Technical Information Report

AAMI/ISO TIR 80001-2-6: 2014

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

AAMI
Advancing Safety in Healthcare Technology

A Technical Report prepared by AAMI and registered with ANSI AAMI/ISO TIR80001-2-6:2014

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

Approved 10 December 2014 by
Association for the Advancement of Medical Instrumentation

Registered 9 August 2015 by
American National Standards Institute, Inc.

Abstract: Provides guidance for stakeholders on implementing RESPONSIBILITY AGREEMENTS 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 ANSI/AAMI/IEC 80001-1. The goal of the RESPONSIBILITY AGREEMENT is that these roles and responsibilities should cover the complete lifecycle of the resulting MEDICAL IT-NETWORK.

Keywords: Responsibility Agreements. IT-network, MEDICAL DEVICES, RESPONSIBLE ORGANIZATIONS, IT suppliers, MEDICAL DEVICE manufacturers

Published by

Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Drive, Suite 301
Arlington, VA 22203-1633
www.aami.org

Printed in the United States of America

ISBN 1-57020-594-9

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. For a TIR, AAMI consults with a technical committee about five years after the publication date (and periodically thereafter) for guidance on whether the document is still useful—that is, to check that the information is relevant or of historical value. If the information is not useful, the TIR is removed from circulation.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

ANSI Registration

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

Contents

Page

Glossary of equivalent standards

International Standards or Technical Reports adopted in the United States may include normative references to other International Standards. AAMI maintains a current list of each International Standard that has been adopted by AAMI (and ANSI). Available on the AAMI website at the address below, this list gives the corresponding U.S. designation and level of equivalency to the International Standard.

www.aami.org/standards/glossary.pdf

Committee representation

Association for the Advancement of Medical Instrumentation

AAMI/SM/WG 02, Information Technology Networks Working Group

The adoption of the ISO 80001-2-6 as a new AAMI/ISO Technical Information Report was initiated by the AAMI Information Technology Working Group.

Committee approval of the standard does not necessarily imply that all committee members voted for its approval.

At the time this document was published, **the AAMI Information Technology Networks Working Group** had the following members:

Chair: Bill Hintz, Medtronic Inc

Members:
John Collins, American Hospital Association
Todd Cooper, Center for Medical interoperability
Becky Crossley, Susquehanna Health
Conor Curtin, Fresenius Medical Care
Yadin David, Biomedical Engineering Consultants LLC
Richard De La Cruz, Silver Lake Group Inc
Christina DeMur, Draeger Medical Systems Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Kurt Elliason, Smiths Medical
Jim Gabalski, Getinge USA
George Gray, Ivenix Inc
Thomas Grobaski, Belimed Inc
Bill Hintz, Medtronic Inc
Catherine Li, FDA/CDRH
Yimin Li, St Jude Medical Inc
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, Mary Beth McDonald Consulting
Andrew Northup, Medical Imaging & Technology Alliance a Division of NEMA
Dave Osborn, Philips Electronics North America
Geoff Pascoe
Steven Rakitin, Software Quality Consulting
Rick Schrenker, Massachusetts General Hospital
Neal Seidl, GE Healthcare
Xianyu Shea, Stryker Medical Division
Ray Silkaitis, Amgen Inc
Bob Steurer, Spacelabs Medical Inc
Chandresh Thakur, CareFusion
Donna-Bea Tillman, Biologics Consulting Group
Daidi Zhong, Chongqing University

Alternates:
James Dundon, Spacelabs Medical Inc
Brian Fitzgerald, FDA/CDRH
Rich Gardner, GE Healthcare
Phil Raymond, Philips Electronics North America
Thomas Schultz, Medtronic Inc WHQ Campus
Ferry Tamtoro, Amgen Inc
Fei Wang, Fresenius Medical Care
Fei Want, Fresenius Medical Care

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Background of AAMI adoption of ISO TR 80001-2-6 Ed.1

As indicated in the foreword to the main body of this document, the International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. The United States is one of the ISO members that took an active role in the development of this technical report.

International Technical Report ISO TR 80001-2-6 Ed.1 was developed jointly by Sub-Committee IEC/SC 62A, Common aspects of electrical equipment used in medical practice and ISO/TC 215, Health informatics, to define the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security.

U.S. participation in this IEC/SC 62A is organized through the U.S. Technical Advisory Group for IEC/SC 62A, administered by AAMI on behalf of the American National Standards Institute (ANSI).

AAMI encourages its committees to harmonize their work with international documents as much as possible. The AAMI Information Technology Working Group, together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed ISO TR 80001-2-6 Ed.1 to formulate the U.S. position while the document was being developed. This close collaboration helped gain widespread U.S. consensus on the document. As the U.S. Technical Advisory Group for IEC/SC 62A, the AAMI Information Technology Networks Working Group voted to adopt the IEC Technical Report as written.

AAMI has adopted other ISO documents. See the Glossary of Equivalent Standards for a list of ISO standards adopted by AAMI, which gives the corresponding U.S. designation and the level of equivalency with the ISO standard.

The concepts incorporated into this technical report should not be considered inflexible or static. This technical information report, like any other, must be reviewed and updated periodically to assimilate progressive technological developments. To remain relevant, it must be modified as technological advances are made and as new data comes to light.

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Suggestions for improving this TIR are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N Fairfax Drive, Suite 301, Arlington VA 22203-1633

NOTE—Beginning with the ISO foreword on page viii, AAMI/ISO TIR 80001-2-6:2014, *Application of risk management for IT-networks incorporating medical — Application guidance — Part 2-6: Guidance for responsibility agreements,* is identical to ISO/TR 80001-2-6 Ed.1.

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/IEC TR 80001-2-6 was prepared by Technical Committee ISO/TC 215, *Heath informatics*, jointly with IEC Subcommittee 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*

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

— *Part 2-7: Application Guidance – Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*

— *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 — Application guidance — Part 2-6: Guidance for responsibility 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
[SOURCE: IEC 80001-1:2010, 2.5]

3.3
EFFECTIVENESS
ability to produce the intended result for the subject of care and the RESPONSIBLE ORGANIZATION
[SOURCE: IEC 80001-1:2010, 2.6]

3.4
EVENT MANAGEMENT
PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner
[SOURCE: IEC 80001-1:2010, 2.7]

3.5
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY
[SOURCE: IEC 80001-1:2010, 2.8]

3.6
HAZARD
potential source of HARM
[SOURCE: IEC 80001-1:2010, 2.9]

3.7
INFORMATION TECHNOLOGY
branch of engineering that deals with the use of computers and telecommunications to retrieve, store, and transmit information

3.8
IT-NETWORK
electronic data transmission facility which can comprise of just a point-to-point wire link between two devices, or a complex arrangement of transmission lines.
[SOURCE: IEC 80001-1:2010, 2.12]

3.9
KEY PROPERTIES
three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY) of MEDICAL IT-NETWORKS
[SOURCE: IEC 80001-1:2010, 2.13]

3.10
MEDICAL DEVICE
Means any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological process,
- supporting or sustaining life,
- control of conception,
- disinfection of MEDICAL DEVICES,
- providing information for medical or diagnostic purposes by means of *in vitro* examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations

Note 2 to entry: Products which may be considered to be MEDICAL DEVICES in some jurisdictions but for which there is not yet a harmonized approach, are:

- aids for disabled/handicapped people;
- devices for the treatment/diagnosis of diseases and injuries in animals;
- accessories for MEDICAL DEVICES (see Note 3 to entry);
- disinfection substances;
- devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' MEDICAL DEVICE to enable that MEDICAL DEVICE to achieve its intended purpose should be subject to the same GHTF procedures as apply to the MEDICAL DEVICE itself. For example, an accessory will be classified as though it is a MEDICAL DEVICE in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to MEDICAL DEVICES are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a "MEDICAL DEVICE."

[SOURCE: IEC 80001-1:2010, 2.14, modified — NOTES changed to "notes to entry" format.]

3.11
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE
[SOURCE: IEC 80001-1:2010, 2.16]

3.12
MEDICAL IT-NETWORK RISK MANAGER
person accountable for RISK MANAGEMENT of a MEDICAL IT-NETWORK
[SOURCE: IEC 80001-1, 2.17]

3.13
MONITORING
on-going review of all RISK MANAGEMENT activities and RISK control options that were put in place to achieve acceptable RISK in the use of MEDICAL IT-NETWORK(S)

3.14
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs in a computer program
[SOURCE: IEC 80001-1:2010, 2.19]

3.15
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders
[SOURCE: IEC 80001-1:2010, 2.21]

3.16
RESPONSIBLE ORGANIZATION
RO
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK
[SOURCE: IEC 80001-1:2010, 2.22]

3.17
RISK
combination of the probability of occurrence of HARM and the severity of that HARM
[SOURCE: IEC 80001-1:2010, 2.23]

3.18
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK
[SOURCE: IEC 80001-13.19:2010, 2.24]

3.19
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION
[SOURCE: IEC 80001-1:2010, 2.25]

3.20
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK
[SOURCE: IEC 80001-1:2010, 2.27]

3.20
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and MONITORING RISK
[SOURCE: IEC 80001-1:2010, 2.28]

3.21
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment
[SOURCE: IEC 80001-1:2010, 2.30

3.22
TOP MANAGEMENT
person or group of people e who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level
[SOURCE: IEC 80001-1:2010, 2.31]

4 Key aspects for RESPONSIBILITY AGREEMENTS

4.1 Reasons and rationale

Among the important aspects of implementing and maintaining a MEDICAL IT-NETWORK is distributing responsibilities for its RISK MANAGEMENT activities. Clear allocation of these responsibilities is indispensable for achieving the targets of the three KEY PROPERTIES as defined by the RESPONSIBLE ORGANIZATION.

RESPONSIBILITY AGREEMENTS are a means to document the roles and responsibilities relating to RISK MANAGEMENT, of the various stakeholders involved in the activities associated with procurement, implementation or through-life /in-service management of MEDICAL IT-NETWORK. Each project/ network will be different and it is possible that some may already have some roles and responsibilities defined and in such cases the RESPONSIBILITY AGREEMENT will simply help with identifying any gaps. In other projects however, the RESPONSIBLE ORGANIZATION may find that it becomes a key PROCESS for establishing the management PROCESSES that will be required to adequately manage RISKS relating to the three KEY PROPERTIES.

4.2 Participants

RESPONSIBILITY AGREEMENTS may not only be needed between the RO, MEDICAL DEVICE manufacturers, and IT suppliers but may also be helpful between different stakeholders within the RESPONSIBLE ORGANIZATION like the biomedical engineering department and the IT department.

4.3 Proposed types of RESPONSIBILITY AGREEMENTS

Depending upon the context for which it is to be used, a RESPONSIBILITY AGREEMENT can span the spectrum from informal to formal. A RESPONSIBILITY AGREEMENT can take the form of a Memorandum of Understanding (MoU) e.g., 1) Planning and & Design Phase, 2) Installation and Go Live Phase, and 3) Maintenance Phase. Later in the life cycle and given that there may be commitments to provide specific services in certain situations, a RESPONSIBILITY AGREEMENT for a system being placed in active clinical service may need to take the form of a legal contract.

4.4 Communication control

4.4.1 Bilateral versus multilateral RESPONSIBILITY AGREEMENTS

In the case that more than two parties are required to be included in RESPONSIBILITY AGREEMENTS the MEDICAL IT-NETWORK RISK MANAGER should consider whether separate bilateral agreements or a common RESPONSIBILITY AGREEMENT should be set up. The difference between these solutions is the extent of information sharing. While a high degree of information sharing is often valuable, it needs to be weighed against privacy of information and increased effort in case of updates.

4.4.2 Non-disclosure agreements

In the event any stakeholder has concerns related to disclosing proprietary information a confidentiality or Non-Disclosure Agreement (NDAs) can be established with the RESPONSIBLE ORGANIZATION. This will ensure that the proprietary information is kept confidential between one or more stakeholders and the RESPONSIBLE ORGANIZATION.

In many cases technical data provided by the MEDICAL DEVICE manufacturer and IT suppliers which are essential for RISK MANAGEMENT of the MEDICAL IT-NETWORK are sensitive to confidentiality. A means to support this confidentiality is to limit the intended audience of this information (see also bilateral vs. multilateral) or to establish NDAs.

4.4.3 Update of information and documentation

Technical information as well as personnel responsible for specified activities may change over time. It is important that these changes are communicated to the stakeholders in a timely manner. This should be done by update of the documentation which contains this information. Furthermore, this requires assigning revision identifiers to the documents. An appropriate mechanism should be described in the RESPONSIBILITY AGREEMENT(S) and should cover possible updates of the RESPONSIBILITIES AGREEMENTS themselves.

4.5 Responsibility for establishing

The overall responsibility for establishing RESPONSIBILITY AGREEMENTS rests with the MEDICAL IT-NETWORK RISK MANAGER (see 4 c) and e) of IEC 80001-1:2010).

