IEC TS 81001-2-2

Edition 1.0 2025-09

INTERNATIONAL STANDARD

Health software and health IT systems safety, effectiveness and security - Part 2-2: Coordination - Guidance for the implementation, disclosure and communication of security needs, risks and controls

ICS 11.040.01; 35.240.80

ISBN 978-2-8327-0739-5

IEC TS 81001-2-2:2025-09(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2025 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC 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: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

CONTENTS

FOREWORD ... 3
INTRODUCTION ... 5
1 Scope ... 7
2 Normative references ... 8
3 Terms and definitions ... 8
4 Use of security capabilities ... 9
4.1 Structure of a *security capability* entry ... 9
4.2 Guidance on the communication of *security* capabilities and shared responsibility ... 9
4.3 Guidance for use of *security* capabilities in the *risk management process* ... 9
4.4 Guidance on the application of *risk management processes* ... 9
5 Security capabilities ... 10
5.1 General ... 10
5.2 Automatic logoff (ALOF) ... 11
5.3 Audit controls (AUDT) ... 11
5.4 Authorization (AUTH) ... 12
5.5 Cybersecurity product upgrades (CSUP) ... 13
5.6 Health data de-identification (DIDT) ... 14
5.7 Data backup and disaster recovery (DTBK) ... 15
5.8 Emergency access (EMRG) ... 15
5.9 Health data integrity and authenticity (IGAU) ... 16
5.10 Malware detection/protection (MLDP) ... 16
5.11 Node authentication (NAUT) ... 17
5.12 Person authentication (PAUT) ... 18
5.13 Physical locks on product (PLOK) ... 19
5.14 Third-party components in product life cycle roadmaps (RDMP) ... 19
5.15 System and application hardening (SAHD) ... 20
5.16 Health data storage confidentiality (STCF) ... 20
5.17 Transmission confidentiality (TXCF) ... 21
5.18 Transmission integrity and authenticity (TXIG) ... 21
6 Additional supporting information ... 21
6.1 General ... 21
6.2 Connectivity capabilities (CONN) ... 22
6.3 Management of personally identifiable information (MPII) ... 22
6.4 Remote services (RMOT) ... 23
6.5 Software Bill of Materials (SBOM) ... 24
6.6 *Security* guides (SGUD) ... 25
7 Examples of some *security* capabilities ... 25
7.1 Example of detailed specification under *security capability*: Person authentication (PAUT) ... 25
7.2 Example for Software Bill of Materials (SBOM) ... 26
8 References and other resources ... 27
8.1 General ... 27
8.2 *Manufacturer* disclosure statement for *medical device security* (MDS2) ... 28
8.3 Application *security* questionnaire (ASQ) ... 28
8.4 HL7 Functional Electronic Health Record (EHR) ... 28

8.5 Standards and frameworks 28
Annex A (informative) Sample scenario showing the exchange of security information 31
A.1 Introduction to the *security* characteristics scenario 31
A.2 Manufacturer Disclosure Statement for Medical device Security (MDS2) 32
Annex B (informative) Examples of regional specification on a few *security* capabilities 46
Annex C (informative) Guidance for selecting *security control*s to satisfy the *security* capabilities 49
C.1 General 49
C.2 Automatic logoff (ALOF) 52
C.3 Audit controls (AUDT) 53
C.4 Authorization (AUTH) 55
C.5 Cybersecurity product upgrades (CSUP) 58
C.6 Health data de-identification (DIDT) 59
C.7 Data backup and disaster recovery (DTBK) 61
C.8 Emergency access (EMRG) 63
C.9 Health data integrity and authenticity (IGAU) 64
C.10 Malware detection/protection (MLDP) 66
C.11 Node authentication (NAUT) 69
C.12 Person authentication (PAUT) 72
C.13 Physical locks on product (PLOK) 74
C.14 Third-party components in product life cycle roadmaps (RDMP) 76
C.15 System and application hardening (SAHD) 78
C.16 Health data storage confidentiality (STCF) 82
C.17 Transmission confidentiality (TXCF) 84
C.18 Transmission integrity and authenticity (TXIG) 86
C.19 Connectivity capabilities (CONN) 87
C.20 Management of personally identifiable information (MPII) 89
C.21 Remote services (RMOT) 90
C.22 Software Bill of Materials (SBOM) 92
C.23 Security guides (SGUD) 93
Annex D (informative) *Security capability* and additional *security* information mapping to C-I-A-A-A 97
Bibliography 99
Alphabetized index of defined terms 103

Figure 1 – *Health software* Field of Application as shown in IEC 81001-5-1 [3] 7
Figure 2 – Sample Structure for "*Medical device*2" 26

Table 1 – Example SBOM for "Medical device2" 27
Table D.1 – Sample mapping by a hypothetical *HDO* 97

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

Health software and health it systems safety, effectiveness and security - Part 2-2: Coordination - Guidance for the implementation, disclosure and communication of 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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 81001-2-2 has been prepared by subcommittee 62A: Common aspects of electrical equipment, software, and systems, of IEC technical committee 62: Medical equipment, software, and systems and ISO technical committee 215: Health informatics. It is a Technical Specification.

This document withdraws and replaces:

– IEC TR 80001-2-2, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls*
– IEC TR 80001-2-8, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*

This document includes the following significant changes:

a) Combines and updates the contents of IEC TR 80001-2-2 and IEC TR 80001-2-8;
b) Extends the scope to *health software* instead to only *medical device* software;
c) Aligns contents and definitions to ISO 81001-1:2021 and the updated IEC 80001-1;
d) Removed the Configuration of Security Features (CNFS) capability, as any configurable *security capability* shall be clearly communicated.
e) Provide *security control* mappings to several new standards, e.g. IEC TR 60601-4-5, IEC 62443-4-2, ISO/IEEE 11073-40102 and the recent versions of previous standards, e.g. ISO/IEC 27002 and NIST 800-53 version 5.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
62A/1668/DTS	62A/1690/RVDTS

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

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 81001 series, published under the general title *Health software and health IT systems safety, effectiveness and security*, can be found on the IEC website.

Terms used throughout this document that have been defined in Clause 3 and the terms referenced in the alphabetical index at the end of the document appear in *italics.*

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,
– withdrawn, or
– revised.

INTRODUCTION

ISO 81001-1 provides the principles, concepts, terms and definitions for *health software* and *health IT system*s, *key properties* of *safety*, *effectiveness* and *security* across the life cycle. ISO 81001-1 and all parts of the ISO 81001 and IEC 81001 series are applicable to all relevant stakeholders including *health software manufacturer*s (including *medical device manufacturer*s) and *healthcare delivery organization*s (*HDOs*). This document provides guidance on the implementation, disclosure and communication of *health software security* needs, *risks* and controls for both *health software manufacturers* (including *medical device manufacturer*) and *HDOs*.

For this document, the term "*manufacturer*" refers to the *health software manufacturer* which includes the *medical device manufacturer*. The term "user" typically refers to the *HDOs* for whom the information exchange resulting from using this document can be applied for their *risk assessments* and to establish a common understanding of the products *security* capabilities, and to further support the shared responsibility between *HDOs* and *manufacturers*.

The informative set of *security capabilities* presented are intended to be the baseline for a *security*-centric discussion between all stakeholders, including *manufacturers*, vendors, *HDOs*, procurements, etc. The level of effort is scalable across organizations of all sizes and it is crucial that it is adapted to the *risk* tolerance and the organizational goals. This document can be used across the life cycle of the *health IT system* and *health IT Infrastructure* into which the *health software* is incorporated, including:

a) administrative and technical *security control*s to protect and maintain the confidentiality, integrity, availability, authenticity, accountability and non-repudiation of data and systems,

b) documentation,

c) *risk management*,

d) shared responsibility,

e) procurement, and

f) agreements.

A *security capability* represents broad categories of technical, administrative and organizational *security controls* which are used to manage *risks* to confidentiality, integrity, availability, authenticity, accountability, non-repudiation and other characteristics, such as authorization, auditing, privacy, resilience, compliance and revocability, which are important for a comprehensive *security* of data and systems. This document presents these categories of *security controls* prescribed for a system and the operational environment to establish *security capabilities* that protect, maintain, and ensure the confidentiality, integrity and availability of data and systems. It is important to note that *security controls* for each *security capability* can be added as the need arises. Controls are intended to protect both data and systems but special attention is given to the protection of personal data and health data. Both special terms have been defined to carefully avoid any law-specific references (e.g. European special categories of personal data or sensitive data and *Personal Health Information* (PHI) in the USA).

The list is not intended to constitute or to support rigorous IT *security* standards-based controls and associated programs of certification and assurance like other ISO/IEC documents (e.g. ISO/IEC 15408 with its Common Criteria for Information Technology Security Evaluation and IEC 62443 for Security for industrial automation and control systems). This document does not contain sufficient detail for exact specification of requirements. However, the classification and structure can be used to organize such requirements with underlying detail sufficient for communication during the life cycle of *health software* or IT equipment component.

This document creates a framework for the disclosure of *security*-related capabilities necessary for managing the *risk* when implementing *health software* as a component of *health IT system*s operating on *health IT infrastructure*s and *IT Infrastructure* for *security* dialog that supports *key properties* of *safety*, *effectiveness* and *security* as conceptualized in ISO 81001-1 and other relevant *security* standards.

