



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of IEC TS 81001-2-2:2025. It supersedes PD IEC/TR 80001-2-2:2012 and PD IEC/TR 80001-2-8:2016, which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 30465 7

ICS 11.040.01; 35.240.80

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2025.

Amendments/corrigenda issued since publication

Date	Text affected



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

AVA Documents
Document Sharing Hub



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 Varembe
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.



Documents

Document Sharing Hub

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 <i>security capability</i> entry	9
4.2 Guidance on the communication of <i>security capabilities</i> and shared responsibility	9
4.3 Guidance for use of <i>security capabilities</i> in the <i>risk management process</i>	9
4.4 Guidance on the application of <i>risk management processes</i>	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 <i>Security guides</i> (SGUD)	25
7 Examples of some <i>security capabilities</i>	25
7.1 Example of detailed specification under <i>security capability</i> : 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 <i>Manufacturer</i> disclosure statement for <i>medical device security</i> (MDS2)	28
8.3 Application <i>security</i> 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 <i>security</i> characteristics scenario.....	31
A.2 Manufacturer Disclosure Statement for Medical device Security (MDS2)	32
Annex B (informative) Examples of regional specification on a few <i>security</i> capabilities	46
Annex C (informative) Guidance for selecting <i>security controls</i> to satisfy the <i>security</i> 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) <i>Security capability</i> and additional <i>security</i> information mapping to C-I-A-A-A.....	97
Bibliography.....	99
Alphabetized index of defined terms	103
Figure 1 – <i>Health software</i> Field of Application as shown in IEC 81001-5-1 [3].....	7
Figure 2 – Sample Structure for “ <i>Medical device2</i> ”	26
Table 1 – Example SBOM for “ <i>Medical device2</i> ”	27
Table D.1 – Sample mapping by a hypothetical <i>HDO</i>	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 systems*, *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 manufacturers* (including *medical device manufacturers*) and *healthcare delivery organizations (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 controls* 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 systems* operating on *health IT infrastructures* 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 *manufacturers* 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.

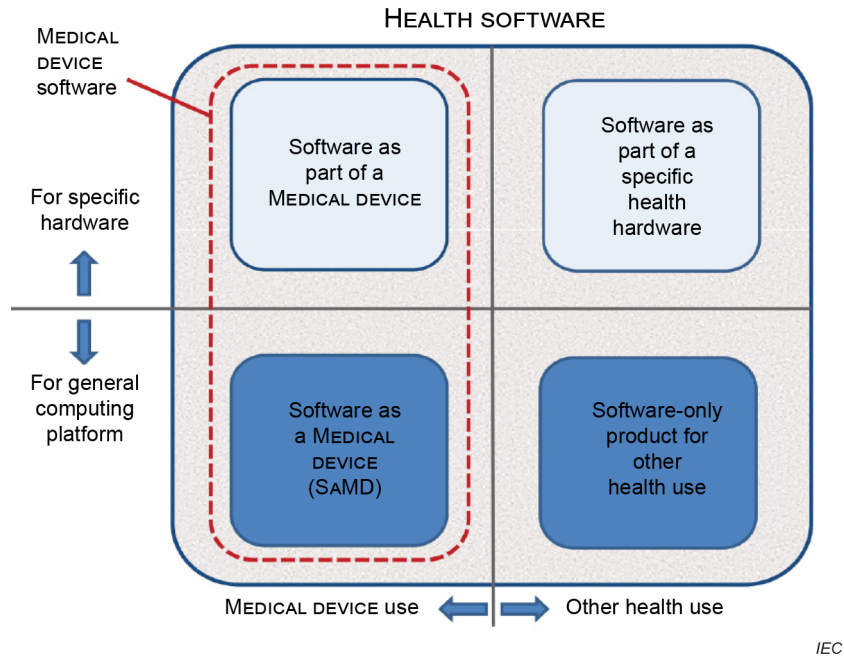
In this document, the following verbal forms are used:

- “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:

- the *security* policies of the *HDO*,
- the product and services *security* policies of the *manufacturer*,
- determinations of *risk* tolerance by the *HDO* or *manufacturer*, and
- 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*

3 Terms and definitions

All terms used in this document are provided in the Alphabetized index of defined terms. For the purposes of this document, the terms and definitions given in ISO 81001-1:2021 and the following apply. In this document, the term “product” is used in its general English meaning, and generally refers to *health software*.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1

intended environment of use

conditions and settings in which users interact with the *health software* – as specified by the *manufacturer*

[SOURCE: IEC 81001-5-1:2021 [3], 3.18]

3.2

interface

shared boundary across which products exchange information

3.3

personally identifiable information

PII

any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

[SOURCE: ISO/TS 82304-2:2021 [54], 3.1.15]

3.4

security control

measure which modifies *security risk* or use

Note 1 to entry: A *security control* can be a *process*, policy, device, practice, or other action.

[SOURCE: IEC Guide 120:2023 [55], 3.14]

4 Use of security capabilities

4.1 Structure of a *security capability* entry

Clause 4 itemizes the common *security capabilities* that can be included in the *health software*, a *medical device* or *health IT system* component. Four letter abbreviations are suggested for each capability as a convenience to reference and tabulation. Each sub-clause provides a broad view of a potentially applicable *security control* or *process* category. Each *security capability* description contains:

- references to source material that informs the *security capability* (i.e. applicable documents, policies and reference materials – here, the *HDO* and *manufacturer* should consider international *security* documents as well as applicable national documents,
- the fundamental *security* goal of the capability (i.e. requirement goal), and
- a statement of the user need for the capability.

4.2 Guidance on the communication of *security capabilities* and shared responsibility

Often, the listed *security capabilities* form the basis for the information exchange among stakeholders. This communication and eventual agreement(s) are intended to address features, roles, and responsibilities among stakeholders regarding *security risks*.

The *Manufacturer Disclosure Statement for Medical device Security* (MDS2) form [15] (Annex A) can be used as a communication tool to document and inform the user about the properties and *security capabilities* of the *health software*.

4.3 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*.

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” clause contains information on possible aspects that shall be considered when using this *security capability*.

The *intended use* and *intended environment of use* of the *health software* when incorporated into the *health IT Infrastructure* informs the selection of which *capabilities* and at what level they should be supported. This can lead to the inclusion of *security capabilities*, for example, the use of authentication on network-connected products that contain patient data. *Security* requirements applicable in the context of a specific *intended use* and in a specific *intended environment of use* should never be adopted or tailored without consideration of their potential impact on *safety* and *effectiveness* of the product.

4.4 Guidance on the application of *risk management processes*

This document uses the terms and definitions provided in ISO 81001-1:2021. As defined in ISO 81001-1, *security* and *cybersecurity* are interchangeable terms, and refer to the process of safeguarding assets in both physical and digital format. Furthermore, the definition of *security* is risk-based, referring to ISO 14971 [23] for the concept of risk, and ISO/IEC Guide 63 definitions are referred for the purpose of maintaining the *key properties of safety, effectiveness, and security*.

For *medical device manufacturers*, the *risk management process* specified in ISO 14971 has been commonly required. In its third edition, ISO 14971 clearly describes that the *processes* specified in that document are also applicable to *security* and provides guidance on *security* in ISO/TR 24971 [24]. ISO/TR 24971 describes that ISO 14971 covers *risks* related to *security*, as the definition of *harm* includes – besides damage to health – *harm* to property and the environment. Indeed, it can still be applied to *security risks* that lead to patient *harm*. This facilitates organizations to extend their existing *risk management processes* to take advantage of the ISO 14971 *risk management process* for a comprehensive approach to address *security risks* as well. In this case, *security*-related concepts should be appropriately mapped and additional *security*-related activities should be implemented under the framework of ISO 14971. In ISO/TR 24971, a *hazard* is described as, for example, a loss or degradation of confidentiality, integrity, or availability, and in a sequence of events, it is explained that a vulnerability can be *exploited* by the threats (see ISO/TR 24971:2020, Figure F.1).)

Another consideration for the application of ISO 14971 to *security risk* is shown in AAMI SW96:2023, using a *security risk management process* in parallel to the existing *safety risk management process*. However, the *process steps* are the same as those specified in ISO 14971 and *security*-specific activities are taken into account in each *process step*. For mapping the concept such as vulnerabilities, threats and *exploits*, several *risk assessment* models shown in AAMI TIR57:2016 (R2023), Annex B, and in AAMI SW96, Annex D.5, can help.

Regardless of which approach is taken, *security risks* can be addressed through the ISO 14971 *risk management process* by appropriately considering vulnerabilities, threats, and *exploits* mappings. Using the framework of ISO 14971 bears the advantage that this document addresses mutual adverse effects from *risk controls* (e.g. where *security controls* can have an adverse effect on usability and vice versa).

For those other than medical device manufacturers, the application of ISO 14971 is not required but can be used. ISO 81001-1 describes *risk management* as the *process* of identifying, assessing, controlling and monitoring *risks*. This can be implemented by *processes* other than ISO 14971. For example, IEC 80001-1 describes the application of *risk management* when an organization integrates health *IT systems* into its *health IT Infrastructure*. Its *risk management process* consists of following steps of *risk analysis* (*hazard* identification, *risk estimation*), *risk evaluation*, *risk control*, analysis of benefit-risk, *verification* of *risk control* measures and *residual risk evaluation* and reporting. This *risk management* framework is also helpful to the *health software* other than *medical devices*.

5 Security capabilities

5.1 General

Intended use, *intended environment of use*, *health IT system*, *health IT Infrastructure*, *IT Infrastructure* and local factors should also determine which *security capabilities* are necessary and which *security controls* most suitably assist in establishing that *security capability*. *Security risk assessment* should be used to identify additional security capabilities beyond those listed in this document. Standards, as listed in Annex C, provide more guidance.

Security capabilities should be in a secure state by default and configurable to support the *HDO security policy*. Any configurable *security capabilities* shall be clearly communicated.

Often security controls are related to the impact on the key concepts of confidentiality, integrity, availability, accountability and authenticity (C-I-A-A-A). A mapping for the security capabilities listed below is provided in Annex D.

5.2 Automatic logoff (ALOF)

Description	The ability of the product to prevent access and misuse by unauthorized users if a session is left open for a period of time.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.4 Automatic Logoff (ALOF)	
Capability goal	Reduce the risk of unauthorized access if a session is left idle for a period of time.	
User need	– Unauthorized users should not have access to health data at an unattended product. – Authorized sessions should automatically terminate or lock after a pre-set period of time. This reduces the <i>risk</i> of unauthorized access to health data when an authorized user left without logging off or locking the display or room. – Automatic log off should include a clearing of sensitive data including health data information from all displays as appropriate. – The <i>HDO</i> should be able to disable the function and set the expiration time (including screen saver) to be able to adhere to the <i>HDO</i> IT policies. – A screen saver with short inactivity time or manually enabled by a shortcut key can be an additional feature. This health data display clearing can be invoked when no key is pressed for some short period (e.g. 15 s to several minutes). This does not log out the user but reduces <i>risk</i> of casual viewing of information. – It is desirable that users should not lose uncommitted work due to automatic logoff. Consider detailing characteristics under ALOF that distinguish between (a) logoff and (b) screen locking with resumption of session.	

5.3 Audit controls (AUDT)

Description	The ability to reliably audit activity on the product.	
Applicable	Standard	See Annex C IHE Technical Frameworks [47] IHE ATNA profile (Audit Trail and Node Authentication Integration Profile) [49]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.5 Audit Controls (AUDT)	
Capability goal	Define harmonized approach towards reliably auditing who is doing what with health data, allowing HDO IT to monitor this using public frameworks, standards and technology. The IHE Audit goal is: to allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). NOTE The IHE audit trail profile is widely supported.	
User need	Capability to record and examine system activity by creating audit trails on a product to track system and health data access, modification, deletion and any configuration changes which impact security and privacy controls. Support for use either as a stand-alone repository (logging audit files in its own file system) or, when configured as such, will send logged information to a separate, HDO-managed central repository. Audit creation and maintenance supported by appropriate audit review tools. Securing of audit data as appropriate (especially if they contain personal data themselves). Audit data that cannot be edited or deleted. Audit data likely contains personal data or health data and all <i>processing</i> (e.g. access, storage and transfer) should have appropriate controls.	

