Technical Information Report

ANSI/AAMI/ IEC TIR80001-2-2:2012

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

AAMI
Advancing Safety in Medical Technology

Copyright Association for the Advancement of Medical Instrumentation

AVA Documents
Document Sharing Hub

Full document details: n etworks i n co rp ora ti n g

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

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

Approved 20 August 2012 by
Association for the Advancement of Medical Instrumentation

Approved 30 September 2012 by
American National Standards Institute, Inc.

Abstract: Step-by-step guide to help in the application of risk management when creating or changing a medical IT-network.

Keywords: medical device, risk management, information technology, interoperability, IT-network

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

Published by

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

© 2012 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of ISO, ANSI, 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 1–57020–461–6

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

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 Technical Report

This AAMI TIR has been registered by the American National Standards Institute as an ANSI Technical Report.

Publication of this ANSI Technical Report has been approved by the accredited standards developer (AAMI). This document is registered as a Technical Report series of publications 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.

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

Contents

Page

Glossary of equivalent standards vi
Committee representation ix
Background of AAMI adoption of IEC/TR 80001-2-2:2012 x
FOREWORD xi
INTRODUCTION xiii
1 Scope 1
2 Normative references 2
3 Terms and definitions 2
4 Use of SECURITY CAPABILITIES 6
4.1 Structure of a SECURITY CAPABILITY entry 6
4.2 Guidance for use of SECURITY CAPABILITIES in the RISK MANAGEMENT PROCESS 7
4.3 Relationship of ISO 14971-based RISK MANAGEMENT to IT security RISK MANAGEMENT 7
5 SECURITY CAPABILITIES 8
5.1 Automatic logoff – ALOF 8
5.2 Audit controls – AUDT 9
5.3 Authorization – AUTH 9
5.4 Configuration of security features – CNFS 11
5.5 Cyber security product upgrades – CSUP 11
5.6 HEALTH DATA de-identification – DIDT 11
5.7 Data backup and disaster recovery – DTBK 12
5.8 Emergency access – EMRG 12
5.9 HEALTH DATA integrity and authenticity – IGAU 13
5.10 Malware detection/protection – MLDP 13
5.11 Node authentication – NAUT 13
5.12 `Person authentication – PAUT 14
5.13 Physical locks on device – PLOK 15
5.14 Third-party components in product lifecycle roadmaps – RDMP 15
5.15 System and application hardening – SAHD 16
5.16 Security guides – SGUD 16
5.17 HEALTH DATA storage confidentiality – STCF 17
5.18 Transmission confidentiality – TXCF 17
5.19 Transmission integrity – TXIG 18
6 Example of detailed specification under SECURITY CAPABILITY: Person authentication – PAUT 18
7 References 19
8 Other resources 21
8.1 General 21
8.2 Manufacture disclosure statement for medical device security (MDS2) 21
8.3 Application security questionnaire (ASQ) 21
8.4 The Certification Commission for Healthcare Information Technology (CCHIT) 21

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

8.5 http://www.cchit.org/get_certifiedHL7 Functional Electronic Health Record (EHR) 21
8.6 Common criteria – ISO/IEC 15408 22
9 Standards and frameworks 22
Annex A (informative) Sample scenario showing the exchange of security information 23
Annex B (informative) Examples of regional specification on a few SECURITY CAPABILITIES 46
Annex C (informative) SECURITY CAPABILITY mapping to C-I-A-A 50
Bibliography 51

Table 1 – Relationship of IT security and ISO 14971-based terminology 8
Table C.1 – Sample mapping by a hypothetical HDO 50

Documents
Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

Glossary of equivalent standards

International Standards adopted in the United States may include normative references to other International Standards. For each International Standard that has been adopted by AAMI (and ANSI), the table below gives the corresponding U.S. designation and level of equivalency to the International Standard. NOTE: Documents are sorted by international designation. The code in the US column, "(R)20xx" indicates the year the document was officially reaffirmed by AAMI. E.g., ANSI/AAMI/ISO 10993-4:2002/(R)2009 indicates that 10993-4, originally approved and published in 2002, was reaffirmed without change in 2009.

Other normatively referenced International Standards may be under consideration for U.S. adoption by AAMI; therefore, this list should not be considered exhaustive.

International designation	U.S. designation	Equivalency
IEC 60601-1:2005 IEC 60601-1:2005/A1:2012 IEC Technical Corrigendum 1 and 2	ANSI/AAMI ES60601-1:2005/(R)2012 ANSI/AAMI ES60601-1:2005/A1:2012 ANSI/AAMI ES60601-1:2005/C1:2009/(R)2012 (amdt) ANSI/AAMI ES60601-1:2005/A2:2010/(R)2012	Major technical variations A1 identical C1 identical to Corrigendum 1 & 2 A2 applies to AAMI, only
IEC 60601-1-11:2010	ANSI/AAMI HA60601-1-11:2011	Major technical variations
IEC 60601-1-2:2007	ANSI/AAMI/IEC 60601-1-2:2007/(R)2012	Identical
IEC 60601-2-2:2009	ANSI/AAMI/IEC 60601-2-2:2009	Identical
IEC 60601-2-4:2010	ANSI/AAMI/IEC 60601-2-4:2010	Identical
IEC 60601-2-16:2012	ANSI/AAMI/IEC 60601-2-16:2012	Identical
IEC 60601-2-19:2009	ANSI/AAMI/IEC 60601-2-19:2009	Identical
IEC 60601-2-20:2009	ANSI/AAMI/IEC 60601-2-20:2009	Identical
IEC 60601-2-21:2009	ANSI/AAMI/IEC 60601-2-21:2009	Identical
IEC 60601-2-24:1998	ANSI/AAMI ID26:2004/(R)2009	Major technical variations
IEC 60601-2-25:2011	ANSI/AAMI/IEC 60601-2-25:2011	Identical
IEC 60601-2-27:2011	ANSI/AAMI/IEC 60601-2-27:2011	Identical
IEC 60601-2-47:2012	ANSI/AAMI/IEC 60601-2-47:2012	Identical
IEC 60601-2-50:2009	ANSI/AAMI/IEC 60601-2-50:2009	Identical
IEC/TR 60878:2009	ANSI/AAMI/IEC TIR60878:2003	Identical
IEC/TR 61289:2011	ANSI/AAMI/IEC TIR61289:2011	Identical
IEC/TR 62296:2009	ANSI/AAMI/IEC TIR62296:2009	Identical
IEC 62304:2006	ANSI/AAMI/IEC 62304:2006	Identical
IEC/TR 62348:2006	ANSI/AAMI/IEC TIR62348:2006	Identical
IEC/TR 62354:2009	ANSI/AAMI/IEC TIR62354:2009	Identical
IEC 62366:2007	ANSI/AAMI/IEC 62366:2007	Identical
IEC 80001-1:2010	ANSI/AAMI/IEC 80001-1:2010	Identical
IEC/TR 80001-2-1:2012	ANSI/AAMI/IEC 80001-2-1:2012	Identical
IEC/TR 80001-2-2:2012	ANSI/AAMI/IEC 80001-2-2:2012	Identical
IEC/TR 80001-2-3:2012	ANSI/AAMI/IEC 80001-2-3:2012	Identical
IEC/TR 80002-1:2009	ANSI/IEC/TR 80002-1:2009	Identical
IEC 80601-2-30:2009 and Technical Corrigendum 1	ANSI/AAMI/IEC 80601-2-30:2009 and ANSI/AAMI/IEC 80601-2-30:2009/C1:2009 (amdt) – consolidated text	Identical (with inclusion) C1 Identical to Corrigendum 1
IEC 80601-2-58:2008	ANSI/AAMI/IEC 80601-2-58:2008	Identical
ISO 5840:2005	ANSI/AAMI/ISO 5840:2005/(R)2010	Identical
ISO 7198:1998	ANSI/AAMI/ISO 7198:1998/2001/(R)2010	Identical
ISO 7199:2009 and Amendment 1:2012	ANSI/AAMI/ISO 7199:2009 and Amendment 1:2012	Identical
ISO 8637:2010	ANSI/AAMI/ISO 8637:2010	Identical
ISO 8638:2010	ANSI/AAMI/ISO 8638:2010	Identical

