

# 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



# **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

*Published by*

Association for the Advancement of Medical Instrumentation  
4301 N. Fairfax Drive, Suite 301  
Arlington, VA 22203-1633  
[www.aami.org](http://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](http://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

This is a preview. Click here to purchase the full publication.

## 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.

# 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

8.5	<a href="http://www.cchit.org/get_certified">http://www.cchit.org/get_certified</a> HL7 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

## 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