4.6 Methods for determination and of responsibilities

The starting point for determination of responsibilities is the preparation of the overall plan for incorporation of MEDICAL DEVICES into the network. In addition, IEC 80001-1:2010, 4.3.5 b) requires for the RISK MANAGEMENT plan a description of activities, roles and responsibilities for all parties involved in operating/maintaining the MEDICAL IT-NETWORK, with respect to RISK MANAGEMENT.

Subclauses 3.4 through 3.6 of the standard define responsibilities for the usually involved parties, e.g. for the provision of specific information.

Setting up this plan requires the participation of the involved MEDICAL DEVICE manufacturers and IT suppliers. Usually, this planning comprises high level meetings with all MEDICAL DEVICE manufacturers and IT suppliers as well as meetings on a very detailed level with experts from at least two involved parties.

The MEDICAL IT-NETWORK RISK MANAGER should determine which level of detail needs to be defined in the RISK MANAGEMENT plan and which level of detail can be left up to the internal plans of the involved parties. The contents of the RESPONSIBILITY AGREEMENT(S) are based on this determination.

Analysis tools can be used to support identification, clarification, and understanding of stakeholder roles in any task of any phase. An example is the Responsible, Accountable, Consulted, Informed (RACI) chart, where the acronym RACI stands for:

- Responsible for performing the task
- Accountable for the task being completed
- Consulted prior to the task being performed
- Informed that the task has been completed.

An example for a RACI chart is contained in Annex A.

4.7 Life cycle considerations

When establishing RESPONSIBILITY AGREEMENTS it should be taken into account that different phases of the lifecycle necessitate different activities and different responsibilities. This should be considered from the very beginning of the project. For our purpose here, the lifecycle of a network can be considered as divided into the Planning and Design, Installation and Go Live, Maintenance phases. The design phase includes the planning phase where the network is designed to meet the needs of the specific healthcare delivery organization, as well as any phase where, for example, the architecture, topology or hardware used within an existing network is modified. The maintenance phase includes times where the network is operational and changes are completed while the network is in operation. Changes to the network during the maintenance phase are restricted to replacement of defective parts. Modification of the network according to CHANGE PERMITS as described in IEC 80001-1 may be seen as part of the maintenance phase.

Reference information supporting these phases is available from various sources. For example:

- Manufacturer Disclosure Statement for MEDICAL DEVICE Security – MDS2
- See also Annex B for information which might be required in specific phases.

5 Elements of a RESPONSIBILITY AGREEMENT

The purpose of this clause is to elaborate upon the requirements of subclause 4.3.4 of the IEC 80001-1:2010. Boxed text [items a) – h)] is copied from 80001-1:2010 to identify the subclauses for which guidance is provided.

NOTE 1 If in the following more than two parties are mentioned this does not impose that multilateral RESPONSIBILITY AGREEMENTS are required or preferable compared to bilateral RESPONSIBILITY AGREEMENTS.

a) the name of the person responsible for RISK MANAGEMENT for the activities covered by the RESPONSIBILITY AGREEMENT

IEC 80001-1:2010, 4.3.4 a) requires provision of the name of the responsible person for the RISK MANAGEMENT project at each of the legal entities, e.g., RESPONSIBLE AGREEMENT between different stakeholders by the REPONSIBILITY ORGANIZATION.

Guidance:

1) In addition to the name the necessary contact data should be provided.

   NOTE Documentation of this information in a separate attachment allows for a more efficient search and easier update.

2) This person should have the authority to perform or initiate and control the tasks covered by the RESPONSIBILITY AGREEMENT in line with the requirements by the standard.

3) For the RESPONSIBLE ORGANIZATION this person is usually the MEDICAL IT-NETWORK RISK MANAGER.

4) Depending on the type and extent of activities covered by the RESPONSIBILITY AGREEMENT, additional persons for each legal entity may be defined together with their specific roles (see also 4.3.4 b) within the RISK MANAGEMENT PROCESS. This is for ease of operation; the overall responsibility stays with the responsible person. Special care should be taken if activities are (completely) outsourced to subcontractors. Even in this case the top responsibility resides within the legal entity covered by the agreement and the name of this person needs to be stated in the RESPONSIBILITY AGREEMENT.

b) the scope of the activities covered by the RESPONSIBILITY AGREEMENT, including a summary of and/or reference to the requirements;

IEC 80001-1:2010, 4.3.4 b) requires a summary of the scope of the activities covered by the RESPONSIBILITY AGREEMENT, including a summary of and/or reference to the requirements. Ownership/assignment of activities related to RISK MANAGEMENT for the project should be summarized in the RESPONSIBILITY AGREEMENT, for example, to support sharing and understanding of all stakeholders' responsibilities.