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

International designation	U.S. designation	Equivalency
ISO 10993-1:2009	ANSI/AAMI/ISO 10993-1:2009	Identical
ISO 10993-2:2006	ANSI/AAMI/ISO 10993-2:2006/(R)2010	Identical
ISO 10993-3:2003	ANSI/AAMI/ISO 10993-3:2003/(R)2009	Identical
ISO 10993-4:2002 and Amendment 1:2006	ANSI/AAMI/ISO 10993-4:2002/(R)2009 and Amendment 1:2006/(R)2009	Identical
ISO 10993-5:2009	ANSI/AAMI/ISO 10993-5:2009	Identical
ISO 10993-6:2007	ANSI/AAMI/ISO 10993-6:2007/(R)2010	Identical
ISO 10993-7:2008	ANSI/AAMI/ISO 10993-7:2008/(R)2012	Identical
ISO 10993-9:2009	ANSI/AAMI/ISO 10993-9:2009	Identical
ISO 10993-10:2010	ANSI/AAMI/ISO 10993-10:2010	Identical
ISO 10993-11:2006	ANSI/AAMI/ISO 10993-11:2006/(R)2010	Identical
ISO 10993-12:2012	ANSI/AAMI/ISO 10993-12:2012	Identical
ISO 10993-13:2010	ANSI/AAMI/ISO 10993-13:2010	Identical
ISO 10993-14:2001	ANSI/AAMI/ISO 10993-14:2001/(R)2006	Identical
ISO 10993-15:2000	ANSI/AAMI/ISO 10993-15:2000/(R)2006	Identical
ISO 10993-16:2010	ANSI/AAMI/ISO 10993-16:2010	Identical
ISO 10993-17:2002	ANSI/AAMI/ISO 10993-17:2002/(R)2008	Identical
ISO 10993-18:2005	ANSI/AAMI BE83:2006/(R)2011	Major technical variations
ISO/TS 10993-19:2006	ANSI/AAMI/ISO TIR10993-19:2006	Identical
ISO/TS 10993-20:2006	ANSI/AAMI/ISO TIR10993-20:2006	Identical
ISO 11135-1:2007	ANSI/AAMI/ISO 11135-1:2007	Identical
ISO/TS 11135-2:2008	ANSI/AAMI/ISO TIR11135-2:2008	Identical
ISO 11137-1:2006	ANSI/AAMI/ISO 11137-1:2006/(R)2010	Identical
ISO 11137-2:2012	ANSI/AAMI/ISO 11137-2:2012	Identical
ISO 11137-3:2006	ANSI/AAMI/ISO 11137-3:2006/(R)2010	Identical
ISO 11138-1:2006	ANSI/AAMI/ISO 11138-1:2006/(R)2010	Identical
ISO 11138-2:2006	ANSI/AAMI/ISO 11138-2:2006/(R)2010	Identical
ISO 11138-3:2006	ANSI/AAMI/ISO 11138-3:2006/(R)2010	Identical
ISO 11138-4:2006	ANSI/AAMI/ISO 11138-4:2006/(R)2010	Identical
ISO 11138-5:2006	ANSI/AAMI/ISO 11138-5:2006/(R)2010	Identical
ISO/TS 11139:2006	ANSI/AAMI/ISO 11139:2006	Identical
ISO 11140-1:2005	ANSI/AAMI/ISO 11140-1:2005/(R)2010	Identical
ISO 11140-3:2007	ANSI/AAMI/ISO 11140-3:2007/(R)2012	Identical
ISO 11140-4:2007	ANSI/AAMI/ISO 11140-4:2007/(R)2012	Identical
ISO 11140-5:2007	ANSI/AAMI/ISO 11140-5:2007/(R)2012	Identical
ISO 11607-1:2006	ANSI/AAMI/ISO 11607-1:2006/(R)2010	Identical
ISO 11607-2:2006	ANSI/AAMI/ISO 11607-2:2006/(R)2010	Identical
ISO 11658:2012	ANSI/AAMI/ISO 11658:2012	Identical
ISO 11663:2009	ANSI/AAMI/ISO 11633:2009	Identical
ISO 11737-1:2006	ANSI/AAMI/ISO 11737-1:2006	Identical
ISO 11737-2:2009	ANSI/AAMI/ISO 11737-2:2009	Identical
ISO/TS 12417:2011	ANSI/AAMI/ISO TIR12417:2011	Identical
ISO 13022:2012	ANSI/AAMI/ISO 13022:2012	Identical
ISO 13408-1:2008	ANSI/AAMI/ISO 13408-1:2008/(R)2011	Identical
ISO 13408-2:2003	ANSI/AAMI/ISO 13408-2:2003	Identical
ISO 13408-3:2006	ANSI/AAMI/ISO 13408-3:2006	Identical
ISO 13408-4:2005	ANSI/AAMI/ISO 13408-4:2005	Identical
ISO 13408-5:2006	ANSI/AAMI/ISO 13408-5:2006	Identical
ISO 13408-6:2006	ANSI/AAMI/ISO 13408-6:2006	Identical

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

International designation	U.S. designation	Equivalency
ISO 13408-7:2012	ANSI/AAMI/ISO 13408-7:2012	Identical
ISO 13485:2003	ANSI/AAMI/ISO 13485:2003/(R)2009	Identical
ISO 13958:2009	ANSI/AAMI/ISO 13958:2009	Identical
ISO 13959:2009	ANSI/AAMI/ISO 13959:2009	Identical
ISO 14155:2011	ANSI/AAMI/ISO 14155:2011	Identical
ISO 14160:2011	ANSI/AAMI/ISO 14160:2011	Identical
ISO 14161:2009	ANSI/AAMI/ISO 14161:2009	Identical
ISO 14708-3:2008	ANSI/AAMI/ISO 14708-3:2008	Identical
ISO 14708-4:2008	ANSI/AAMI/ISO 14708-4:2008	Identical
ISO 14708-5:2010	ANSI/AAMI /ISO 14708-5:2010	Identical
ISO 14937:2009	ANSI/AAMI/ISO 14937:2009	Identical
ISO/TR 14969:2004	ANSI/AAMI/ISO TIR14969:2004	Identical
ISO 14971:2007	ANSI/AAMI/ISO 14971:2007/(R)2010	Identical
ISO 15223-1:2012	ANSI/AAMI/ISO 15223-1:2012	Identical
ISO 15223-2:2010	ANSI/AAMI/ISO 15223-2:2010	Identical
ISO 15225:2010	ANSI/AAMI/ISO 15225:2010	Identical
ISO 15674:2009	ANSI/AAMI/ISO 15674:2009	Identical
ISO 15675:2009	ANSI/AAMI/ISO 15675:2009	Identical
ISO 15882:2008	ANSI/AAMI/ISO 15882:2008	Identical
ISO 15883-1:2006	ANSI/AAMI ST15883-1:2009 and A2:2012	Major technical variations
ISO/TR 16142:2006	ANSI/AAMI/ISO TIR16142:2005	Identical
ISO 17664:2004	ANSI/AAMI ST81:2004	Major technical variations
ISO 17665-1:2006	ANSI/AAMI/ISO 17665-1:2006	Identical (with inclusions)
ISO/TS 17665-2:2009	ANSI/AAMI/ISO TIR17665-2:2009	Identical
ISO 18472:2006	ANSI/AAMI/ISO 18472:2006/(R)2010	Identical
ISO/TS 19218-1:2011	ANSI/AAMI/ISO TIR19218-1:2011	Identical
ISO 20857:2010	ANSI/AAMI/ISO 20857:2010	Identical
ISO 22442-1:2007	ANSI/AAMI/ISO 22442-1:2007	Identical
ISO 22442-2:2007	ANSI/AAMI/ISO 22442-2:2007	Identical
ISO 22442-3:2007	ANSI/AAMI/ISO 22442-3:2007	Identical
ISO/TR 22442-4:2010	ANSI/AAMI/ISO TIR22442-4:2010	Identical
ISO 23500:2011	ANSI/AAMI/ISO 23500:2011	Identical
ISO/TS 23810:2012	ANSI/AAMI/ISO TIR23810:2012	Identical
ISO 25539-1:2003 and A1:2005	ANSI/AAMI/ISO 25539-1:2003/(R)2009 and A1:2005/(R)2009	Identical
ISO 25539-2:2008	ANSI/AAMI/ISO 25539-2:2008	Identical
ISO 25539-3:2011	ANSI/AAMI/ISO 25539-3:2011	Identical
ISO 26722:2009	ANSI/AAMI/ISO 26722:2009	Identical
ISO 27185:2012	ANSI/AAMI/ISO 27185:2012	Identical
ISO 27186:2010	ANSI/AAMI/ISO 27186:2010	Identical
ISO 80369-1:2010	ANSI/AAMI/ISO 80369-1:2010	Identical
ISO 81060-1:2007	ANSI/AAMI/ISO 81060-1:2007	Identical
ISO 81060-2:2009	ANSI/AAMI/ISO 81060-2:2009	Identical

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

Committee representation

Association for the Advancement of Medical Instrumentation

Information Technology Working Group

The adoption of IEC/TR 80001-2-2 as a new AAMI/IEC Technical Information Report was initiated by the AAMI Information Technology Working Group. U.S. cochairs of AAMI/SM/WG 02, William Hintz of Medtronic, Inc. and Richard Schrenker of Massachusetts General Hospital, played an active part in developing the IEC Technical Report.

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

Cochairs:
William Hintz, Medtronic Inc. WHQ Campus
Richard A. Schrenker, Massachusetts General Hospital

Members:
John T. Collins, MSEE, American Society for Healthcare Engineering
Todd Cooper, 80001 Experts (Independent Expert)
Rebecca K. Crossley, CBET, Susquehanna Health System (Independent Expert)
Conor Curtin, Fresenius Medical Care Renal Therapies Group
Yadin David, EdD CCE PE HCSP, Biomedical Engineering Consultants LLC (Independent Expert)
Karen S. Delvecchio, GE Healthcare
Christina DeMur, Draeger Medical Systems Inc.
Sherman Eagles, SoftwareCPR
Donald J. Fournier, Draeger Medical Systems Inc.
Joseph Freitas, CareFusion
Kenneth J. Fuchs, Mindray DS USA Inc.
George W. Gray, Fluidnet Corporation
Thomas Grobaski, Belimed Inc
William Hintz, Medtronic Inc. WHQ Campus
Yimin Li, Stryker Instruments Division
Marshall Magee, Welch Allyn Inc.
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, St Jude Medical Inc.
Tresia L. O'Shea, Getinge USA
Geoffrey A. Pascoe, MSCCS BEE GSEC, (Independent Expert)
Steven R. Rakitin, Software Quality Consulting (Independent Expert)
Terrie L. Reed, MSIE, FDA/CDRH
Richard A. Schrenker, Massachusetts General Hospital
Bob Steurer, Spacelabs Medical Inc.
Micheal T. Suelzer, PhD, Baxter Healthcare Corporation
Donna-Bea Tillman, PhD, (Independent Expert)
Daidi Zhong, PhD, Chongqing University (Independent Expert)

Alternates:
James Dundon, Spacelabs Medical Inc.
Brian J. Fitzgerald, Eur Ing MIMM, FDA/CDRH
Thomas W. Schultz, Medtronic Inc WHQ Campus
Xianyu Shea, Stryker Instruments Division
Fei Wang, Fresenius Medical Care Renal Therapies Group

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.

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

Background of ANSI/AAMI adoption of IEC/TR 80001-2-2:2012

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

International technical report IEC/TR 80001-2-2:2012 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 is organized through the U.S. Technical Advisory Group for IEC/SC 62A administered by the Advanced Medical Technology Association (AdvaMed) on behalf of the American National Standards Institute. AAMI administers the International Secretariat for IEC/SC 62A on behalf of the United States, and U.S. experts made a considerable contribution to this International Technical Report.

AAMI encourages its committees to harmonize their work with International Standards in the area of risk management of information technology as it relates to medical devices. The AAMI Information Technology Working Group together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC/TR 80001-2-2 to formulate the U.S. position and comments 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, AdvaMed granted AAMI permission to consider adoption of IEC/TR 80001-2-2 as a new AAMI Technical Information Report. Following AAMI procedures, the AAMI Information Technology Working Group voted to adopt the IEC technical report as written.

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

The concepts incorporated in this technical information 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.

As used within the context of this document, “should” indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action should be avoided but is not prohibited. “May” is used to indicate that a course of action is permissible within the limits of the technical information report. “Can” is used as a statement of possibility and capability. Finally, “must” is used only to describe “unavoidable” situations, including those mandated by government regulation.

Suggestions for improving this document are invited. Comments and suggested revisions should be sent to Standards Department, AAMI, 4301 N. Fairfax Dr. Suite 301, Arlington, VA 22203-1633.

NOTE- Beginning with the IEC foreword on page xi, this AAMI Technical Information Report is identical to IEC/TR 80001-2-2:2012.

© 2012 Association for the Advancement of Medical Instrumentation ANSI/AAMI/IEC TR80001-2-2:2012

Documents
Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-2, which is a technical report, has been prepared a Joint Working Group of subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62*:* Electrical equipment in medical practice and ISO technical committee 215: Health informatics.

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
62A/783/DTR	62A/807/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'color inside' logo on the cover page of this publication indicates that it contains colors which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a color printer.

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

INTRODUCTION

IEC 80001-1, which deals with the application of RISK MANAGEMENT to IT-networks incorporating medical devices, provides the roles, responsibilities and activities necessary for RISK MANAGEMENT. This technical report provides additional guidance in how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT PROCESS and stakeholder communications and agreements.

The informative set of common, high-level SECURITY CAPABILITIES presented here i intended to be the starting point for a security-centric discussion between vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sized RESPONSIBLE ORGANIZATIONS as each evaluates RISK under the capabilities and decides what to include or not include according to its RISK tolerance and resource planning. This technical report might be used in the preparation of documentation designed to communicate product SECURITY CAPABILITIES and options. This documentation could be used by the RESPONSIBLE ORGANIZATION as input to their IEC 80001 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. Other IEC-80001-1 technical reports will provide step-by-step guidance in the RISK MANAGEMENT PROCESS. Furthermore, the SECURITY CAPABILITIES encourage the disclosure of more detailed security controls – perhaps those specified in one or more security standards as followed by the RESPONSIBLE ORGANIZATION or the MEDICAL-DEVICE manufacturer (for example, ISO 27799:2008, ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2011, the ISO 22600 series, the ISO 13606 series, and ISO/HL7 10781:2009, which covers the Electronic Health Record System Functional Model). This report remains agnostic as to the underlying controls framework; it only proposes a structure for the disclosure and communication among the RESPONSIBLE ORGANIZATION (here called the healthcare delivery organization – HDO), the MEDICAL DEVICE manufacturer (MDM) and the IT-vendor.

The capabilities outlined here comprise a disclosure set of controls which support the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity or system/data availability. Capabilities can be added to or further elaborated as the need arises. Controls are intended to protect both data and systems but special attention is given to the protection of both PRIVATE DATA and its subset called HEALTH DATA. Both of these special terms have been defined to carefully avoid any law-specific references (e.g., EC Sensitive Data or USA ePHI).

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

Documents
Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

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

1 Scope

This part of IEC 80001 creates a framework for the disclosure of security-related capabilities and RISKS necessary for managing the RISK in connecting MEDICAL DEVICES to IT-NETWORKS and for the security dialog that surrounds the IEC 80001-1 RISK MANAGEMENT of IT-NETWORK connection. This security report presents an informative set of common, high-level security-related capabilities useful in understanding the user needs, the type of security controls to be considered and the RISKS that lead to the controls. INTENDED USE and local factors determine which exact capabilities will be useful in the dialog about RISK.

