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)

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 It also gives information on projects, replaced and withdrawn publications.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

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;

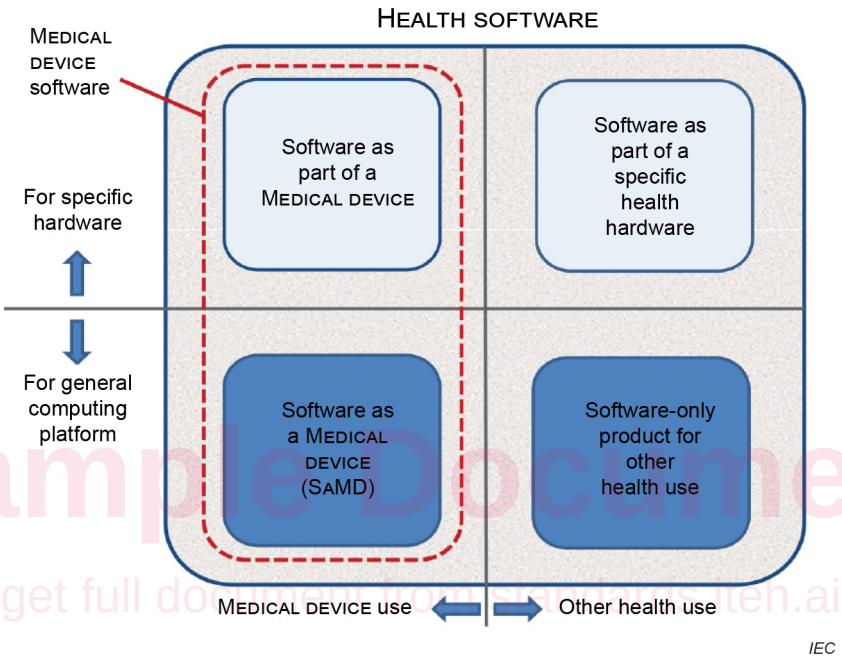
– "may" indicates a permission;

– "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*

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 14791 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 *HDO* 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 *risk* 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 *HDO* should be able to disable the function and set the expiration time (including screen saver) to be able to adhere to the *HDO* 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 *risk* 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 *HDO* 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 *process*ing (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), *Information Technology - Role-Based Access Control* 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, *Health informatics – Privilege management and access control – Part 1: Overview and policy management* [44] ISO 13606-4, *Health informatics – Electronic health record communication – Part 4: Security* [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 *HDO* consistent with the *intended use*. 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 *HDO*'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 *HDO* and service staff as defined by that policy. – *Health software* typically support a permissions-based system providing access to system functions and data appropriate to the role(s) of the individual in the *HDO* (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 *health software* that supports role-based access control typically falls to a professional or team with expertise in both healthcare informatics and IT *security*. • Service staff can access the system in a manner that supports their preventive maintenance, problem investigation, and problem elimination activities. – Authorization permits the *HDO* to effectively deliver healthcare while (1) maintaining system and data *security* 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 *intended use* 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 *security* updates for the product.	
Applicable	**Standard**	See Annex C ISO/IEC 29147, *Information technology – Security techniques – Vulnerability disclosure* [26] ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes* [27]
	Policies	Local *HDO* IT Policies
Reference material	MDS2 – 2.3.7 *Cybersecurity* product updates (CSUP) NEMA/MITA CSP 2-2021 – Lifecycle Best Practices Framework for Medical Imaging Devices [29]	
Capability goal	Maintain the *security* of the *health software*. Establish a clear agreement on who is technically responsible for the specific items of patch management of the *health software* 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 HDO personnel. Installation and upgrade of product *security* patches by on-site service staff, remote service staff, and possibly authorized *HDO* staff (downloadable patches). – Installation of applicable *health software security* patches and mitigations as soon as possible after appropriate *risk assessment* for the *health software* in accordance with regulations, requiring the following. • High-*risk* vulnerabilities as determined by *risk assessment* should be addressed with the highest priority. • The *health software* vendor and the *HDO* are required to assure continued safe and effective clinical functionality of their products. Understanding of local *medical device* regulation (in general, *medical device* should not be patched or modified without explicit written instructions from the *manufacturer*). • Adequate testing should be done to discover any unanticipated side effects of the patch on the *health software* (performance or functionality) that can endanger a patient. • User, especially *HDO* IT staff and *HDO* 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 *manufacturer* notifies the customer when updates are approved for installation; • if product performs automatic installation of software updates; • if *manufacturer* has an approved list of third-party software that can be installed on the product; • whether *manufacturer* permits the user to install *manufacturer*-approved third-party software on the product themselves; • if product has a mechanism in place to prevent installation of unapproved software; • if *manufacturer* has a *process* in place to assess product vulnerabilities and updates; • if *manufacturer* provides customers with review and approval status of updates. – Document *manufacturer* restrictions on applying *security* patches. – Document details on all software or firmware that require *security* updates during its operational life. NOTE This can be implemented through a SBOM or more user centric documentation.	