imperative that all stakeholders are explicitly aware and accepting of their responsibilities. A RESPONSIBILITY AGREEMENT serves as a vehicle to accomplish this.

0.2 Normative requirements from IEC 80001-1

In addition to the languages of subclause 4.3.4 describing the RESPONSIBILITY AGREEMENT, subclauses 3.5 and 3.6 require information to be made available to the RESPONSIBLE ORGANIZATION by MEDICAL DEVICE manufacturers and IT supplier, respectively. Both subclauses acknowledge the possibility that the information identified may be insufficient to address the RESPONSIBLE ORGANIZATION'S RISK MANAGEMENT needs by including the following notes:

NOTE 1 Where the content made available does not meet the RESPONSIBLE ORGANIZATION'S RISK MANAGEMENT need, additional content can be made available under a RESPONSIBILITY AGREEMENT.

NOTE 2 A RESPONSIBILITY AGREEMENT between the RESPONSIBLE ORGANIZATION and a MEDICAL DEVICE manufacturer can be used to identify and share the documentation needed.

Application of risk management for IT-networks incorporating medical devices — Part 2-6: Application guidance — Part 2-6: Guidance for responsiblity agreements

1 Scope

1.1 Purpose

This Technical Report provides guidance on implementing RESPONSIBILITY AGREEMENTS, which are described in IEC 80001-1 as used to establish the roles and responsibilities among the stakeholders engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK in order to support compliance to IEC 80001-1. Stakeholders may include RESPONSIBLE ORGANIZATIONS, IT suppliers, MEDICAL DEVICE manufacturers and others. The goal of the RESPONSIBILITY AGREEMENT is that these roles and responsibilities should cover the complete lifecycle of the resulting MEDICAL IT-NETWORK.

1.2 Prerequisites

The RESPONSIBLE ORGANIZATION'S (ROs) TOP MANAGEMENT has accepted responsibility for the successful implementation of IEC 80001-1. As required by IEC 80001-1, the RO has created and approved policies for the RISK MANAGEMENT PROCESS and RISK acceptability criteria while balancing the three KEY PROPERTIES with the mission of the RO. The RO has identified and provisioned adequate resources and assigned qualified personnel to perform tasks related to the standard. The RO has appointed a MEDICAL IT-NETWORK RISK MANAGER and is prepared to establish the RESPONSIBILITY AGREEMENT.

2 Normative references

The following document, in whole or in part, is normatively referenced in this document and is indispensable for its application. As a dated reference, only the edition cited applies.

IEC 80001-1:2010, *Application of risk management for IT -networks incorporating medical devices – Part 1: Roles, responsibilities and activities*

3 Terms and definitions

3.1
CHANGE PERMIT
outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT activities subject to specified constraints

[SOURCE: IEC 80001-1:2010, 2.3]

3.2
DATA AND SYSTEM SECURITY
operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability