Technical Information Report

AAMI/ISO TIR 80001-2-6: 2014

This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchase decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.
PREVIEW COPY

This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.

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
PREVIEW COPY

This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.

Published by

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

© 2015 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of ISO and AAMI. No part of this publication may be reproduced or distributed in any form, including an electronic retrieval system, without the prior written permission of AAMI. All requests pertaining to this document should be submitted to AAMI. It is illegal under federal law (17 U.S.C. § 101, et seq.) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violators risk legal action, including civil and criminal penalties, and damages of $100,000 per offense. For permission regarding the use of all or any part of this document, complete the reprint request form at www.aami.org or contact AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633. Phone: +1-703-525-4890; Fax: +1-703-525-1067.

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.
## Glossary of equivalent standards ................................................................. v
## Committee representation ........................................................................... vi
## Background of AAMI adoption of ISO TR 80001-2-6 Ed.1 ........................ vii
## Foreword ...................................................................................................... viii
## Introduction ................................................................................................ ix

### 1 Scope ........................................................................................................ 1
1.1 Purpose .................................................................................................. 1
1.2 Prerequisites ........................................................................................... 1

### 2 Normative References ............................................................................... 1

### 3 Terms and Definitions .............................................................................. 1

### 4 Key aspects for RESPONSIBILITY AGREEMENTS ................................ 4
4.1 Reasons and rationale ................................................................................ 4
4.2 Participants .............................................................................................. 4
4.3 Proposed types of RESPONSIBILITY AGREEMENTS ............................... 4
4.4 Communication control ............................................................................ 4
  4.4.1 Bilateral versus multilateral RESPONSIBILITY AGREEMENTS ............ 4
  4.4.2 Non-disclosure agreements .................................................................. 4
  4.4.3 Update of information and documentation ........................................... 5
4.5 Responsibility for establishing ................................................................. 5
4.6 Methods for determination and of responsibilities ................................... 5
4.7 Life cycle considerations .......................................................................... 5

### 5 Elements of a RESPONSIBILITY AGREEMENT .................................... 5

### Annex A (informative)  RACI chart ............................................................. 9

### Annex B (informative)  Typical documents ................................................. 10

---

**PREVIEW COPY**

This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision. For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.
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 Ellis, The 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 Schrenger, 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
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.


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

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, Health 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 they would 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.
This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.

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.