Guidance:

1) This section of the RESPONSIBILITY AGREEMENT should include a summary of each of the stakeholder's roles and responsibilities as they relate to the project. Where stakeholders will share responsibility for activities related to RISK MANAGEMENT, this section should summarize how they will work together to accomplish the tasks.

2) Further details of roles and responsibilities and co-operation are required in response to IEC 80001-1:2010, 4.3.4 f) and g) below.

3) Where information such as details of responsibilities is contained in other configuration controlled documentation and it is appropriate to do so, the RESPONSIBILITY AGREEMENT should reference that documentation rather than duplicate their content.

4) IEC 80001-1:2010, 4.3.5 b) requires the MEDICAL IT-NETWORK RISK MANAGER to produce a RISK MANAGEMENT plan that describes the activities, roles and responsibilities for all parties involved in operating/maintaining the MEDICAL IT-NETWORK, with respect to RISK MANAGEMENT. Since the scope of activities that need to be covered in the RESPONSIBILITY AGREEMENT are likely to be a subset of the overall activities for the project the identification, of these activities could be undertaken as part of the preparation of the overall RISK MANAGEMENT plan for incorporation of MEDICAL DEVICES into the network.

5) The MEDICAL IT-NETWORK RISK MANAGER should determine which level of detail needs to be defined in the RISK MANAGEMENT plan and which level of detail can be left up to the internal plans of the involved parties.

6) Requirements might comprise expected output, required input, or time constraints, including response times on adverse events.

c) a list of the MEDICAL DEVICES and other equipment which are to be incorporated into the IT-NETWORK or changed, together with the names of MEDICAL DEVICE manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project

IEC 80001-1:2010, 4.3.4 c) requires a list of MEDICAL DEVICES and other equipment which are to be incorporated into the IT-NETWORK or changed, together with the names of MEDICAL DEVICE manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project.

Guidance:

1. Other equipment could include general purpose network devices, general purpose servers running general purpose or health related software applications.

2) The RESPONSIBLE ORGANIZATION should carefully consider the level of detail needed with respect to description of the MEDICAL DEVICES, e.g., software versions or accessories that are considered within the scope of the system. The level of detail needs to be sufficient to enable the impact of changes to be and managed, e.g., model numbers, part numbers and firmware/ software versions. Insufficient specification early on may lead to false assumptions or further information requests later on in the project or when managing changes.

3) Where a listed MEDICAL DEVICE is not supplied by its manufacturer, either the supplier of the device will need to obtain the required information from the original manufacturer, or the RESPONSIBLE ORGANIZATION may need to consider including the manufacturer in the RESPONSIBILITY AGREEMENT. There might be further situations where other involved parties are required to provide technical information. All organizations referred to in this section e) should be included in the information required by paragraphs a) and b).

d) a list of documents to be supplied by the MEDICAL DEVICE manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT-NETWORK

IEC 80001-1:2010, 4.3.4 d) requires a list of documents to be supplied by the MEDICAL DEVICE manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT-NETWORK.

Guidance:

1. The documents required may include instructions for assembly, installation, adjustment and testing of such components necessary for the RESPONSIBLE ORGANIZATION to manage RISK and maintain the KEY PROPERTIES OF SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY of the MEDICAL IT-NETWORK.
2. Such documentation should include interface specifications and specifications for other components compatible with those devices to be installed when compliance of the system or subsystem depends on their compatibility. Lists of known non-compatible components should also be provided. Such specifications may describe pertinent physical characteristics of the components and/or may list by manufacturer model number the components which are compatible.
3. Some of the documentation may be supplied with the device. Other documents may be available from the MEDICAL DEVICE manufacturers or IT supplier only on specific request and possibly at extra cost. Where additional information may be required for RISK MANAGEMENT, the RESPONSIBLE ORGANIZATION should request the appropriate information and provide supporting rationale for this request.
4. The list of documentation should be linked to the list of MEDICAL DEVICES and the organization responsible for their provision according to IEC 80001-1:2010, 4.3.4 c).
5. All requests for documentation should include dates by which the documentation is to be supplied.

