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

IEC/TR 80001-2-2:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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

CONTENTS

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*

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]

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:
   - 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

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, containg 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]

3.24
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[SOURCE: IEC 80001-1:2010, definition 2.27]

3.25
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

[SOURCE: IEC 80001-1:2010, definition 2.28]

3.26
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 80001-1:2010, definition 2.30]

3.27
SECURITY CAPABILITY
broad category of technical, administrative or organizational controls to manage RISKS to confidentiality, integrity, availability and accountability of data and systems

3.28
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

[SOURCE: IEC 80001-1:2010, definition 2.32, modified – three notes to the original definition have not been retained.]

4 Use of SECURITY CAPABILITIES

4.1 Structure of a SECURITY CAPABILITY entry

The SECURITY CAPABILITIES clause below (Clause 5) itemizes the common SECURITY CAPABILITIES that can be included in a MEDICAL DEVICE or IT component. Four letter abbreviations are suggested for each capability as a convenience to reference and tabulation. Each section provides a broad view of a potentially applicable security control or PROCESS category. Each capability description contains:

– references to source material that informs the capability (i.e., applicable standards, policies and reference materials – here, the HDO and MDM should consider international security standards as well as applicable country-based standards such as the security elements present in NIST 800-39/53/66/... (US), NEN 7510 (NL), ASIP requirements (FR), Personal Information Protection Law & Guideline for Medical Information System Safety Management (JP), etc.);
– the fundamental security goal of the capability (i.e., requirement goal); and
– a statement of user (healthcare provider) need for the capability.

Often, the listed SECURITY CAPABILITIES form the basis for discussion among RESPONSIBILITY AGREEMENT participants. This discussion and eventual agreement(s) are intended to address features, roles, and responsibilities among stakeholders regarding security RISKS.

4.2 Guidance for use of SECURITY CAPABILITIES in the RISK MANAGEMENT PROCESS

All SECURITY CAPABILITIES are potential security RISK CONTROL options. The selection of a security RISK CONTROL option follows after identifying the need for mitigation of a security RISK. See IEC/TR 80001-2-1:2012, for step-by-step details of the RISK MANAGEMENT PROCESS where the selection, implementation and VERIFICATION of RISK CONTROLS are performed from steps 6 though to 8.

The SECURITY CAPABILITIES address security RISK CONTROL options as follows:

– The ‘requirement goal’ lists the potential security RISKS that can be addressed using that SECURITY CAPABILITY.
– The ‘user need’ section contains information on possible aspects that need to be considered when using this SECURITY CAPABILITY

It is essential that the reader understand that a specific security solution developed for a particular device in one use scenario might be inappropriate in another. The INTENDED USE of the MEDICAL DEVICE when incorporated into the MEDICAL IT-NETWORK informs the selection of which capabilities and at what level they should be supported. Sometimes this leads to important inclusion of SECURITY CAPABILITIES, for example, the use of user names and passwords on network-connected devices that contain patient data. Other times, the context of the INTENDED USE excludes a whole class of security controls; for example, a small, embedded software device like a SPO_2 monitor has little use for embedded security audit trails on the device itself. Security requirements applicable in the context of a specific INTENDED USE and in a specific environment should never be adopted without consideration of their potential impact on SAFETY and EFFECTIVENESS of the product.

4.3 Relationship of ISO 14971-based RISK MANAGEMENT to IT security RISK MANAGEMENT

For information on applying security RISK MANAGEMENT at the organizational level see ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27799:2008. For the incorporation of a MEDICAL DEVICE onto an IT-NETWORK, some may choose to use ISO/IEC 27005:2011 for IT security RISK MANAGEMENT PROCESSES that can be adapted to complement the ISO 14971-based RISK MANAGEMENT PROCESS in IEC 80001-1:2010 (i.e., SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY). See the step-by-step technical report IEC/TR 80001-2-1:2012 for more detail on how to carry out RISK MANAGEMENT.

IEC 80001-1:2010 includes in the definition of HARM the KEY PROPERTIES of SAFETY, EFFECTIVENESS, and the breach of DATA AND SYSTEMS SECURITY. The HARM qualifying phrase "…breach of DATA AND SYSTEMS SECURITY" is equivalent to an executed exploit in the domain of IT security (e.g., cyber security). In the treatment of HAZARDS in IT security, a system vulnerability may lead to a breach event (via an exploit). In similar manner, a threat is anything that poses danger to DATA AND SYSTEMS SECURITY. This parallels a HAZARD as a potential source of HARM. Simply put, threats utilize vulnerabilities that can result in an exploit (known potential for HARM) or as noted in ISO/IEC 27005:2011, "Information security RISK is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause HARM to an organization."

This technical report uses security and RISK-related terms from both the IT and the traditional MEDICAL DEVICE (ISO 14971-based) RISK MANAGEMENT worlds. Table 1 can be used to relate both the IT security and ISO 14971-based terminology – it is inexact but aligns the concepts.

Table 1 – Relationship of IT security and ISO 14971-based terminology

IT security RISK MANAGEMENT	ISO 14971-based RISK MANAGEMENT
Vulnerability – recognized exposure that, in the presence of a threat, can lead to a reduction of data or systems information assurance	An attribute of a system that creates the potential for HARM (specifically to data and systems), i.e., a HAZARD arising from an attribute that is demonstrably exploitable (in IT terms).
Threat – something (either intentional or accidental) that can cause HARM to systems and organizations.	A circumstance or event that could lead to HARM, i.e., a HAZARD arising from a vulnerability plus the potentially activating circumstance or event (in IT, often involving a threat agent).
Exposure – situation that can cause HARM	HAZARDOUS SITUATION
Exploit (noun) – software or command(s) that breaches security *Threat + Vulnerability + "activation" → HARM*	instance of HARM *HAZARD+ HAZARDOUS SITUATION + "sequence of events" → HARM*
RISK – effect of uncertainty on objectives [ISO/IEC 27005:2011]	RISK – combination of the probability of occurrence of HARM and the severity of that HARM [ISO 14971:2007]
Countermeasures, safeguards, security controls	RISK CONTROL options (in IT, sometimes called mitigations in when rationalized by RISK ANALYSIS)
Compromise to confidentiality, integrity, or availability of systems or data (includes privacy breach)	HARM