5.4 Authorization (AUTH)

Description	The ability of the product to determine the authorization of users.	
Applicable	Standard	See Annex C ANSI/INCITS 359-2012 (R2022), <i>Information Technology - Role-Based Access Control</i> IHE Technical Frameworks [47], including: – Audit Trail and Node Authentication (ATNA) [49] – Enterprise User Authentication (EUA) [50] – Cross-Enterprise User Assertion (XUA) [51] IHE IT Infrastructure White Paper – Access Control [48] ISO/TS 22600-1, <i>Health informatics – Privilege management and access control – Part 1: Overview and policy management</i> [44] ISO 13606-4, <i>Health informatics – Electronic health record communication – Part 4: Security</i> [22]
	Policies	Local HDO IT Policies
Reference material	MDS2 – 2.3.6 Authorization (AUTH)	
Capability goal	Control of access to sensitive data including health data and functions only as necessary to perform the tasks required by the <i>HDO</i> consistent with the <i>intended use</i>. When authorization is given personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	
User need	– Avoiding unauthorized access to data and functions in order to (1) preserve system and data confidentiality, integrity and availability and (2) remain within permitted uses of data and systems. – As defined by the <i>HDO</i>'s IT policy and based on the authenticated individual user's identification, the authorization capability allows each user to only access approved data and only perform approved functions on the product. – Authorized users include <i>HDO</i> and service staff as defined by that policy. – <i>Health software</i> typically support a permissions-based system providing access to system functions and data appropriate to the role(s) of the individual in the <i>HDO</i> (role-based access control, RBAC). For example: • Users can perform their assigned tasks using all appropriate product functions (e.g. monitor or scan patients). • Responsibility for quality assurance testing activities in <i>health software</i> that supports role-based access control typically falls to a professional or team with expertise in both healthcare informatics and IT <i>security</i>. • Service staff can access the system in a manner that supports their preventive maintenance, problem investigation, and problem elimination activities. – Authorization permits the <i>HDO</i> to effectively deliver healthcare while (1) maintaining system and data <i>security</i> and (2) following the principle of appropriate data access minimization. Authorization can be managed locally or enterprise-wide (e.g. via centralized directory). NOTE Where <i>intended use</i> does not permit the time necessary for logging onto and off of a product (e.g. high-throughput use), the local IT policy can permit reduced authorization controls presuming adequacy of controlled and restricted physical access.	

5.5 Cybersecurity product upgrades (CSUP)

Description	The ability to install <i>security</i> updates for the product.	
Applicable	Standard	See Annex C ISO/IEC 29147, <i>Information technology – Security techniques – Vulnerability disclosure</i> [26] ISO/IEC 30111, <i>Information technology – Security techniques – Vulnerability handling processes</i> [27]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.7 <i>Cybersecurity</i> product updates (CSUP) NEMA/MITA CSP 2-2021 – Lifecycle Best Practices Framework for Medical Imaging Devices [29]	
Capability goal	Maintain the <i>security</i> of the <i>health software</i> . Establish a clear agreement on who is technically responsible for the specific items of patch management of the <i>health software</i> and its related environment.	
User need	– Establish a standardized process for patch installation and upgrades by on-site service staff, remote service staff, and authorized <i>HDO</i> personnel. Installation and upgrade of product <i>security</i> patches by on-site service staff, remote service staff, and possibly authorized <i>HDO</i> staff (downloadable patches). – Installation of applicable <i>health software security</i> patches and mitigations as soon as possible after appropriate <i>risk assessment</i> for the <i>health software</i> in accordance with regulations, requiring the following. • High-risk vulnerabilities as determined by <i>risk assessment</i> should be addressed with the highest priority. • The <i>health software</i> vendor and the <i>HDO</i> are required to assure continued safe and effective clinical functionality of their products. Understanding of local <i>medical device</i> regulation (in general, <i>medical device</i> should not be patched or modified without explicit written instructions from the <i>manufacturer</i>). • Adequate testing should be done to discover any unanticipated side effects of the patch on the <i>health software</i> (performance or functionality) that can endanger a patient. • User, especially <i>HDO</i> IT staff and <i>HDO</i> service, requires proactive information on assessed or validated patches. – It is essential that updates and upgrades are appropriately communicated to the end user, including: • expected patch release schedule; • whether <i>manufacturer</i> notifies the customer when updates are approved for installation; • if product performs automatic installation of software updates; • if <i>manufacturer</i> has an approved list of third-party software that can be installed on the product; • whether <i>manufacturer</i> permits the user to install <i>manufacturer</i>-approved third-party software on the product themselves; • if product has a mechanism in place to prevent installation of unapproved software; • if <i>manufacturer</i> has a <i>process</i> in place to assess product vulnerabilities and updates; • if <i>manufacturer</i> provides customers with review and approval status of updates. – Document <i>manufacturer</i> restrictions on applying <i>security</i> patches. – Document details on all software or firmware that require <i>security</i> updates during its operational life. NOTE This can be implemented through a SBOM or more user centric documentation.	