e) technical information to be supplied by the MEDICAL DEVICE or IT manufacturers and other equipment suppliers that is necessary to perform RISK ANALYSIS for the IT-NETWORK

IEC 80001-1:2010, 4.3.4 e) requires a list of documents to be supplied by the MEDICAL DEVICE manufacturer or IT manufacturers and other equipment suppliers that is necessary to perform RISK ANALYSIS for the IT- NETWORK. In addition to the requirements under paragraph d), information specific to RISK MANAGEMENT should be supplied. Where additional information may be required for RISK MANAGEMENT, the RESPONSIBLE ORGANIZATION should request the appropriate information and provide supporting rationale for this request

Guidance:

See also Annex C for technical information which might be necessary for RISK MANAGEMENT.

f) definition of roles and responsibilities in managing potentially adverse events

IEC 80001-1:2010, 4.3.4 f) requires a definition of roles and responsibilities in managing potentially adverse events.

Guidance:

1) Adverse events may be defined and classified by the RO's RISK acceptability and/or regulatory agencies.

2) Prior to the RO placing the system into clinical use and for the entire lifecycle of the system [see also IEC 80001-1:2010, 4.6.2 on EVENT MANAGEMENT, the RESPONSIBLE ORGANIZATION'S MEDICAL IT- NETWORK RISK MANAGER is responsible for identifying and negotiating the roles and responsibilities of the MEDICAL DEVICE manufacturers, IT manufacturers, other equipment suppliers and departments within the RESPONSIBLE ORGANIZATION.

3) The RO should provide a summary of responsibilities detailed in the RESPONSIBILITY AGREEMENT as appropriate

g) identify the nature of the co-operation required

IEC 80001-1:2010, 4.3.4 g) requires the nature of the co-operation required between stakeholders be identified. In addition to the provided documentation, stakeholders can require additional co-operation from each other. When additional co-operation is required among stakeholders the nature of the required co- operation should be summarized within the RESPONSIBILITY AGREEMENT.

Guidance:

To minimize duplication, the RESPONSIBILITY AGREEMENT may refer out to other documents for the detail.

h) state:

— who is responsible for requesting such co-operation;

— who is responsible for responding to such requests; and

— what criteria will be used to judge the adequacy of such response?

IEC 80001-1:2010, 4.3.4 h) requires the summary should include who is responsible for requesting additional co-operation and who is responsible for responding to requests for additional co-operation.

Guidance:

1) The summary may also provide guidance for assessing stakeholder performance, e.g., criteria for assessing reasonableness of requests, and adequacy of responses.
2) The information in the RESPONSIBILITY AGREEMENT that fulfils the requirements of 4.3.4 g) and h) should be updated throughout the lifecycle of the MEDICAL IT-NETWORK as people and scopes change over time.

Annex A
(informative)

RACI chart

The example in Figure A.1 provides guidance how the method RACI chart can be used for a RESPONSIBILITY AGREEMENT to identify responsibilities in different phases of a project among different stakeholder groups.

Department:	
Procedure:	
Updated:	

Item	Task	RO	IT	MDV
1	**Project phase: Planning & Design**			
1.1.	MEDICAL DEVICE manufacturer provides performance requirement	C,I		A,R
1.2	RESPONSIBLE ORGANIZATION asks MEDICAL DEVICE manufacturer about known RISKS of the own MEDICAL DEVICE incorporation with IT-NETWORKS	A,R		I
1.3	MEDICAL DEVICE manufacturer provides RISK relevant information back to RO	I		A,R
1.4	RESPONSIBLE ORGANIZATION performs a RISK ASSESSMENT survey	R, A	I, C	I, C
2	**Project phase: Installation and go life**			
2.1	RESPONSIBLE ORGANIZATION sets up a quality assurance contract or service level agreement with each MEDICAL DEVICE manufacturer and each IT supplier	A, R	C, A, I	C, A, I
2.2	MEDICAL DEVICE manufacturer provides a list of implemented MEDICAL DEVICES into target *IT-NETWORK* to RESPONSIBLE ORGANIZATION, incl. e.g. type of device, serial number, IP address in target network	I		A,R
2.3	IT supplier provides the network plan with defined responsibility for interfaces	C,I	A,R	C, I
2.4	RESPONSIBLE ORGANIZATION creates RISK MANAGEMENT file according ISO 80001-1	A, R		
3	**Project phase: maintenance**			
3.1	MEDICAL DEVICE manufacturer conducts maintenance tasks or safety checks on MEDICAL DEVICES	C,I		A,R
3.2	IT supplier conducts maintenance tasks on IT components	C, I	A, R	
3.3	RESPONSIBLE ORGANIZATION maintains RISK MANAGEMENT file according ISO 80001-1	A, R		

R	Responsible for performing the task
A	Accountable for the task being completed
C	Consulted prior to the activity being performed
I	Informed that the task has been completed

Figure A.1 – Example RACI chart

Annex B
(informative)

Typical documents

Annex B provides an overview about typical documents required or provided within different project phases. Table B.1 should create a common understanding about available documents and their content within the different stakeholder groups.

