IEC TR 80001-2-8

Edition 1.0 2016-05

TECHNICAL REPORT

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

IEC TR 80001-2-8:2016-05(en)

IEC TR 80001-2-8

Edition 1.0 2016-05

TECHNICAL REPORT

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 11.040.01

ISBN 978-2-8322-3412-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-8, which is a technical report, has been prepared by subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice, and ISO technical committee 215: Health informatics. [1)]

_____

1) This document contains original material that is © 2013, Dundalk Institute of Technology, Ireland. Permission is granted to ISO and IEC to reproduce and circulate this material, this being without prejudice to the rights of Dundalk Institute of Technology to exploit the original text elsewhere.

It is published as a double logo technical report.

The text of this technical report is based on the following documents of IEC:

Enquiry draft	Report on voting
62A/1018/DTR	62A/1043A/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 14 P-members out of 31 having cast a vote.

This publication has been drafted in accordance with the ISO IEC Directives, Part 2.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

A list of all parts of the IEC 80001 series, published under the general title *Application of risk management for it-networks incorporating medical devices,* can be found on the IEC website.

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

The IEC 80001-1 standard, the *Application of risk management to IT-networks incorporating medical devices*, provides the roles, responsibilities and activities necessary for RISK MANAGEMENT. IEC TR 80001-2-2, the *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls* is a technical report that provides additional guidance in relation to how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT PROCESS and stakeholder communications and agreements. This technical report provides guidance for the establishment of each of the SECURITY CAPABILITIES presented in IEC TR 80001-2-2.

IEC TR 80001-2-2 contains an informative set of common, descriptive SECURITY CAPABILITIES intended to be the starting point for a security-centric discussion between the vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sizes of RESPONSIBLE ORGANIZATIONS (henceforth called healthcare delivery organizations – HDOs) as each evaluates RISK using the SECURITY CAPABILITIES and decides what to include or not to include according to their RISK tolerance and available resources. This documentation can be used by HDOs as input to their IEC 80001 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. Other IEC 80001 technical reports will provide step-by-step guidance in the RISK MANAGEMENT PROCESS. IEC TR 80001-2-2 SECURITY CAPABILITIES encourage the disclosure of more detailed SECURITY CONTROLS. This technical report identifies SECURITY CONTROLS from key security standards which aim to provide guidance to a RESPONSIBLE ORGANIZATION when adapting the framework outlined in IEC TR 80001-2-2.

The framework outlined in IEC TR 80001-2-2 requires shared responsibility between HDOs and MEDICAL DEVICE manufacturers (MDMs). Similarly, this guidance applies to both stakeholders, as a shared responsibility, to ensure safe MEDICAL DEVICE IT networks. In order to build a secure MEDICAL DEVICE IT network a joint effort from both stakeholders is required.

A SECURITY CAPABILITY, as defined in IEC TR 80001-2-2, represents a broad category of technical, administrative and/or organizational SECURITY CONTROLS[2)] required to manage RISKS to confidentiality, integrity, availability and accountability of data and systems. This document presents these categories of SECURITY CONTROLS prescribed for a system and the operational environment to establish SECURITY CAPABILITIES to protect the confidentiality, integrity, availability and accountability of data and systems. The SECURITY CONTROLS support the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity or system/data availability. The SECURITY CONTROLS for each SECURITY CAPABILITY can be added to as the need arises[3)]. Controls are intended to protect both data and systems but special attention is given to the protection of both PRIVATE DATA and its subset called HEALTH DATA.

In addition to providing a basis for discussing RISK and respective roles and responsibilities toward RISK MANAGEMENT, this report is intended to supply:

a) Health Delivery Organizations (HDOs) with a catalogue of management, operational and administrative SECURITY CONTROLS to maintain the EFFECTIVENESS of a SECURITY CAPABILITY for a MEDICAL DEVICE on a MEDICAL DEVICE IT-NETWORK;

b) MEDICAL DEVICE manufacturers (MDMs) with a catalogue of technical SECURITY CONTROLS for the establishment of each of the 19 SECURITY CAPABILITIES.

---

2) For the purpose of consistency throughout this report, the term SECURITY CONTROLS refers to the technical, administrative and organizational controls/safeguards prescribed to establish SECURITY CAPABILITIES.

3) The selection of SECURITY CAPABILITIES and SECURITY CONTROLS will vary due to the diversity of MEDICAL DEVICE products and context in relation to environment and INTENDED USE. Therefore, this technical report is not intended as a “one size fits all” solution.

This report presents the 19 SECURITY CAPABILITIES, their respective "requirement goal" and "user need" (identical to that in IEC TR 80001-2-2) with a corresponding list of SECURITY CONTROLS from a number of security standards. The security standards used for mapping SECURITY CONTROLS to SECURITY CAPABILITIES include[4]:

- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*

  NIST Special Publication 800-53 covers the steps in the RISK MANAGEMENT Framework that address SECURITY CONTROL selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline SECURITY CONTROLS based on a FIPS 199 worst-case impact analysis, tailoring the baseline SECURITY CONTROLS, and supplementing the SECURITY CONTROLS based on an organizational assessment of RISK. The security rules cover 17 areas including access control, incident response, business continuity, and disaster recoverability.

- ISO IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

  This standard defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will fulfil the most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes.

  This standard also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

- ISO IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

  This standard defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.

  This standard defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

- IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

  This standard provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels, SL-C (control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

- ISO IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

  This standard outlines guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security RISK environment(s). It is designed to be used by organizations that intend to:

---

4) The selection of security standards used in this technical report does not represent an exhaustive list of all potentially useful standards.

1) select controls within the PROCESS of implementing a MEDICAL DEVICE system based on ISO IEC 27001;

2) implement commonly accepted information SECURITY CONTROLS;

3) develop their own information security management guidelines.

- ISO 27799:—[5], *Health informatics – Information security management in health using ISO IEC 27002*

  This standard defines guidelines to support the interpretation and implementation in health informatics of ISO IEC 27002 and is a companion to that standard.

  It specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, HDOs and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

5) To be published.

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

1 Scope

This part of IEC 80001, which is a Technical Report, provides guidance to Health Delivery Organizations (HDOs) and MEDICAL DEVICE manufacturers (MDMs) for the application of the framework outlined in IEC TR 80001-2-2. Managing the RISK in connecting MEDICAL DEVICES to IT-NETWORKS requires the disclosure of security-related capabilities and RISKS. IEC TR 80001-2-2 presents a framework for this disclosure and the security dialog that surrounds the IEC 80001-1 RISK MANAGEMENT of IT-NETWORKS. IEC TR 80001-2-2 presents an informative set of common, descriptive security-related capabilities that are useful in terms of gaining an understanding of user needs. This report addresses each of the SECURITY CAPABILITIES and identifies SECURITY CONTROLS for consideration by HDOs and MDMs during RISK MANAGEMENT activities, supplier selection, device selection, device implementation, operation etc.

It is not intended that the security standards referenced herein are exhaustive of all useful standards; rather, the purpose of this technical report is to identify SECURITY CONTROLS, which exist in these particular security standards (listed in the introduction of this technical report), that apply to each of the SECURITY CAPABILITIES.

This report provides guidance to HDOs and MDMs for the selection and implementation of management, operational, administrative and technical SECURITY CONTROLS to protect the confidentiality, integrity, availability and accountability of data and systems during development, operation and disposal.

All 19 SECURITY CAPABILITIES are not required in every case and the identified SECURITY CAPABILITIES included in this report should not be considered exhaustive in nature. The selection of SECURITY CAPABILITIES and SECURITY CONTROLS should be based on the RISK EVALUATION and the RISK tolerance with consideration for protection of patient SAFETY, life and health. INTENDED USE, operational environment, network structure and local factors should also determine which SECURITY CAPABILITIES are necessary and which SECURITY CONTROLS most suitably assist in establishing that SECURITY CAPABILITY.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities*

IEC TR 80001-2-2:2012, *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*[6)]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
DATA AND SYSTEMS SECURITY
operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

[SOURCE: IEC 80001-1:2010, 2.5]

3.2
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, 2.6]

3.3
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEMS SECURITY

[SOURCE: IEC 80001-1:2010, 2.8]

3.4
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, 2.9]

3.5
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This term generically defines PRIVATE DATA and it subset, HEALTH DATA, within this report to permit users of this report to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to “Personal Data” and “Sensitive Data”; in the USA, HEALTH DATA might be changed to “Protected Health Information (PHI)” while making adjustments to text as necessary.

3.6
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

[SOURCE: IEC 80001-1:2010, 2.10]

---

6) IEC TR 80001-2-2 contains many additional standards, policies and reference materials which are also indispensable for the application of this Technical Report.

3.7
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, 2.12]

3.8
MEDICAL DEVICE
means any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
   - diagnosis, prevention, monitoring, treatment or alleviation of disease,
   - diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
   - investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
   - supporting or sustaining life,
   - control of conception,
   - disinfection of MEDICAL DEVICES,
   - providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be MEDICAL DEVICES in some jurisdictions but for which there is not yet a harmonized approach, are:

- aids for disabled/handicapped people;
- devices for the treatment/diagnosis of diseases and injuries in animals;
- accessories for MEDICAL DEVICES (see Note to entry 3);
- disinfection substances;
- devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' MEDICAL DEVICE to enable that MEDICAL DEVICE to achieve its INTENDED PURPOSE should be subject to the same GHTF procedures as apply to the MEDICAL DEVICE itself. For example, an accessory will be classified as though it is a MEDICAL DEVICE in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to MEDICAL DEVICES are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[SOURCE: IEC 80001-1:2010, 2.14]

3.9
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, 2.16]

3.10
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, 2.18]

3.11
PRIVATE DATA
any information relating to an identified or identifiable person

3.12
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, 2.19]

3.13
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

[SOURCE: IEC 80001-1:2010, 2.21, modified – The note has been deleted.]

3.14
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

[SOURCE: IEC 80001-1:2010, 2.22, modified – The notes have been deleted.]

3.15
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, 2.23]

3.16
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, 2.24]

3.17
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, 2.25]

3.18
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

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

3.19
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

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

3.20
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

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

3.21
SECURITY CAPABILITY
broad category of technical, administrative or organizational controls to manage RISKS to confidentiality, integrity, availability and accountability of data and systems

3.22
SECURITY CONTROL
management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[SOURCE: NIST IR 7298]

3.23
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

[SOURCE: IEC 80001-1:2010, 2.32]

4 Guidance for establishing SECURITY CAPABILITIES

4.1 General

This clause presents each of SECURITY CAPABILITIES, as outlined in IEC TR 80001-2-2, with corresponding tables (Tables 1 to 19) of recommended SECURITY CONTROLS from the following standards:

Technical SECURITY CONTROLS:

- NIST SP-800-53;
- ISO IEC 15408-2;
- ISO IEC 15408-3;
- IEC 62443-3-3;

Operational/administrative SECURITY CONTROLS:

- ISO IEC 27002;
- ISO 27799.

For infrastructure and MEDICAL IT NETWORK SECURITY CONTROLS, ISO IEC 27002 and ISO 27799 are grouped together in the below tables as the standards are fully aligned.

ISO IEC 27002 specifies a set of detailed controls for managing information security. ISO 27799 specifies additional guidance specifically for health information security and provides health information security best practice guidelines.

4.2 Automatic logoff – ALOF

Requirement goal: Reduce the RISK of unauthorized access to HEALTH DATA from an unattended workspot.

Prevent misuse by other users if a system or workspot is left idle for a period of time.

User need: Unauthorized users are not able to access HEALTH DATA at an unattended workspot.

Authorized user sessions need to 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 the workspot without logging off or locking the display or room.

Automatic logoff needs to include a clearing of HEALTH DATA from all displays as appropriate.

The local authorized IT administrator needs to be able to disable the function and set the expiration time (including screen saver)

A screen saver with short inactivity time or manually enabled by a shortcut key might be an additional feature. This HEALTH DATA display clearing could be invoked when no key is pressed for some short period (e.g. 15 s to several minutes). This would not log out the user but would reduce RISK of casual viewing of information.

It is desirable that clinical 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.

Table 1 – ALOF controls

Standard	Reference	Control
SP 800-53	AC-1	Access control policy and management
	AC-2	Account management
	AC-7	Unsuccessful logon attempts
	AC-11	Session lock
	AC-12	Session termination
	AC-23	Data mining protection
	AC-24	Access control decisions
	CM-4	Security impact analysis
	IA-4	Identifier management
	IA-11	Re-authentication
ISO IEC 15408-2	FTA_SSL	Session locking and termination
	FMT_SAE	Security attribute expiration
	FIA_UAU	User authentication
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	

Table 1 *(continued)*

Standard	Reference	Control
IEC 62443-3-3	SR 2.5	Session lock
	SR 2.6	Remote session termination
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the Information Security Policy
	9.1.1	Access control policy
	9.4.2	Secure logon procedures
	11.2.8	Unattended user equipment
	11.2.9	Clear desk and clear screen policy
	18.2.2	Compliance with security policies and standards

4.3 Audit controls – AUDT

Requirement 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.

Our industry agreed upon and HDO IT strongly prefers Integrating the Healthcare Enterprise (IHE) audit trail profile support.

Audit goal (from IHE): 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).

User need: Capability to record and examine system activity by creating audit trails on a device to track system and HEALTH DATA access, modification, or deletion.

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 and/or HEALTH DATA and all processing (e.g. access, storage and transfer) should have appropriate controls.

Table 2 – AUDT controls

Standard	Reference	Control
SP 800-53	AC-21	Information sharing
	AC-23	Data mining protection
	AU-1	Audit and accountability policy and procedures
	AU-2	Audit events
	AU-3	Content of audit records
	AU-4	Audit storage capacity
	AU-5	Response to audit processing failures
	AU-6	Audit review, analysis and reporting
	AU-7	Audit reduction and report generation
	AU-8	Time stamps
	AU-9	Protection of audit information
	AU-10	Non-repudiation
	AU-11	Audit record retention
	AU-12	Audit generation
	AU-13	Monitoring for information disclosure
	AU-14	Session audit
	AU-15	Alternate audit capacity
	AU-16	Cross-organizational auditing
ISO IEC 15408-2	FAU_ARP	Security audit automatic response
	FAU_GEN	Security audit data generation
	FAU_SAA	Security audit analysis
	FAU_SAR	Security audit review
	FAU_SEL	Security audit event selection
	FAU_STG	Security audit event storage
	FCO_NRO	Non-repudiation of origin
	FCO_NRR	Non-repudiation of receipt
	FMT_SAE	Security attribute expiration
	FPT_STM	Time stamps
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 2.8	Auditable events
	SR 2.9	Audit storage capacity
	SR 2.10	Response to audit processing failures
	SR 2.11	Timestamps
	SR 2.12	Non-repudiation
	SR 3.9	Protection of audit information
	SR 6.1	Audit reduction and report generation
	SR 6.2	Continuous monitoring

Table 2 *(continued)*

Standard	Reference	Control
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.2	Segregation of duties
	6.2.2	Teleworking
	12.4.1	Event logging
	12.4.2	Protection of log information
	12.4.3	Administrator and OPERATOR logs
	12.4.4	Clock synchronisation
	12.7.1	Information systems audit controls
	16.1.7	Collection of evidence
	18.1.3	Protection of records
	18.1.4	Privacy and protection of personally identifiable information

4.4 Authorization – AUTH

Requirement goal: Following the principle of data minimization, provide control of access to HEALTH DATA and functions only as necessary to perform the tasks required by the HDO consistent with the INTENDED USE.

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 HDO 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 device.

Authorized users include HDO and service staff as defined by that policy.

- MEDICAL DEVICES 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: OPERATORS can perform their assigned tasks using all appropriate device functions (e.g. monitor or scan patients).
- Quality staff (e.g. medical physicist) can engage in all appropriate quality and assurance testing activities.
- Service staff can access the system in a manner that supports their preventive maintenance, problem investigation, and problem elimination activities.

Authorization permits the RISK 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).

Where INTENDED USE does not permit the time necessary for logging onto and off of a device (e.g. high-throughput use), the local IT Policy can permit reduced authorization controls presuming adequacy of controlled and restricted physical access.

Table 3 – AUTH controls

Standard	Reference	Control
SP 800-53	AC-1	Access control policy and management
	AC-2	Account management
	AC-3	Access enforcement
	AC-5	Separation of duties
	AC-6	Least privilege
	AC-7	Unsuccessful logon attempts
	AC-17	Remote access
	AC-18	Wireless access
	AC-19	Access control for mobile devices
	AC-21	Information sharing
	AC-23	Data mining protection
	AC-24	Access control decisions
	PL-4	Rules of behavior
ISO IEC 15408-2	FDP_ACC	Access control policy
	FIA_ATD	User attribute definition
	FMT_MOF	Management of functions in TSF
	FMT_MSA	Management of security attributes
	FMT_MTD	Management of TSF data
	FMT_REV	Revocation
	FMT_SAE	Security attribute expiration
	FMT_SMR	Security management roles
	FTA_LSA	Limitation on scope of selectable attributes
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.3	Account management
	SR 2.1	Authorization enforcement
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.1	Information security roles and responsibilities
	6.1.2	Segregation of duties
	7.2.1	Management responsibilities
	8.1.3	Acceptable use of assets
	8.2.3	Handling of assets
	9.1.1	Access control policy
	9.1.2	Access to networks and network services
	9.2.1	User registration and de-registration
	9.2.2	User access provisioning
	9.2.3	Management of privileged access rights
	9.2.4	Management of secret authentication information of users
	9.4.1	Information access restriction
	9.4.4	Use of privileged utility programs
	9.4.5	Access control to program source code

Table 3 *(continued)*

Standard	Reference	Control
ISO IEC 27002	12.1.1	Documented operating procedures
ISO 27799	13.1.3	Segregation in networks
	13.2.4	Confidentiality or non-disclosure agreements

4.5 Configuration of security features – CNFS

Requirement goal: To allow the HDO to determine how to utilize the product SECURITY CAPABILITIES to meet their needs for policy and/or workflow.

User need: The local authorized IT administrator needs to be able to select the use of the product SECURITY CAPABILITIES or not to use the product SECURITY CAPABILITIES. This can include aspects of privilege management interacting with SECURITY CAPABILITY control.

Table 4 – CNFS controls

Standard	Reference	Control
SP 800-53	AC-2	Account management
	AC-5	Separation of duties
	AC-6	Least privilege
	CM-1	Configuration management policy and procedures
	CM-2	Baseline configuration
	CM-3	Configuration change control
	CM-4	Security impact analysis
	CM-5	Access restrictions for change
	CM-6	Configuration settings
	CM-7	Least functionality
	CM-9	Configuration management plan
	SA-10	Developer configuration management
ISO IEC 15408-2	FIA_ATD	User attribute definition
	FMT_MOF	Management of functions in TSF
	FMT_MSA	Management of security attributes
	FMT_MTD	Management of TSF data
	FMT_REV	Revocation
	FMT_SMF	Specification of management functions
	FMT_SMR	Security management roles
	FTA_LSA	Limitation on scope of selectable attributes
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.3	Account management
	SR 7.6	Network and security configuration settings
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.1	Information security roles and responsibilities
	6.1.2	Segregation of duties
	9.1.1	Access control policy

Table 4 *(continued)*

Standard	Reference	Control
ISO IEC 27002	9.2.3	Management of privileged access rights
ISO 27799	9.2.4	Management of secret authentication information of users
	9.4.1	Information access restriction
	9.4.4	Use of privileged utility programs
	12.1.1	Documented operating procedures
	12.1.2	Change management
	12.2.1	Controls against malware
	14.2.2	System change control procedures
	14.2.3	Technical review of applications after operating platform changes
	9.2.4	Management of secret authentication information of users
	14.2.4	Restrictions on changes to software packages
	14.2.9	System acceptance testing
	18.1.5	Regulation of cryptographic controls

4.6 Cyber security product upgrades – CSUP

Requirement goal: Create a unified way of working. Installation / Upgrade of product security patches by on-site service staff, remote service staff, and possibly authorized HDO staff (downloadable patches).

User need: Installation of third party security patches on medical products as soon as possible in accordance with regulations requiring:

- Highest priority is given to patches that address high-RISK vulnerabilities as judged by objective, authoritative, documented, MDM vulnerability RISK EVALUATION.
- The medical product vendor and the healthcare provider are required to assure continued safe and effective clinical functionality of their products. Understanding of local MEDICAL DEVICE regulation (in general, MEDICAL DEVICES should not be patched or modified without explicit written instructions from the MDM).
- Adequate testing has to be done to discover any unanticipated side effects of the patch on the medical product (performance or functionality) that might endanger a PATIENT.

User, especially HDO IT staff and HDO service, requires proactive information on assessed/validated patches.

Table 5 – CSUP controls

Standard	Reference	Control
SP 800-53	AC-17	Remote access
	CM-2	Baseline configuration
	CM-3	Configuration change control
	CM-4	Security impact analysis
	CM-5	Access restrictions for change
	IA-1	Identification and authentication policy and procedures

Table 5 *(continued)*

	Reference	Control
SP 800-53	IA-9	Service identification and authentication
	MA-1	System maintenance policy and procedures
	MA-2	Controlled maintenance
	MA-3	Maintenance tools
	MA-4	Nonlocal maintenance
	MA-5	Maintenance personnel
	MA-6	Timely maintenance
	MP-1	Media protection policy and procedures
	SA-8	Security engineering principles
	SA-11	Developer security testing and evaluation
	SA-14	Criticality analysis
	SI-11	Error handling
ISO IEC 15408-2	*No applicable* SECURITY CONTROL*s*	
ISO IEC 15408-3	ALC_FLR	Flaw remediation
	ATE_COV	Coverage
	ATE_DPT	Depth
	ATE_FUN	Functional tests
	ATE_IND	Independent tests
	AVA_VAN	Vulnerability analysis
IEC 62443-3-3	*No applicable* SECURITY CONTROLS	
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	12.1.2	Change management
	12.2.1	Controls against malware
	12.5.1	Installation of software on operational systems
	12.6.1	Management of technical vulnerabilities
	12.6.2	Restrictions on software installation
	14.1.1	Information security requirements analysis and specification
	14.2.2	System change control procedures
	14.2.3	Technical review of applications after operating platform changes
	14.2.4	Restrictions on changes to software packages
	14.2.5	Secure system engineering principles
	14.2.8	System security testing
	14.2.9	System acceptance testing
	18.2.2	Compliance with security policies and standards

4.7 HEALTH DATA de-identification – DIDT

Requirement goal: Ability of equipment (application software or additional tooling) to directly remove information that allows identification of patient.

Data scrubbing prior to shipping back to factory; architecting to allow remote service without HEALTH DATA access/exposure; in-factory quarantine, labelling, and training.

User need: Clinical user, service engineers and marketing need to be able to de-identify HEALTH DATA for various purposes not requiring PATIENT identity.

Table 6 – DIDT controls

Standard	Reference	Control
SP 800-53	AC-8	System use notification
	AC-21	Information sharing
	AC-23	Data mining protection
	AR-7	Privacy-enhanced system design and development
	AT-1	Security assurance and training policy and protection
	AU-3	Content of audit records
	AU-9	Protection of audit information
	AU-11	Audit record retention
	DM-1	Minimization of personally identifiable information
	DM-2	Data retention and disposal
ISO IEC 15408-2	*No applicable* SECURITY CONTROLS	
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 4.2	Information persistence
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	7.2.2	Information security awareness, education and training
	8.1.3	Acceptable use of assets
	8.1.4	Return of assets
	8.2.1	Classification of information
	8.2.2	Labelling of information
	8.2.3	Handling of assets
	8.3.1	Management of removable media
	8.3.2	Disposal of media
	11.2.4	Equipment maintenance
	11.2.6	Security of equipment and assets off-premises
	11.2.7	Secure disposal or re-use of equipment
	12.1.4	Separation of development, testing and operational environments
	14.3.1	Protection of test data
	18.1.4	Privacy and protection of personally identifiable information
	18.2.2	Compliance with security policies and standards

4.8 Data backup and disaster recovery – DTBK

Requirement goal: Assure that the healthcare provider can continue business after damage or destruction of data, hardware, or software.

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.

NOTE This requirement might not be appropriate for smaller, low-cost devices and can, in practice, rely on the ability to collect new, relevant data in the next acquisition cycle (e.g. short-duration heart rate data lost due to occasional wireless signal loss)

Table 7 – DTBK controls

Standard	Reference	Control
SP 800-53	AU-9	Protection of audit information
	CM-1	Configuration management policy and procedure
	CM-2	Baseline configuration
	CM-3	Configuration change control
	CM-5	Access restrictions for changes
	CM-6	Configuration settings
	CP-1	Contingency planning policy and procedures
	CP-2	Contingency plan
	CP-3	Contingency training
	CP-4	Contingency plan testing
	CP-6	Alternate storage site
	CP-7	Alternate processing site
	CP-8	Telecommunications services
	CP-9	Information system backup
	CP-10	Information system recovery and reconstitution
	CP-13	Alternative security mechanisms
	IR-1	Incident response policy and procedures
	IR-2	Incident response training
	IR-3	Incident response testing
	IR-4	Incident handling
	IR-5	Incident monitoring
	IR-6	Incident reporting
	IR-7	Incident response assistance
	IR-8	Incident response plan
	IR-9	Information spillage response
	IR-10	Integrated information security analysis team
	SI-1	System and information integrity policy and procedures
	PM-9	RISK MANAGEMENT strategy
ISO IEC 15408-2	FDP_ROL	Rollback
	FPT_ITA	Availability of exported TSF data
	FPT_RCV	Trusted recovery
	FRU_FLT	Fault tolerance
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	

Table 7 *(continued)*

Standard	Reference	Control
IEC 62443-3-3	SR 2.8	Auditable events
	SR 3.6	Deterministic output
	SR 7.3	Control system backup
	SR 7.4	Control system recovery and reconstitution
ISO IEC 27002	5.1.1	Policies for information security
ISO 27799	5.1.2	Review of the information security policy
	6.1.1	Information security roles and responsibilities
	6.1.3	Contact with authorities
	11.1.4	Protecting against external and environmental threats
	12.1.1	Documented operating procedures
	12.3.1	Information backup
	16.1.1	Responsibilities and procedures
	16.1.2	Reporting information security events
	16.1.5	Response to information security incidents
	16.1.6	Learning from information security incidents
	16.1.7	Collection of evidence
	17.1.1	Planning information security continuity
	17.1.2	Implementing information security continuity
	17.1.3	Verify, review and evaluate information security continuity
	18.1.3	Protection of records
	18.1.4	Privacy and protection of personally identifiable information

4.9 Emergency access – EMRG

Requirement goal: Ensure that access to protected HEALTH DATA is possible in case of an emergency situation requiring immediate access to stored HEALTH DATA.

User need: During emergency situations, the clinical user needs to be able to access HEALTH DATA without personal user id and authentication (break-glass functionality).

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 needs to require and record self-attested user identification as entered (without authentication).

HDO can solve this through procedural approach using a specific user account or function of the system.

The administrator needs to be able to enable/disable any emergency functions provided by the product dependent on technical or procedural controls are required.

Table 8 – EMRG controls

Standard	Reference	Control
SP 800-53	AC-1	Access control policy and management
	AC-2	Account management
	AC-14	Permitted actions without identification or authentication
	IA-1	Identification and authentication policy and procedures
	RA-5	Vulnerability scanning
ISO IEC 15408-2	FDP_ACC	Access control policy
	FDP_ACF	Access control functions
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.4	Identifier management
	SR 1.5	Authenticator management
	SR 2.8	Auditable events
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.1	Information security roles and responsibilities
	7.2.2	Information security awareness, education and training
	9.1.1	Access control policy
	9.1.2	Access to networks and network services
	9.2.2	User access provisioning
	9.2.3	Management of privileged access rights
	9.2.5	Review of user access rights
	9.4.1	Information access restriction
	9.4.4	Use of privileged utility programs
	12.1.1	Documented operating procedures
	12.4.1	Event logging
	17.1.1	Planning information security continuity
	17.1.2	Implementing information security continuity
	17.1.3	Verify, review and evaluate information security continuity

4.10 HEALTH DATA integrity and authenticity – IGAU

Requirement goal: Assure that HEALTH DATA has not been altered or destroyed in non-authorized manner and is from the originator. Assure integrity of HEALTH DATA.

User need: User wants the assurance that HEALTH DATA is reliable and not tampered with.

Solutions are to include both fixed and also removable media.

Table 9 – IGAU controls

Standard	Reference	Control
SP 800-53	SA-13	Trustworthiness
	SC-12	Cryptographic key establishment and management
	SC-13	Cryptographic protection
	SC-17	Public key infrastructure certificates
	SC-28	Protection of information at rest
	SI-1	System and information integrity policy and procedures
	SI-3	Malicious code protection
	SI-7	Software and information integrity
	SI-10	Information input validation
ISO IEC 15408-2	FAU_ARP	Security audit automatic response
	FDP_DAU	Data authentication
	FDP_ITT	Internal TOE transfer
	FDP_SDI	Stored data integrity
	FDP_UIT	Inter_TSF user data integrity transfer protection
	FPT_ITT	Internal TOE TSF data transfer
	FPT_TRC	Internal TOE TSF data replication consistency
	FPT_TST	Self test
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 3.1	Communication integrity
	SR 3.3	Security functionality VERIFICATION
	SR 3.4	Software and information integrity
	SR 3.5	Input validation
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	8.1.1	Inventory of assets
	8.1.2	Ownership of assets
	8.1.3	Acceptable use of assets
	8.2.2	Labelling of information
	8.2.3	Handling of assets
	9.1.1	Access control policy
	10.1.1	Policy on the use of cryptographic controls
	10.1.2	Key management
	12.4.1	Event logging
	13.2.1	Information transfer policies and procedures
	18.1.3	Protection of records
	18.1.4	Privacy and protection of personally identifiable information
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards

4.11 Malware detection/protection – MLDP

Requirement goal: Product supports regulatory, HDO and user needs in ensuring an effective and uniform support for the prevention, detection and removal of malware. This is an essential step in a proper defence in depth approach to security.

Malware application software is updated, malware pattern data files kept current and operating systems and applications are patched in a timely fashion. Post-updating VERIFICATION testing of device operation for both continued INTENDED USE and SAFETY is often necessary to meet regulatory quality requirements.

User need: HDOs need to detect traditional malware as well as unauthorized software that could interfere with proper operation of the device/system.

Table 10 – MLDP controls

Standard	Reference	Control
SP 800-53	CM-3	Configuration change control
	IR-1	Incident response policy and procedures
	IR-2	Incident response training
	IR-3	Incident response testing
	IR-4	Incident handling
	IR-5	Incident monitoring
	IR-6	Incident reporting
	IR-7	Incident response assistance
	IR-8	Incident response plan
	MA-3	Maintenance tools
	MP-2	Media access
	RA-5	Vulnerability scanning
	SA-4	Acquisition PROCESS
	SA-8	Security engineering principles
	SA-12	Supply chain protection
	SA-13	Trustworthiness
	SC-7	Boundary protection
	SC-26	Honeypots
	SC-28	Protection of information at rest
	SC-30	Concealment and misdirection
	SC-34	Non-modifiable executable programs
	SC-35	Honeyclients
	SC-37	Out-of-band channels
	SC-44	Detonation chambers
	SI-2	Flaw remediation
	SI-3	Malicious code protection
	SI-4	Information system monitoring
	SI-7	Software and information integrity
	SI-15	Information output filtering

Table 10 *(continued)*

Standard	Reference	Control
ISO IEC 15408-2	FPT_TST	Self test
	FAU_ARP	Security audit automatic response
	FAU_SAA	Security audit analysis
	FDP_IFF	Information flow control functions
	FDP_ITT	Internal TOE transfer
	FDP_SDI	Stored data integrity
	FDP_UIT	Inter_TSF user data integrity transfer protection
	FPT_FLS	Fail secure
	FPT_ITI	Integrity of exported TSF data
	FPT_RPL	Replay detection
	FPT_TRC	Internal TOE TSF data replication consistency
ISO IEC 15408-3	ADV_IMP	Implementation representation
	ADV_INT	TSF internals
	ADV_TDS	TOE design
	ALC_DVS	Development security
	ALC_FLR	Flaw Remediation
IEC 62443-3-3	SR 1.2	Software PROCESS and device identification and authentication
	SR 2.3	Use control for portable and mobile devices
	SR 3.2	Malicious code protection
	SR 3.3	Security functionality VERIFICATION
	SR 5.3	General purpose person-to-person communication restrictions
	SR 6.2	Continuous monitoring
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.4	Contact with special interest groups
	6.2.1	Mobile device policy
	7.2.2	Information security awareness, education and training
	9.1.2	Access to networks and network services
	10.1.1	Policy on the use of cryptographic controls
	11.2.4	Equipment maintenance
	12.1.2	Change management
	12.2.1	Controls against malware
	12.4.1	Event logging
	12.4.2	Protection of log information
	12.4.3	Administrator and OPERATOR logs
	12.4.4	Clock synchronisation
	12.5.1	Installation of software on operational systems
	12.6.1	Management of technical vulnerabilities
	12.6.2	Restrictions on software installation

Table 10 *(continued)*

ISO IEC 27002 ISO 27799	12.7.1	Information systems audit controls
	13.1.1	Network controls
	13.1.2	Security of network services
	13.1.3	Segregation in networks
	13.2.1	Information transfer policies and procedures
	13.2.3	Electronic messaging
	14.2.2	System change control procedures
	14.2.3	Technical review of applications after operating platform changes
	14.2.4	Restrictions on changes to software packages
	14.2.7	Outsourced development
	14.2.8	System security testing
	14.2.9	System acceptance testing
	16.1.2	Reporting information security events
	16.1.7	Collection of evidence
	18.2.2	Compliance with security policies and standards

4.12 Node authentication – NAUT

Requirement goal:	Authentication policies need to be flexible to adapt to local HDO IT policy. As necessary, use node authentication when communicating HEALTH DATA.
User need:	Capability of managing cross-machine accounts on a modality to protect HEALTH DATA access.
	Support for stand-alone and central administration.
	Support for node authentication according to industry standards.
	To detect and prevent entity falsification (provide non-repudiation).

Table 11 – NAUT controls

Standard	Reference	Control
SP 800-53	AC-2	Account management
	AC-7	Unsuccessful logon attempts
	AC-14	Permitted actions without identification or authentication
	AC-17	Remote access
	AC-18	Wireless access
	AC-19	Access control for mobile devices
	AU-2	Audit events
	AU-10	Non-repudiation
	CM-1	Configuration management policy and procedures
	CM-3	Configuration change control
	CM-6	Configuration settings
	IA-1	Identification and authentication policy and procedures

Table 11 *(continued)*

Standard	Reference	Control
SP 800-53	IA-2	Identification and authentication (organizational users)
	IA-3	Device identification and authentication
	IA-4	Identifier management
	IA-5	Authenticator management
	IA-7	Cryptographic module authentication
	IA-8	Identification and authentication (non-organizational users)
	IA-10	Adaptive identification and authentication
	IA-11	Re-authentication
	MA-1	System maintenance policy and procedures
	MA-4	Nonlocal maintenance
	SC-12	Cryptographic key establishment and management
	SC-13	Cryptographic protection
ISO IEC 15408-2	FAU_GEN	Security audit data generation
	FAU_SAA	Security audit analysis
	FCO_NRO	Non-repudiation of origin
	FCO_NRR	Non-repudiation of receipt
	FCS_CKM	Cryptographic key management
	FCS_COP	Cryptographic operation
	FIA_AFL	Authentication failures
	FIA_ATD	User attribute definition
	FIA_SOS	Specification of secrets
	FIA_UAU	User authentication
	FIA_UID	User identification
	FMT_MSA	Management of security attributes
	FPT_RPL	Replay detection
	FTA_LSA	Limitation on scope of selectable attributes
	FTA_TSE	TOE session establishment
	FTP_ITC	Inter-TSF trusted channel
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.2	Software PROCESS and device identification and authentication
	SR 1.3	Account management
	SR 1.4	Identifier management
	SR 1.5	Authenticator management
	SR 1.6	Wireless access management
	SR 1.8	Public key infrastructure (PKI) certificates
	SR 1.9	Strength of public key authentication
	SR 1.10	Authenticator feedback
	SR 1.11	Unsuccessful login attempts
	SR 1.13	Access via untrusted networks
	SR 4.3	Use of cryptography
ISO IEC 27002	5.1.1	Policies for information security

Table 11 *(continued)*

Standard	Reference	Control
ISO 27799	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	6.2.2	Teleworking
	9.2.4	Management of secret authentication information of users
	9.4.1	Information access restriction
	9.4.2	Secure log-on procedures
	10.1.1	Policy on the use of cryptographic controls
	10.1.2	Key management
	11.2.1	Equipment siting and protection
	11.2.4	Equipment maintenance
	11.2.6	Security of equipment and assets off-premises
	12.1.1	Documented operating procedures
	12.1.2	Change management
	12.4.1	Event logging
	12.4.3	Administrator and OPERATOR logs
	12.7.1	Information systems audit controls
	14.2.2	System change control procedures
	18.1.1	Identification of applicable legislation and contractual requirements
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards

4.13 Person authentication – PAUT

Requirement goal: Authentication policies need to 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 devices, network resources and HEALTH DATA and to generate non- repudiatable audit trails. This feature should be able to identify unambiguously and with certainty the individual who is accessing the network, device or resource.

NOTE This requirement is relaxed during “break-glass” operation. See capability “Emergency access.”

User need: Capability of managing accounts on a modality to protect HEALTH DATA access.

Desirable to link to personal settings/preferences.

Support for stand-alone and central administration.

Single sign-on and same password on all workspots.

To detect and prevent person falsification (provide non-repudiation).

Role based access control (RBAC) capability desirable.

Table 12 – PAUT controls

Standard	Reference	Control
SP 800-53	AC-2	Account management
	AC-7	Unsuccessful logon attempts
	AC-14	Permitted actions without identification or authentication
	AC-17	Remote access
	AC-18	Wireless access
	AU-2	Audit events
	AU-10	Non-repudiation
	CM-1	Configuration management policy and procedures
	IA-1	Identification and authentication policy and procedures
	IA-2	Identification and authentication (organizational users)
	IA-4	Identifier management
	IA-5	Authenticator management
	IA-7	Cryptographic module authentication
	IA-8	Identification and authentication (non-organizational users)
	IA-10	Adaptive identification and authentication
	IA-11	Re-authentication
	SC-12	Cryptographic key establishment and management
ISO IEC 15408-2	FAU_GEN	Security audit data generation
	FAU_SAA	Security audit analysis
	FCO_NRO	Non-repudiation of origin
	FCO_NRR	Non-repudiation of receipt
	FCS_CKM	Cryptographic key management
	FCS_COP	Cryptographic operation
	FIA_AFL	Authentication failures
	FIA_ATD	User attribute definition
	FIA_SOS	Specification of secrets
	FIA_UAU	User authentication
	FIA_UID	User identification
	FMT_MSA	Management of security attributes
	FMT_SMR	Security management roles
	FPT_RPL	Replay detection
	FTA_LSA	Limitation on scope of selectable attributes
	FTA_TSE	TOE session establishment
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.1	Human user identification and authentication
	SR 1.3	Account management
	SR 1.4	Identifier management
	SR 1.5	Authenticator management
	SR 1.6	Wireless access management
	SR 1.7	Strength of password-based authentication

Table 12 *(continued)*

Standard	Reference	Control
IEC 62443-3-3	SR 1.8	Public Key Infrastructure (PKI) certificates
	SR 1.9	Strength of public key authentication
	SR 1.10	Authenticator feedback
	SR 1.11	Unsuccessful login attempts
	SR 1.13	Access via untrusted networks
	SR 2.3	Use Control for portable and mobile devices
	SR 2.8	Auditable events
	SR 2.11	Timestamps
	SR 2.12	Non-repudiation
	SR 4.1	Information confidentiality
	SR 4.3	Use of cryptography
	SR 6.2	Continuous monitoring
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	6.2.2	Teleworking
	9.2.1	User registration and de-registration
	9.2.4	Management of secret authentication information of users
	9.4.2	Secure logon procedures
	10.1.1	Policy on the use of cryptographic controls
	10.1.2	Key management
	12.1.1	Documented operating procedures
	12.1.2	Change management
	12.4.1	Event logging
	12.4.3	Administrator and OPERATOR logs
	12.7.1	Information systems audit controls
	18.1.1	Identification of applicable legislation and contractual requirements
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards

4.14 Physical locks on device – PLOK

Requirement goal: Assure that unauthorized access does not compromise the system or data confidentiality, integrity and availability.

User need: Reasonable assurance that 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 device.

Systems are reasonably free from tampering or component removal that might compromise integrity, confidentiality or availability. Tampering (including device removal) is detectable.

Table 13 – PLOK controls

Standard	Reference	Control
SP 800-53	AC-1	Access control
	AU-2	Audit events
	CA-7	Continuous monitoring
	CP-6	Alternate storage site
	MP-2	Media access
	MP-4	Media
	MP-7	Media use
	PE-1	Physical and environmental protection policy and procedures
	PE-2	Physical access authorizations
	PE-3	Physical access control
	PE-4	Access control for transmission medium
	PE-5	Access control for output devices
	PE-6	Monitoring physical access
	PE-9	Power equipment and power cabling
	PE-18	Location of information system components
	PL-2	System security plan
	RA-5	Vulnerability scanning
	SC-8	Transmission confidentiality and integrity
ISO IEC 15408-2	FPT_PHP	TSF physical protection
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.1	Human user identification and authentication
	SR 1.3	Account management
	SR 1.5	Authenticator management
	SR 4.1	Information confidentiality
	SR 7.7	Least functionality
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	8.3.1	Management of removable media
	11.1.1	Physical security perimeter
	11.1.2	Physical entry controls
	11.1.3	Securing offices, rooms and facilities
	11.1.5	Working in secure areas
	11.1.6	Delivery and loading areas
	11.2.1	Equipment siting and protection
	11.2.2	Supporting utilities
	11.2.3	Cabling security
	11.2.4	Equipment maintenance
	12.1.1	Documented operating procedures
	12.4.1	Event logging

Table 13 *(continued)*

Standard	Reference	Control
ISO IEC 27002	12.6.1	Management of technical vulnerabilities
ISO 27799	12.7.1	Information systems audit controls
	16.1.2	Reporting information security events
	18.2.2	Compliance with security policies and standards

4.15 Third-party components in product lifecycle roadmaps – RDMP

Requirement goal: HDOs want an understanding of security throughout the full life cycle of a MEDICAL DEVICE.

MDM plans such that products are sustainable throughout their life cycle according internal quality systems and external regulations. Products provided with clear statement of expected life span.