5.6 Health data de-identification (DIDT)

Description	The ability of the product to protect <i>PHI</i> , where possible, by directly removing information that allows (re-)identification of a patient.	
Applicable	Standard	See Annex C NEMA DICOM Supplement 142: Clinical Trial De-identification Profiles NEMA DICOM Supplement 55: Attribute Level Confidentiality (including De-identification) 5 Sept 2002 ISO 25237, <i>Health Informatics – pseudonymization</i> [25] ISO/IEC 20889, <i>Privacy enhancing data de-identification terminology and classification of techniques</i> [42] NIST IR 8053:2015, <i>De-Identification of Personal Information</i> [43] NOTE 1 Pseudonymization and use of any manner of patient-identifying keys permit data to be re-identified and, as such, are not de-identification methods. NOTE 2 When conducting for instance research or analysis, there can be a need to be able to re-identify or at least to be able to keep all the records for a patient together. In pseudonymization, the algorithm used can be intentionally reversible or intentionally not reversible.
	Policies	Local <i>HDO</i> IT Policies HIPAA § 164.514(b) – Implementation specifications: Requirements for de-identification of protected health information
Reference material	MDS2 – 2.3.8 Health Data De-Identification (DIDT) Sweeney, L. 2002. <i>K-anonymity: a model for protecting privacy</i>. International Journal on Uncertainty, Fuzziness and Knowledge-based systems, 10(5), 557-570.	
Capability goal	Ability of the product to directly remove information that allows (re-)identification of a patient and to provide adequate pseudonymization.	
User need	Clinical user, service engineers and marketing should be able to de-identify health data for various purposes not requiring patient identity. Data scrubbing prior to shipping back to factory; architecting to allow remote service without health data access or exposure; in-factory quarantine, labelling, and training. Additional tooling can be required if the product is defective and cannot execute the function anymore. Where removal of all personal identifiers is undesired, pseudonymization can be used to appropriately protect health data, e.g. for research and analysis; data sharing; quality control and audits. <i>Manufacturers</i> should provide detailed information about the de-identification and pseudonymization capabilities of the product, to ensure that users can easily locate and understand the <i>security</i>-related information they need.	

5.7 Data backup and disaster recovery (DTBK)

Description	The ability to recover after damage to or destruction of product data, hardware, software or site configuration information.	
Applicable	Standard	See Annex C ISO/IEC 20000-1 [18] and ISO/IEC 20000-2, <i>Service continuity planning and testing</i> [19]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.9 <i>Data backup and disaster recovery</i> (DTBK)	
Capability goal	Document the necessity and steps for periodic back-ups. Confidentiality and integrity of backups should be validated periodically; this should also be checked during installation. Ensure the backup restore time meets the organizational recovery goals.	
User need	Reasonable assurance that persistent system settings and persistent health data stored on products can be restored after a system failure or compromise so that business can be continued.	

5.8 Emergency access (EMRG)

Description	The ability of the product user to access protected health data and <i>health software</i> essential performance, in case of an emergency situation requiring immediate access (break-glass functionality).	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies HIPAA § 164.312(a)(2)(ii) – <i>Emergency access procedure</i>
Reference material	MDS2 – 2.3.10 <i>Emergency access</i> (EMRG)	
Capability goal	Ensure that access to protected health data is possible in case of an emergency situation requiring immediate access to stored health data. Ensure that access to the <i>health software</i> essential performance is possible in case of an emergency situation requiring immediate access.	
User need	– During emergency situations, where personal user identification and authentication mechanisms are not available, the authorized clinical user needs to have access to health data or <i>health software</i> essential performance. – Emergency access is to be detected, recorded and reported. Ideally including some manner of immediate notification to the system administrator or medical staff (in addition to audit record). – Emergency access should require and record self-attested user identification as entered (without authentication). – <i>HDO</i> can solve this through procedural approach using a specific user account or function of the system. – The administrator should be able to enable and disable any emergency functions provided by the product dependent on which technical or procedural controls are required. NOTE <i>HDO</i>'s should define the emergency conditions for the product to be used, e.g. in a Business Continuity Plan.	

5.9 Health data integrity and authenticity (IGAU)

Description	The ability of the product to verify integrity and authenticity, and to assure the availability of stored health data on both fixed and removable media.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.11 Health data integrity and authenticity (IGAU) NEMA <i>Security and Privacy Auditing</i> [30]	
Capability goal	Assure that health data has not been altered or destroyed in non-authorized manner and is from the originator.	
User need	Ensure the health data is reliable by having appropriate integrity and authenticity mechanisms. User wants the assurance that health data is reliable and not tampered with.	

5.10 Malware detection/protection (MLDP)

Description	The ability of the product to effectively prevent, detect and remove malware.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.12 malware detection/protection (MLDP) NEMA <i>Defending Medical Information Systems Against Malicious Software</i> [31]	
Capability goal	<i>Health software</i> ensures an effective and uniform support for the prevention, detection, and removal of malware. This is an essential step in a defense in depth approach to <i>security</i> .	
User need	<i>HDOs</i> should detect traditional malware as well as unauthorized software that could interfere with proper operation of the product or system. Malware protection software is updated, if required malware pattern data files should be kept current. Post-updating the malware protection software <i>verification</i> testing of product operation for both continued <i>intended use</i> and <i>safety</i> is often necessary to meet regulatory quality requirements.	

5.11 Node authentication (NAUT)

Description	The ability of the product to authenticate communication partners and nodes.	
Applicable	Standard	See Annex C IHE ATNA profile (Audit Trail and Node Authentication Integration Profile) [49] ITU-T Recommendation X.509, Information technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks [53]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.13 Node Authentication (NAUT) IHE: Enabling Document Sharing Health Information Exchange Using IHE Profiles [47] NEMA/COCIR/JIRA Joint <i>Security</i> and Privacy Committee White Paper: Management of Machine Authentication Certificates, May 2007	
Capability goal	Authentication policies shall be flexible to adapt to local <i>HDO</i> IT policy. As necessary, use node authentication when communicating health data.	
User need	– Capability of managing cross-machine accounts to protect sensitive data including health data and access to <i>health software</i> functions. – Support for stand-alone and central administration. – Support for node authentication according industry standards. – To detect and prevent entity falsification (provide non-repudiation).	