In addition to providing a basis for discussing *risk* and respective roles and responsibilities toward *risk management*, this document is intended to supply:

a) *HDOs* with a catalogue of management, operational and administrative *security controls* to maintain the *effectiveness* of a *security capability* for a product as a component of a *health IT system* being implemented on an organization's *health IT Infrastructure*;

b) *manufacturers* with a catalogue of technical *security controls* for the establishment of each of the *security capabilities*;

c) guidance on the communication of information on *security* capabilities between manufactures and *HDOs* as described in a sample scenario showing the exchange of *security* information (Annex A).

This document presents the *security capabilities*, their respective "requirement goal" and "user need" with a corresponding mapping of *security controls* from a number of *security* standards in Annex C.

This document remains agnostic as to the underlying controls framework. It only proposes a structure for the implementation, disclosure and communication among the *manufacturers* and other stakeholders. While this document can be used independently, it is best used in conjunction with other documents in the ISO/IEC 80001 and ISO/IEC 81001 series. Furthermore, the *security capabilities* encourage the use of more detailed *security controls* – perhaps those specified in one or more *security* standards as followed by the *HDO* or the *manufacturer*.

In this document, the conjunctive "or" is used as an "inclusive or" so a statement is true if any combination of the conditions is true.

In this document, the following verbal forms are used:

– "shall" indicates a requirement;

– "should" indicates a recommendation;

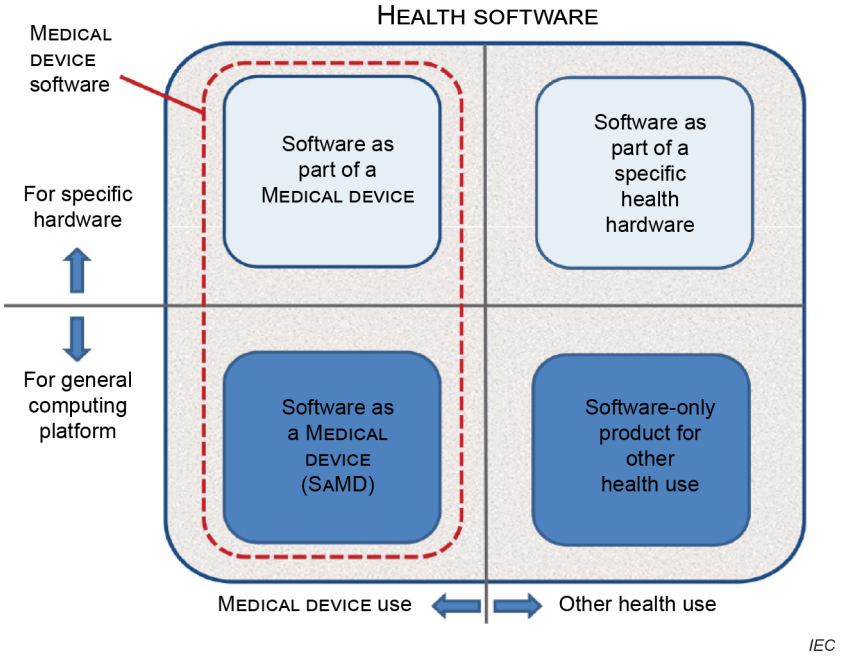
– "may" indicates a permission;

– "can" is used to describe a possibility or capability.

1 Scope

This document presents an informative set of common, high-level *security-related capabilities* and additional considerations to be used across the life cycle of *health software* and *health IT systems*, for the information exchange between the *health software manufacturers* (including *medical device manufacturers)*, *healthcare delivery organizations* (*HDOs*) and other stakeholders. It is applicable to *health software* running on any platform and in any environment such as cloud, on premise or hybrid.

Figure 1 provides a graphical representation of the *health software* which fully includes *medical device* software.



SOURCE: IEC 82304-1:2016, Figure A.1 [56]

Figure 1 – *Health software* Field of Application as shown in IEC 81001-5-1 [3][1]

While important *security* topics, the following are outside the scope of this document:

a) the *security* policies of the *HDO*,
b) the product and services *security* policies of the *manufacturer*,
c) determinations of *risk* tolerance by the *HDO* or *manufacturer*, and
d) clinical studies where there is a need to secure personal data.

As *security risks* can be caused by any product on *health IT systems* and *health IT Infrastructure*, considerations in this document can be applied for other products that are not *health software*.

[1] Numbers in square brackets refer to the Bibliography.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security - Part 1: Principles and concepts*