Goal is to proactively manage impact of life cycle of components throughout a product's full life cycle. This commercial off-the-shelf or 3rd party software includes operating systems, database systems, report generators, medical imaging processing components etc. (assumption is that existing product creation processes already manages hardware component obsolescence). Third party includes here also internal suppliers of security vulnerable components with own life cycle and support programs.

User need: HDO contracts, policy and regulations require that vendors maintain/support the system during product life.

Updates and upgrades are expected when platform components become obsolete.

HDOs and service provider show extreme care in irreversibly erasing HEALTH DATA prior to storage devices 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.

Table 14 – RDMP controls

Standard	Reference	Control
SP 800-53	MA-1	System maintenance policy and procedures
	MA-2	Controlled maintenance
	MA-3	Maintenance tools
	MA-6	Timely maintenance
	MP-1	Media protection policy and procedures
	MP-8	Media downgrading
	SA-1	System and services acquisition policy and procedures
	SA-3	System development life cycle
	SA-4	Acquisition PROCESS
	SA-5	Information system documentation
	SA-8	Security engineering principles
	SA-9	External information system services
	SA-10	Developer configuration management
	SA-11	Developer security testing and evaluation

Table 14 *(continued)*

Standard	Reference	Control
SP 800-53	SA-12	Supply chain protection
	SA-15	Development PROCESS, standards and tools
	SA-16	Developer-provided training
	SA-17	Developer security architecture and design
	SA-21	Developer screening
ISO IEC 15408-2	FMT_MOF	Management of functions in TSF
	FMT_MSA	Management of security attributes
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 4.2	Information persistence
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	12.1.1	Documented operating procedures
	12.1.2	Change management
	14.1.1	Information security requirements analysis and specification
	14.2.1	Secure development policy
	14.2.2	System change control procedures
	14.2.3	Technical review of applications after operating platform changes
	14.2.4	Restrictions on changes to software packages
	14.2.5	Secure system engineering principles
	14.2.6	Secure development environment
	14.2.7	Outsourced development
	14.2.8	System security testing
	14.2.9	System acceptance testing
	18.1.1	Identification of applicable legislation and contractual requirements
	18.1.2	Intellectual property rights
	18.2.1	Independent review of information security
	18.2.2	Compliance with security policies and standards
	18.2.3	Technical compliance review

4.16 System and application hardening – SAHD

Requirement goal: Adjust SECURITY CONTROLS on the MEDICAL DEVICE and/or software applications such that security is maximized ("hardened") while maintaining INTENDED USE. Minimize attack vectors and overall attack surface area via port closing; service removal, etc.

User need: User requires a system that is stable and provides just those services specified and required according to its INTENDED USE with a minimum of maintenance activities.

HDO IT requires systems connected to their network to be secure on delivery and hardened against misuse and attacks.

It is desirable for the user to inform the MDM of suspected security breaches and perceived weaknesses in user equipment.

Table 15 – SAHD controls

Standard	Reference	Control
SP 800-53	AC-19	Access control for mobile devices
	CM-6	Configuration settings
	CM-7	Least functionality
	SA-14	Criticality analysis
	SA-17	Developer security architecture and design
	SA-18	Tamper resistance and detection
	SC-25	Thin nodes
	SC-28	Protection of information at rest
	SC-29	Heterogeneity
	SC-30	Concealment and misdirection
	SC-31	Covert channel analysis
	SC-35	Honeyclients
	SC-40	Wireless link protection
	SC-41	Port and I/O device access
	SC-42	Sensor capability and data
	SC-43	Usage restrictions
	SI-11	Error handling
ISO IEC 15408-2	FMT_MSA	Management of security attributes
	FPT_PHP	TSF physical protection
ISO IEC 15408-3	ASE_TSS	TOE summary specification
	ADV_ARC	Security architecture
	ADV_TDS	TOE design
	ALC_DEL	Delivery
	ACO_COR	Composition rationale
	ACO_REL	Reliance of independent component
IEC 62443-3-3	SR 2.1	Authorization enforcement
	SR 2.2	Wireless use control
	SR 2.3	Use control for portable and mobile devices
	SR 3.4	Software and information integrity
	SR 5.1	Network segmentation
	SR 5.2	Zone boundary protection
	SR 5.3	General purpose person-to-person communication restrictions
	SR 5.4	Application partitioning
	SR 7.7	Least functionality
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	12.4.2	Protection of log information
	12.5.1	Installation of software on operational systems
	12.6.2	Restrictions on software installation
	13.1.1	Network controls
	13.1.2	Security of network services

Table 15 *(continued)*

Standard	Reference	Control
ISO IEC 27002	13.1.3	Segregation in networks
ISO 27799	14.2.1	Secure development policy
	14.2.4	Restrictions on changes to software packages
	14.2.8	System security testing
	18.2.2	Compliance with security policies and standards

4.17 Security guides – SGUD

Requirement goal: Ensure that security guidance for OPERATORS and administrators of the system is available. Separate manuals for OPERATORS and administrators (including MDM sales and service) are desirable as they allow understanding of full administrative functions to be kept only by administrators.

User need: OPERATOR should be clearly informed about his 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 RISK ASSESSMENT per appropriate regulatory requirement.

Sales and service also need information about the system's SECURITY CAPABILITIES and secure way of working.

It is desirable for the user to know how and when to inform the MDM of suspected security breaches and perceived weaknesses in user equipment.

Table 16 – SGUD controls

Standard	Reference	Control
SP 800-53	AC-1	Access control policy and management
	AC-2	Account management
	AT-1	Security awareness and training policy and procedures
	AT-2	Security awareness training
	AT-3	Security training
	CP-1	Contingency planning policy and procedures
	CP-2	Contingency plan
	CP-3	Contingency training
	IR-1	Incident response policy and procedures
	IR-2	Incident response training
	IR-7	Incident response assistance
	IR-8	Incident response plan
	PL-1	Security planning policy and procedures
	PL-2	System security plan
	PL-4	Rules of behaviour
	PL-7	Security concept of operations

Table 16 *(continued)*

Standard	Reference	Control
SP 800-53	PL-8	Information security architecture
	PS-1	Personnel security policy and procedures
	SA-4	Acquisition PROCESS
	SA-5	Information system documentation
	SA-16	Developer-provided training
	SC-1	System and communications protection policy and procedures
	SI-1	System and information integrity policy and procedures
	SI-2	Flaw remediation
	SI-3	Malicious code protection
	SI-4	Information system monitoring
	SI-5	Security alerts, advisories, and directives
	SI-6	Security functionality VERIFICATION
	SI-7	Software and information integrity
	SI-8	Spam protection
	SI-10	Information input validation
	SI-11	Error handling
	SI-12	Information handling and retention
	SI-17	Fail-safe procedures
	PM-1	Information security program plan
	PM-9	RISK MANAGEMENT strategy
	PM-12	Insider threat program
	PM-14	Testing, training and monitoring
	PM-15	Contacts with security groups and associations
	PM-16	Threat awareness program
ISO IEC 15408-2	FAU_GEN	Security audit data generation
	FAU_SAR	Security audit review
	FDP_ACC	Access control policy
	FDP_ACF	Access control functions
ISO IEC 15408-3	APE_REQ	Security requirements
	ASE_INT	ST introduction
	ASE_CCL	Conformance claims
	ASE_SPD	Security problem definition
	ASE_OBJ	Security objectives
	ASE_TSS	TOE summary specification
	ADV_FSP	Functional specification
	AGD_OPE	Operational user guidance
IEC 62443-3-3	*No applicable* SECURITY CONTROLS	
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.1.2	Segregation of duties
ISO IEC 27002	6.1.3	Contact with authorities