5.12 Person authentication (PAUT)

Description	The ability of the product to authenticate human users.	
Applicable	Standard	See Annex C NIST SP 800-63 series, <i>Digital Identity Guidelines</i> [17] IHE Technical Frameworks [47], including: – Audit Trail and Node Authentication (ATNA) [49] – Personnel White Pages (PWP) [52] – Enterprise User Authentication (EUA) [50] – Cross-Enterprise User Assertion (XUA) [51] ITU-T Recommendation X.509, Information technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks [53]
	Policies	SANS <i>Security Policy Project</i> Local <i>HDO</i> IT Policies
Reference material	MDS 2 – 2.3.15 Person authentication (PAUT)	
Capability goal	Authentication policies shall be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when providing access to health data. To control access to products, network resources and health data and to generate non-repudiable audit trails. This feature should be able to identify unambiguously and with certainty the individual who is accessing the network, product or resource. NOTE 1 This requirement is relaxed during “break-glass” operation. See capability “Emergency access.” NOTE 2 <i>Security</i> measures shall not impede medical care or compromise patient <i>safety</i>. For instance, in emergency situations where swift access to patient information is vital, alternative secure methods guided by thorough <i>risk assessment</i> should be in place to ensure that care is not delayed.	
User need	– Creation and use of unique accounts for users and role-based access control (RBAC, local and remote) for a network connected product to control and monitor network access and activity. – Person authentication should be configurable by an authorized user to disable access controls where access to the <i>health software</i> is controlled by other means, e.g. access-controlled areas like operating rooms and radiology suites. – Capability of managing accounts on a modality to protect health data access. – Users can be asked to associate personal preferences with user accounts. This can help products and systems used by multiple users, departments or even multiple <i>HDOs</i>. – Support for stand-alone and central administration. – Single sign-on, access via biometrical recognition, physical tokens or any combination thereof. – Authenticity of electronic records should be signed electronically which requires a means to authenticate the signer. Electronic signatures are expected to: • have the same impact as hand-written signatures within the boundaries of the company, • be permanently linked to their respective record, and • include the time and date that they were applied. – To detect and prevent person falsification (provide non-repudiation).	

5.13 Physical locks on product (PLOK)

Description	The physical locks for the product to prevent unauthorized users with physical access from compromising the IT-security of the system.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.16 Physical locks (PLOK)	
Capability goal	Assure that unauthorized users with physical access do not compromise IT-security of the system. This includes, but is not limited to confidentiality, integrity, and availability of data.	
User need	– Reasonable assurance that sensitive data including health data stored on products or media is and stays secure in a manner proportionate to the sensitivity and volume of data records on the product. – Systems are reasonably free from tampering or component removal that can compromise integrity, confidentiality, or availability. Tampering (including product removal) is detectable.	

5.14 Third-party components in product life cycle roadmaps (RDMP)

Description	<i>Manufacturers</i> plans for security support of third-party component during the product life cycle.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 2.3.17 <i>Roadmap for Third-Party Applications and Software Components in Device Life Cycle</i> (RDMP) NEMA CPSP 1-2021 – <i>Supply Chain Best Practices</i> [28]	
Capability goal	<i>HDOs</i> want an understanding of security throughout the life cycle of <i>health software</i>. The <i>manufacturer</i> plans such that products are sustainable throughout their life cycle according to quality management systems and regulations. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes [21] is an example of quality management standard. Proactively manage impact of life cycle of components throughout a product's full life cycle. For example, the ability to provide security patches for software components could be analysed and managed in accordance with IEC 81001-5-1:2021, 4.3 [3]. The commercial off-the-shelf or third-party software includes operating systems, database systems, report generators, MIP components, etc. (assumption is that existing PCP already manages hardware component obsolescence). NOTE Third party also includes internal suppliers of security vulnerable components with own life cycle and support programs.	
User need	– <i>HDO</i> contracts, policy and regulations require that vendor maintain and support the system during product life. – Updates and upgrades are expected when platform components become obsolete. – <i>HDOs</i> and service provider show extreme care in irreversibly erasing health data prior to storage products being decommissioned (discarded, reused, resold or recycled). Such activities should be logged and audited. – Sales and service are well informed about security support offered per product during its life cycle.	

5.15 System and application hardening (SAHD)

Description	The product's inherent resistance to cyber-attacks and malware.	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.19 System and application hardening (SAHD) IEC 81001-5-1, <i>Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle</i> [3]	
Capability goal	Set configurable <i>security controls</i> on the <i>health software</i> such that <i>security</i> is maximized (“hardened”) while maintaining <i>intended use</i> and fit for the <i>intended environment of use</i> .	
User need	- Minimize attack vectors and overall attack surface area via port closing, service removal, etc. <i>HDO</i> IT requires systems connected to their network to be secure on delivery and hardened against misuse and attacks. - The user to inform the <i>manufacturer</i> of suspected <i>security</i> breaches and perceived weaknesses in user equipment. - The <i>health software</i> is resilient to attacks and capable of automated response and recovery.	

5.16 Health data storage confidentiality (STCF)

Description	The ability of the product to mitigate the potential for compromise to the confidentiality of health data stored on the product or removable media.	
Applicable	Standard	See Annex C NEMA DICOM Part 15: <i>Security and System Management Profiles</i> [32] NEMA DICOM Supplement 51: <i>Media security</i> NEMA DICOM Supplement 55: <i>Attribute level confidentiality</i> (including de-identification) 5 Sept 2002 (Final text)
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.21 <i>Data storage confidentiality</i> (STCF) Schneier B. 1996. <i>Applied Cryptography</i> , Second Edition. John Wiley & Sons, New York, NY.	
Capability goal	The <i>manufacturer</i> establishes technical controls to mitigate the potential for compromise to the confidentiality of health data stored on products or removable media. Note that also other data assets, such as passwords, shall be stored with appropriate confidentiality measures.	
User need	- Reasonable assurance that health data stored on products or media is and stays secure. - Encryption has to be provided for health data stored on <i>health software</i> based on <i>risk analysis</i>. - For health data stored on removable media, encryption can protect confidentiality for clinical users but also <i>manufacturer</i> service and application engineers collecting clinical data. - A mechanism for encryption key management consistent with conventional use, service access, emergency “break-glass” access, preferably or where required under the control of the <i>HDO</i>. - Encryption method and strength takes into consideration the volume (extent of record collection or aggregation), sensitivity of data and regional/user requirements.	