Table B.1 — Typical documents required or provided within different project phases

Stakeholder		**Project phase**					
		Planning and design		**Implementation and go give**			**Maintenance**
		Kick off	**Planning and design**	**Implementation and**	**Training**	**Go live**	
MEDICAL DEVICE manufacturer	Document type	Technical Information, specification, interface description	Security specification according to IEC/TR 80001-2-2, network topology	Service Report, Implementation Protocols	Training record, operating manual	Network plan with defined responsibilities for inter-faces, List of MEDICAL DEVICE according to 5c	Service Report, Service Information

Stakeholder		Project phase					
		Planning and design		Implementation and go give			Maintenance
		Kick off	Planning and	Implementation and	Training	Go live	
MEDICAL DEVICE Manufacturer (cont.)	Information/ content	Performance Requirements, e.g. type of connection, used protocols, intended use, required ports, network requirements, IT hardware requirements, IT software requirements, known RISKS of MEDICAL DEVICE incorporated with IT-NETWORKS	Degree of fulfilment of system security requirements description of used subnet components, e.g. active network components, server, databases	Overview about current implementation of the MD into the IT-NETWORK successful pass of defined test from the manufacturer documentation of activities during implementation	Documentation of the training for users incl. intended use and appropriate use Operating instructions	Current network topology incl. range of used IP addresses in target IT-NETWORK type of medical product incl. serial number, software version, IP addresses	Maintenance tasks with impact on the target IT-NETWORK product changes with impact on the target IT- NETWORK safety checks
IT supplier	Document type	Technical Information, specification	Network plan	Implementation protocols		Network plan with defined responsibilities for interfaces, list of IT components which are integrated into the IT-NETWORK,	Service Report

Stakeholder		**Project phase**					
		Planning and design		**Implementation and go give**			**Maintenance**
		Kick off	**Planning and design**	**Implementation and**	**Training**	**Go live**	
IT supplier (cont.)	Information/ content	Performance Requirements, e.g. type of connection, used protocols, intended use, required ports, network requirements, IT hardware requirements, IT software requirements	Description of the overall network topology and boundaries to all subnets (in case the IT supplier is in charge)	documentation of activities during implementation Successful pass of defined test from the manufacturer		Current network topology incl. range of used IP addresses in target IT-NETWORK type of IT components incl. serial number, software version, IP addresses	Maintenance tasks with impact on the target IIT-NETWORK product changes with impact on the target IT-NETWORK
RESPONSIBLE ORGANIZATION	Document type	Network plan, specification target IT-NETWORK	network plan, RISK and responsibility assessment survey	RESPONSIBILITY AGREEMENT, service level agreement, quality assurance contracts		Final network plan, Overall list of MEDICAL DEVICES and IT components, RISK MANAGEMENT file	Service level agreement, quality assurance contracts, RISK MANAGEMENT file, network plan

Stakeholder		Project phase					
		Planning and design		Implementation and go give			Maintenance
		Kick off	Planning and design	Implementation and	Training	Go live	
RESPONSIBLE ORGANIZATION (cont.)	Information/ content	Network topology where medical products have to be integrated hardware and software description of the target IT-NETWORK	Description of the overall network topology and boundaries to all subnets (in case the RO is in charge) Description of potential RISKS of the integration of MEDICAL DEVICES in IT-NETWORKS Description of responsibilities	Defined responsibilities between the different stake holders e.g. defined response times and tasks e.g. defined PROCESS for information exchange		Overall list of all integrated MEDICAL DEVICES and IT components, incl. type, serial number, software version, IP addresses Overall current network topology incl. range of used IP addresses in target IT-NETWORK	Maintained service level agreements with IT vendors Maintained quality assurance contract with MEDICAL DEVICE manufacturer and IT vendor Maintained RISK MANAGEMENT file according IEC 80001-1