The capability descriptions in this report are intended to supply:

a) health delivery organizations (HDOs),

b) MEDICAL DEVICE manufacturers (MDMs), and

c) IT vendors

with a basis for discussing RISK and their respective roles and responsibilities toward its management. This discussion among the RISK partners serves as the basis for one or more RESPONSIBILITY AGREEMENTS as specified in IEC 80001-1.

The present report provides broad descriptions of the security-related capabilities with the intent that any particular device or use of a device will have to have at least one additional level of specification detail under each capability. This will often be site and application-specific and may invoke RISK and security controls standards as applicable.

At this introductory stage of IEC 80001-1 standardization, the SECURITY CAPABILITIES in this report provide a common, simple classification of security controls particularly suited to MEDICAL IT NETWORKS and the incorporated devices. The list is not intended to constitute or to support rigorous IT security standards-based controls and associated programs of certification and assurance such as might be found in other ISO standards (e.g., ISO/IEC 15408 with its Common Criteria for Information Technology Security Evaluation). The present report does not contain sufficient detail for exact specification of requirements in a request for proposal or product security disclosure sheet. However, the classification and structure can be used to organize such requirements with underlying detail sufficient for communication during the purchase and integration PROCESS for a MEDICAL DEVICE or IT equipment component. Again, this report is intended to act as a basis for discussion and agreement sufficient to initial integration project RISK MANAGEMENT. Additionally, security only exists in the context of the organizational security policies. Both:

a) the security policies of the healthcare delivery organization (HDO), and

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

b) the product and services security policies of the MEDICAL DEVICE manufacturer (MDM)

are outside of the scope of this report. In addition, the Technical Report does not address clinical studies where there is a need for securing the selective disclosure of PRIVATE DATA or HEALTH DATA.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) 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
DATA AND SYSTEMS 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, definition 2.5, modified — two notes integral to understanding the scope of the original definition have been deleted.]

3.2
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, definition 2.6]

3.3
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, definition 2.7]

3.4
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, definition 2.8]

3.5
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, definition 2.9]

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

3.6
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD(s)

[SOURCE: ISO 14971:2007, definition 2.4]

3.7
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This generically defines PRIVATE DATA and it subset, HEALTH DATA, within this document to permit users of this document to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to "Personal Data" and "Sensitive Data"; in the USA, HEALTH DATA might be changed to "Protected Health Information (PHI)" while making adjustments to text as necessary.

3.8
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

[SOURCE: IEC 80001-1:2010, definition 2.10]

3.9
INTEROPERABILITY
a property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, definition 2.11]

3.10
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
a system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, definition 2.12, modified – the two notes to the original definition have not been retained.]

3.11
KEY PROPERTIES
three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, definition 2.13]

3.12
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:

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g

– 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);
– 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, definition 2.14]

3.13
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, definition 2.16]

3.14
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, definition 2.18]

3.15
PRIVATE DATA
any information relating to an identified or identifiable person

© 2012 Association for the Advancement of Medical Instrumentation ANSI/AAMI/IEC TIR80001-2-2:2012

Documents Document Sharing Hub

Copyright Association for the Advancement of Medical Instrumentation

Full document details: n etworks i n co rp ora ti n g

3.16
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, definition 2.19]

3.17
RESIDUAL RISK
RISK remaining after RISK CONTROL measures have been taken

[SOURCE: IEC 80001-1:2010, definition 2.20]

3.18
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

[SOURCE: IEC 80001-1:2010, definition 2.21, modified – a note to the original definition, containing examples, has not been retained.]

3.19
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry: In this Technical Report, to avoid confusion associated with the notion of security responsibility, the RESPONSIBLE ORGANIZATION of IEC 80001-1 is given the name healthcare delivery organization (HDO).

[SOURCE: IEC 80001-1:2010, definition 2.22, modified — a note to the original definition, containing examples, has not been retained; a note to entry has been added.]

3.20
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, definition 2.23]

3.21
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, definition 2.24]

3.22
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, definition 2.25]

3.23
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: IEC 80001-1:2010, definition 2.26]

Documents Document Sharing Hub
Copyright Association for the Advancement of Medical Instrumentation
Full document details: n etworks i n co rp ora ti n g