5.17 Transmission confidentiality (TXCF)

Description	The ability of the product to ensure the confidentiality of transmitted data.	
Applicable	Standard	See Annex C IHE ATNA profile (<i>Audit Trail and Node Authentication Integration Profile</i>) [49] NEMA DICOM Part 15: <i>Security and System Management Profiles</i> [32] IETF: <i>Transport Layer Security in Network Working Group</i> RFC 5246, <i>The Transport Layer Security (TLS) Protocol Version 1.2</i> RFC 8446, <i>The Transport Layer Security (TLS) Protocol Version 1.3</i> ITU-T Recommendation X.509, <i>Information technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks</i> [53]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.22 Transmission confidentiality (TXCF)	
Capability goal	The IT-system can sufficiently ensure the confidentiality of data during transmission.	
User need	Assurance that data confidentiality is appropriately maintained during transmission.	

5.18 Transmission integrity and authenticity (TXIG)

Description	The ability of the product to ensure the integrity and authenticity of transmitted data.	
Applicable	Standard	See Annex C IHE ATNA profile (<i>Audit Trail and Node Authentication Integration Profile</i>) [49] NEMA DICOM Part 15: <i>Security and System Management Profiles</i> [32] ITU-T Recommendation X.509, <i>Information technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks</i> [53] NIST SP 800-63 series, <i>Digital Identity Guidelines</i> [17]
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.23 Transmission integrity (TXIG) NEMA SPC Certificates white paper.	
Capability goal	Product appropriately protects the integrity of data during transmission and authenticates the source of the transmission.	
User need	Ensure the data is reliable by having appropriate integrity and authenticity mechanisms.	

6 Additional supporting information

6.1 General

While specific *security capabilities* were discussed in Clause 5, there is a need to document additional information that is required for *security* management by the various stakeholders. Such information should address all activities in the life cycle such as installation, configuration, use and disposal. This pertains to general *security* guidance (SGUD), remote connectivity (RMOT), details on the usage of software components (SBOM), system network requirements and capabilities (CONN) and if and how the *health software processes* personal data (MPH).

Depending on the *intended use*, *intended environment of use*, and further considerations, additional information can be required.

NOTE The tables below are intended to address *risk*.

6.2 Connectivity capabilities (CONN)

Description	All physical and virtual <i>interfaces</i> for the product to enable appropriate connectivity <i>security control</i> .	
Applicable	Standard	See Annex C
	Policies	Local <i>HDO</i> security and privacy policies
Reference material	MDS2 – 2.3.14 Connectivity Capabilities (CONN)	
Capability goal	Provide guidance on local and remote connections for normal use.	
User need	- Understanding connectivity capabilities and their security impact; enabling secure use of connectivity features for access to network and information sources. - Information is needed for normal (e.g. <i>HDO</i> operations) and service connectivity (e.g. <i>manufacturer</i>); this should address both local and remote connections.	

6.3 Management of personally identifiable information (MPII)

Description	Management of <i>personally identifiable information</i> .	
Applicable	Standard	See Annex C ISO/IEC 27701, Security techniques – Extension to ISO/IEC 27001 [11] and ISO/IEC 27002 for privacy information management – Requirements and guidelines [13] ISO/TS 14265, Health Informatics – Classification of purposes for processing <i>personal health information</i> [20]
	Policies	Local <i>HDO</i> security and privacy policies. General Data Protection Regulation (EU 2016/679 - GDPR) Health Insurance Portability and Accountability Act (US HIPAA)
Reference material	MDS2 – 2.3.3 Management of Personally identifiable information (MPII)	
Capability goal	Ensure <i>personally identifiable information</i> can be managed correctly by all involved stakeholders	
User need	The users should understand what <i>personally identifiable information</i> is generated or collected by the <i>health software</i> including the related data flows to support appropriate <i>risk assessment</i> and the need for data processing agreements.	

6.4 Remote services (RMOT)

Description	All types of service providers activities via remote connections.	
Applicable	Standard	See Annex C ISO/TS 11633-1 specifies the <i>risk assessment</i> required to protect remote maintenance activities [45] ISO/TR 11633-2 provides a practical example of a <i>risk analysis</i> for remote maintenance services [46]
	Policies	N/A
Reference material	MDS2 – 2.3.24 Remote Service (RMOT)	
Capability goal	To enable service providers to perform activities such as, but not limited to maintenance of the system via a network or other remote connection.	
User need	– The <i>HDO</i> of the remotely connected products and the remote service provider should agree on the connected services and references to be used for remote connection. – Remote connectivity exposes the <i>HDO</i> of the remotely connected products and the remote service provider to <i>risks</i> related to confidentiality, integrity, and availability of information and systems. Therefore, <i>risk</i> measures are required. – The <i>manufacturer</i> should apply <i>risk management</i> for remote connectivity including the impact on <i>safety</i> and <i>effectiveness</i>.	

6.5 Software Bill of Materials (SBOM)

Description	List of software components, their relationships and other associated information.	
Applicable	Standard	See Annex C ISO 19770-2, <i>Information technology – IT asset management – Part 2: Software identification tag</i> [39] NISTIR 8060, <i>Guidelines for the Creation of Interoperable Software Identification (SWID) Tags</i> [40] ISO/IEC 5962, <i>Information technology – SPDX® Specification V2.2.1</i> [41] CycloneDX: https://cyclonedx.org/
	Policies	Local <i>HDO</i> IT Policies
Reference material	MDS2 – 2.3.18 Software bill of materials (SBOM) IMDRF Principles and Practices for Software Bill of Materials for <i>medical device Cybersecurity</i>: 2023 (N73) [34] Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), Third edition, 2024, CISA [35] NTIA, US Department of Commerce, The Minimum Elements for a Software Bill of Materials (SBOM), 2021-07-12 [36] NTIA, How to Guide for SBOM Generation, 2021 [37] MITRE, Data normalization challenges and mitigations in software bill of materials (SBOM) processing, a white paper for <i>medical device manufacturers</i>, October 2024 [38]	
Capability goal	SBOM lists the identified software components and other associated information. SBOM is a nested inventory for software, a list of ingredients that make up software components. The <i>manufacturer</i> generates appropriately updated SBOM such that products are sustainable throughout their life cycle according internal quality systems and external regulations (see also RMDP for planning). The <i>manufacturer</i> manages their product SBOM merging SBOM information from component supplier under the proactive management of impacts from components life cycle.	
User need	– SBOM is updated and provided to <i>HDO</i> throughout the product life cycle. – SBOM can be used for <i>HDO</i>'s operational <i>security</i> planning and awareness. <i>HDO</i> proactively manages vulnerabilities using provided SBOM and input from own sources such as ISAOs/CERT. – SBOM could be generated and ingested in machine readable format such as SPDX and CycloneDX NOTE The VEX (Vulnerability Exploitability eXchange) concept can be used together with SBOM, especially to determine the impact of vulnerabilities. The VEX concept can be automated as well as SBOM generation/ingesting.	

