IEC/TR 80001-2-2

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XA

ICS 11.040.01

ISBN 978-2-83220-202-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 8
3 Terms and definitions 8
4 Use of SECURITY CAPABILITIES 12
4.1 Structure of a SECURITY CAPABILITY entry 12
4.2 Guidance for use of SECURITY CAPABILITIES in the RISK MANAGEMENT PROCESS 12
4.3 Relationship of ISO 14971-based RISK MANAGEMENT to IT security RISK MANAGEMENT 13
5 SECURITY CAPABILITIES 14
5.1 Automatic logoff – ALOF 14
5.2 Audit controls – AUDT 14
5.3 Authorization – AUTH 15
5.4 Configuration of security features – CNFS 16
5.5 Cyber security product upgrades – CSUP 16
5.6 HEALTH DATA de-identification – DIDT 17
5.7 Data backup and disaster recovery – DTBK 17
5.8 Emergency access – EMRG 17
5.9 HEALTH DATA integrity and authenticity – IGAU 18
5.10 Malware detection/protection – MLDP 18
5.11 Node authentication – NAUT 18
5.12 `Person authentication – PAUT 19
5.13 Physical locks on device – PLOK 19
5.14 Third-party components in product lifecycle roadmaps – RDMP 20
5.15 System and application hardening – SAHD 20
5.16 Security guides – SGUD 21
5.17 HEALTH DATA storage confidentiality – STCF 21
5.18 Transmission confidentiality – TXCF 22
5.19 Transmission integrity – TXIG 22
6 Example of detailed specification under SECURITY CAPABILITY: Person authentication – PAUT 22
7 References 23
8 Other resources 25
8.1 General 25
8.2 Manufacture disclosure statement for medical device security (MDS2) 25
8.3 Application security questionnaire (ASQ) 25
8.4 The Certification Commission for Healthcare Information Technology (CCHIT) 25
8.5 http://www.cchit.org/get_certifiedHL7 Functional Electronic Health Record (EHR) 26
8.6 Common criteria – ISO/IEC 15408 26
9 Standards and frameworks 26
Annex A (informative) Sample scenario showing the exchange of security information 27
Annex B (informative) Examples of regional specification on a few SECURITY CAPABILITIES 48

Annex C (informative) SECURITY CAPABILITY mapping to C-I-A-A 52
Bibliography 53

Table 1 – Relationship of IT security and ISO 14971-based terminology 13
Table C.1 – Sample mapping by a hypothetical HDO 52

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.

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

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).

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

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*