Table 16 *(continued)*

Standard	Reference	Control
ISO 27799	6.2.1	Mobile device policy
	6.2.2	Teleworking
	7.2.2	Information security awareness, education and training
	9.4.2	Secure logon procedures
	12.1.1	Documented operating procedures
	13.2.1	Information transfer policies and procedures
	14.1.1	Information security requirements analysis and specification
	14.2.1	Secure development policy
	14.2.2	System change control procedures
	14.2.3	Technical review of applications after operating platform changes
	15.1.1	Information security policy for supplier relationships
	16.1.1	Responsibilities and procedures
	16.1.5	Response to information security incidents
	18.1.1	Identification of applicable legislation and contractual requirements
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards
	18.2.3	Technical compliance review

4.18 HEALTH DATA storage confidentiality – STCF

Requirement goal: MDM establishes technical controls to mitigate the potential for compromise to the integrity and confidentiality of HEALTH DATA stored on products or removable media.

User need: Reasonable assurance that HEALTH DATA stored on products or media is and stays secure.

Encryption has to be considered for HEALTH DATA stored on MEDICAL DEVICES based on RISK ANALYSIS.

For HEALTH DATA stored on removable media, encryption might protect confidentiality/ integrity for clinical users but also MDM service and application engineers collecting clinical data.

A mechanism for encryption key management consistent with conventional use, service access, emergency “break-glass” access.

Encryption method and strength takes into consideration the volume (extent of record collection/aggregation) and sensitivity of data.

Table 17 – STCF controls

Standard	Reference	Control
SP 800-53	SC-12	Cryptographic key establishment and management
	SC-13	Cryptographic protection
	SC-17	Public key infrastructure certificates
	SC-28	Protection of information at rest
ISO IEC 15408-2	FCS_CKM	Cryptographic key management
	FCS_COP	Cryptographic operation
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 4.1	Information confidentiality
	SR 4.3	Use of cryptography
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	6.2.2	Teleworking
	8.2.2	Labelling of information
	8.2.3	Handling of assets
	8.3.1	Management of removable media
	9.1.1	Access control policy
	9.1.2	Access to networks and network services
	9.4.1	Information access restriction
	10.1.1	Policy on the use of cryptographic controls
	10.1.2	Key management
	12.1.4	Separation of development, testing and operational environments
	12.3.1	Information backup
	14.3.1	Protection of test data
	18.1.3	Protection of records
	18.1.4	Privacy and protection of personally identifiable information
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards

4.19 Transmission confidentiality – TXCF

Requirement goal: Device meets local laws, regulations and standards (e.g. USA HIPAA, EU 95/46/EC derived national laws) according to HDO needs to ensure the confidentiality of transmitted HEALTH DATA.

User need: Assurance that HEALTH DATA confidentiality is maintained during transmission between authenticated nodes. This allows transport of HEALTH DATA over relatively open networks and/or environment where strong HDO IT policies for HEALTH DATA integrity and confidentiality are in use.

See IEC TR 80001-2-3:2012 for more information on RISK MANAGEMENT for wireless network systems.

Table 18 – TXCF controls

Standard	Reference	Control
SP 800-53	PE-4	Access control for transmission medium
	SC-1	System and communications protection policy and procedures
	SC-8	Transmission confidentiality and integrity
	SC-12	Cryptographic key establishment and management
	SC-13	Cryptographic protection
ISO IEC 15408-2	FCS_CKM	Cryptographic key management
	FCS_COP	Cryptographic operation
	FDP_ITT	Internal TOE transfer
	FDP_UCT	Inter-TSF user data confidentiality transfer protection
	FPT_ITT	Internal TOE TSF data transfer
	FTP_ITC	Inter-TSF trusted channel
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 1.8	Public key infrastructure (PKI) certificates
	SR 4.1	Information confidentiality
	SR 4.3	Use of cryptography
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	6.2.1	Mobile device policy
	6.2.2	Teleworking
	10.1.1	Policy on the use of cryptographic controls
	10.1.2	Key management
	12.2.1	Controls against malware
	12.3.1	Information backup
	13.1.1	Network controls
	13.1.2	Security of network services
	13.1.3	Segregation in networks
	13.2.1	Information transfer policies and procedures
	13.2.2	Agreements on information transfer
	13.2.3	Electronic messaging
	13.2.4	Confidentiality or non-disclosure agreements
	14.1.2	Securing application services on public networks
	14.1.3	Protecting application services transactions
	18.1.1	Identification of applicable legislation and contractual requirements
	18.1.3	Protection of records
	18.1.4	Privacy and protection of personally identifiable information
	18.1.5	Regulation of cryptographic controls
	18.2.2	Compliance with security policies and standards

4.20 Transmission integrity – TXIG

Requirement goal: Device protects the integrity of transmitted HEALTH DATA.

User need: Assurance that integrity of HEALTH DATA is maintained during transmission. This allows transmission of HEALTH DATA over relatively open networks or environment where strong policies for HEALTH DATA integrity are in use.

Table 19 – TXIG controls

Standard	Reference	Control
SP 800-53	PE-4	Access control for transmission medium
	SC-1	System and communications protection policy and procedures
	SC-8	Transmission confidentiality and integrity
	SI-1	System and information integrity policy and procedures
	SI-3	Malicious code protection
ISO IEC 15408-2	FDP_ITT	Internal TOE transfer
	FDP_UIT	Inter_TSF user data integrity transfer protection
	FPT_ITI	Integrity of exported TSF data
	FPT_ITT	Internal TOE TSF data transfer
	FTP_ITC	Inter-TSF trusted channel
ISO IEC 15408-3	*No applicable* SECURITY CONTROLS	
IEC 62443-3-3	SR 3.1	Communication integrity
	SR 3.8	Session integrity
ISO IEC 27002 ISO 27799	5.1.1	Policies for information security
	5.1.2	Review of the information security policy
	12.2.1	Controls against malware
	12.3.1	Information backup
	13.1.1	Network controls
	13.1.2	Security of network services
	13.1.3	Segregation in networks
	13.2.1	Information transfer policies and procedures
	13.2.2	Agreements on information transfer
	13.2.3	Electronic messaging
	18.2.2	Compliance with security policies and standards

Bibliography

[1] IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[2] IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[3] IEC TR 80001-2-3:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks*

[4] ISO IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

[5] ISO IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

[6] ISO IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

[7] ISO IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

[8] ISO 27799:—[7)], *Health informatics – Information security management in health using ISO/IEC 27002*

[9] HIMSS/NEMA Standard HN 1-2013, *Manufacturer Disclosure Statement for Medical Device Security*

[10] NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*, Richard Kissel, Editor, Computer Security Division Information Technology Laborator, National Institute of Standards and Technology, May 2013

[11] NIST SP 800-53 Revision 4:2013, *Security and Privacy Controls for Federal Information Systems and Organizations*, http://dx.doi.org/10.6028/NIST.SP.800-53r4

_____

7) To be published.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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