6.6 Security guides (SGUD)

Description	Availability of <i>security</i> guidance for user and administrator (including <i>manufacturer</i> sales and service) of the system.	
Applicable	Standard	See Annex C IEC 80001-1:2021, <i>Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software</i> [1]; Annex B, Guidance for accompanying document Information. IEC 81001-5-1:2021, <i>Health Software and Health IT Systems Safety, Effectiveness and Security – Part 5-1: Security – Activities in the product life cycle</i> [3]; Annex E (informative) Documents specified in IEC 62443-4-1.
	Policies	Local <i>HDO</i> IT Policies IMDRF/IMDRF CYBER WG/N60 FINAL: 2020, <i>Principles and Practices for medical device Cybersecurity</i> [33], 5.5.2 Customer Security Documentation.
Reference material	MDS2 – 2.3.20 Security Guidance (SGUD)	
Capability goal	Ensure that <i>security</i> guidance for users and administrators of the system is available. Separate manuals for users and administrators (including <i>manufacturer</i> sales and service) are desirable as they allow understanding of full administrative functions to be kept only by administrators.	
User need	– Users should be clearly informed about their responsibilities and secure way of working with the system. – The administrator needs information about managing, customizing and monitoring the system (i.e. access control lists, audit logs, etc.). – Administrator needs clear understanding of security capabilities to allow health data <i>risk assessment</i> per appropriate regulatory requirement. – Sales and service also need information about the system's security capabilities and secure way of working. – Inform the <i>manufacturer</i> of any observed weakness.	

7 Examples of some *security* capabilities

7.1 Example of detailed specification under *security capability*: Person authentication (PAUT)

The previous *security capabilities* clause provided a description of the basic capability along with user need and source material. In actual use, a capability can be more detailed by the *manufacturer* in a *security* statement for the *HDO* in a request for product *security* information.

The following is an example of a *manufacturer's* disclosure under the “Person Authentication” capability. For the target *health software*, the disclosure would indicate presence or absence of that *security capability*.

Person authentication (PAUT)

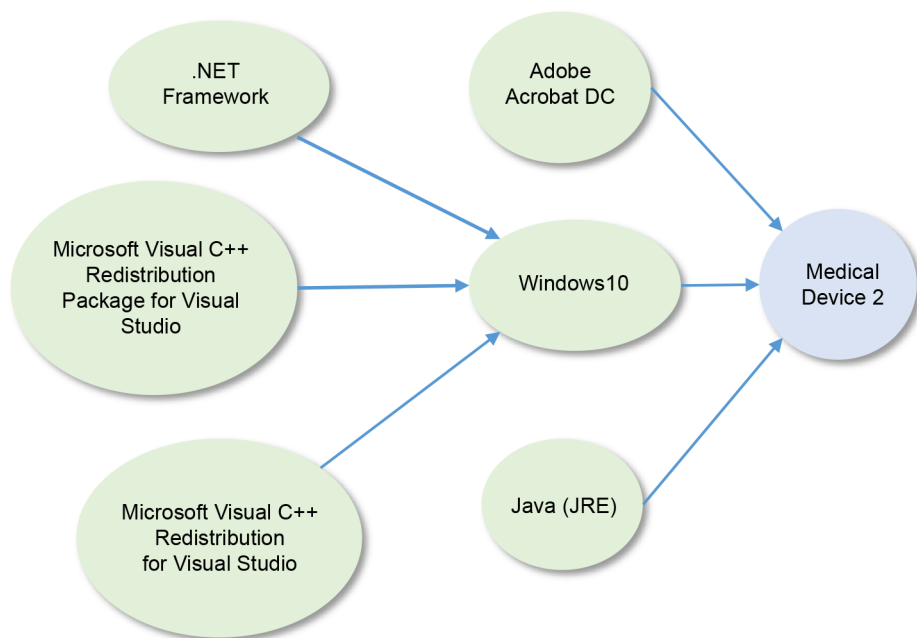
- a) Product supports locally administered (on the product) User accounts operation. Capability for *HDO* IT and optionally the service engineer to manage the local user accounts.
- b) Use of *HDO* central administration of user accounts according the IHE EUA profile.
- c) Support for identifying multiple simultaneous users for role based access control.
- d) Single sign-on for modalities with multiple work spots or single work spots running multiple applications.
- e) Visible indication of who is the current user to make it easier to identify who is using the system, and determine if it is necessary to close the session.
- f) Support fast user switching. By supporting this, signing off and on is not a time-consuming task.

NOTE Examples for regional considerations of the documentation can be found in Annex B.

7.2 Example for Software Bill of Materials (SBOM)

Given Figure 2 (Sample Structure for “*Medical device 2*”), Table 1 shows an example SBOM for a hypothetical “*Medical device 2*” from “MDM1” using the NTIA’s minimum requirements.

NOTE The specific SBOM details are subject to regulatory and customer needs.



IEC

Figure 2 – Sample Structure for “*Medical device2*”

Table 1 – Example SBOM for “Medical device2”

#	Supplier Name	Component Name	Version of the Component	Other Unique Identifiers	Dependency Relationship	Author of SBOM Data	Timestamp
1	MDM1	Medical device 2	2.5.9	pkg supplier/MDM1/Medical device 2@2.5.9	self	MDM1	2021-08-19T08:14:01+09:00
2	Microsoft	Windows 10	1903	pkg supplier/Microsoft/Windows 10@1903	Included in id#1	Microsoft	2021-01-21T03:14:07+09:00
3	Microsoft	.NET Framework	4.5.2	pkg supplier/Microsoft/.NET Framework@4.5.2	Included in id#2	Microsoft	2021-01-13T05:54:00+09:00
4	Microsoft	Microsoft Visual C++ Redistributable Packages for Visual Studio	2013 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable Packages for Visual Studio@2013 update_5	Included in id#2	Microsoft	2015-08-11T05:54:00+09:00
5	Microsoft	Microsoft Visual C++ Redistributable for Visual Studio	2012 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable for Visual Studio@2012 update_5	Included in id#2	Microsoft	2014-01-14T05:54:00+09:00
6	Adobe	Adobe Acrobat DC	19.008	pkg supplier/Adobe/Adobe Acrobat DC@19.008	Included in id#1	MDM1	2021-01-19T03:14:07+09:00
7	Oracle	Java (JRE)	1.8.0 update_191	pkg supplier/Oracle/Java (JRE)@1.8.0 update_191	Included in id#1	MDM1	2017-12-21T03:14:07+09:00

NOTE See also [37].

8 References and other resources

8.1 General

Clause 8 describes the detail behind the abbreviated references used in Clauses 5, 6 and 7. It contains some description and reference to standards and resources that also itemize the security capabilities of *health software* or applications. The focus of each of these resources is slightly different and therefore they should be carefully applied according to their original context.

Reference Document	Title
IHE	Integrated Healthcare Enterprise: https://www.ihe.net/resources/technical_frameworks/ Note on ATNA: https://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication Audit Trail and Node Authentication (ATNA) Integration Profile [49] is designed to support access control by limiting network access between nodes and limiting access to each node to authorized users (locally authenticated). It involves User Authentication, Connection Authentication, and Audit Trails. It supports actors including – Secure Nodes, – Audit Repository, and – Time Server. The actions are to maintain time, authenticate nodes, and recording audit events. It is based upon standards established by the IETF IT Infrastructure Technical Framework including standards for Secure Communications, Audit Log Transport, Audit Log Message. Among these standards are RFC 5246, WS-I Basic Security Profile 1.1, RFC 5424, RFC 5425, RFC 5426, RFC 3164, RFC 3881, ISO 12052:2017, DICOM: Supplement 95 https://www.dicomstandard.org/News-dir/ftsup/docs/sups/sup95.pdf.
Local <i>HDO</i> IT Policies	Policies created by our product user's organization specifying the acceptable use of information technology.

8.2 **Manufacturer disclosure statement for medical device security (MDS2)**

Manufacture Disclosure Statement for *medical device security* – developed by NEMA and HIMSS to capture *medical device security capabilities* in a standardized form. Assists professionals responsible for *security-risk assessment* in the management of *medical device security* issues.

<https://www.nema.org/standards/view/Manufacturer-disclosure-statement-for-medical-device-security>

8.3 **Application security questionnaire (ASQ)**

Application Security Questionnaire – developed by HIMSS to capture Information System security and privacy *capabilities*.

<https://www.himss.org/application-security-questionnaire>

8.4 **HL7 Functional Electronic Health Record (EHR)**

The goal of the EHR Work Group is to further the HL7 mission of designing standards to support the exchange of information for clinical decisions and treatments, and help lay the groundwork for nationwide *interoperability* by providing common language parameters that can be used in developing systems that support electronic records.

https://www.hl7.org/implement/standards/product_section.cfm?section=11

<https://confluence.hl7.org/display/EHR>

8.5 **Standards and frameworks**

The Bibliography contains a list of documents and frameworks referenced within this document. The following organizations are sources of additional information.

CIS	The Center for Internet <i>Security</i> Benchmarks and <i>Security</i> Tools https://cisecurity.org
CISA	US <i>Cybersecurity</i> & Infrastructure <i>Security</i> Agency https://www.cisa.gov
NSA	US National <i>Security</i> Agency https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/
ENISA	European Union Agency for <i>Cybersecurity</i> . https://www.enisa.europa.eu/
IETF	The Internet Engineering Task Force Papers: Network Working Group RFC 5246 August 2008: The TLS Protocol Version 1.2. and replaced by TLS Protocol Version 1.3. https://datatracker.ietf.org/doc/html/rfc8446
SANS	The SANS (SysAdmin, Audit, Network, <i>Security</i>) Institute: https://www.sans.org/ The SANS <i>Security</i> Policy Project – “...everything you need for rapid development and implementation of information <i>security</i> policies.” https://www.sans.org/information-security-policy/ SANS Information <i>Security</i> white papers https://www.sans.org/white-papers SANS <i>security</i> glossary https://www.sans.org/security-resources/glossary-of-terms/
WEDI	Workgroup for Electronic Data Interchange <i>Security</i> and Privacy Workgroup (SNIP) https://www.wedi.org/
IHE	Integrated Healthcare Enterprise https://www.ihe.net/ IHE Technical Frameworks [47] IHE ATNA profile (Audit Trail and Node Authentication Integration Profile) [49] IHE EUA (Enterprise User Authentication) [50]

Additional frameworks

ASIP requirements	France l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) https://esante.gouv.fr
DICOM	Digital Imaging and Communications in Medicine (DICOM) National Electrical <i>Manufacturers</i> Association. https://www.dicomstandard.org/
Japan Law/Guidance	JP Act on the Protection of Personal Information (PFI) https://www.japaneselawtranslation.go.jp/en/laws/view/2781 and Guideline for Medical Information System <i>Safety</i> Management https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html (Japanese only), Ministry of Health, Labor and Welfare, Japan