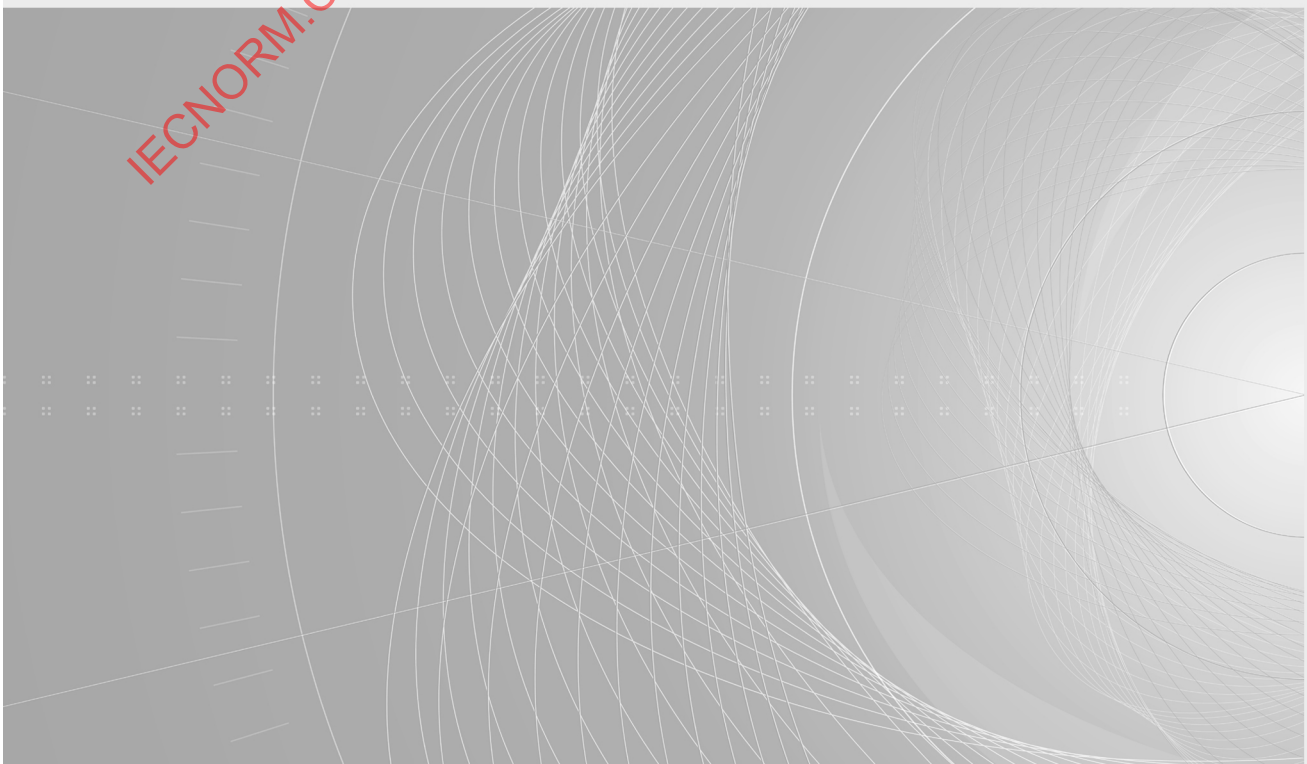
IEC/TR 80001-2-2

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls



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

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

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

IEC/TR 80001-2-2

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XA

ICS 11.040.01

ISBN 978-2-83220-202-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

FOREWORD

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

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

IEC 80001-2-2, which is a technical report, has been prepared a Joint Working Group of subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62*:* Electrical equipment in medical practice and ISO technical committee 215: Health informatics.

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

Enquiry draft	Report on voting
62A/783/DTR	62A/807/RVC

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

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

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IEC 80001-1, which deals with the application of RISK MANAGEMENT to IT-networks incorporating medical devices, provides the roles, responsibilities and activities necessary for RISK MANAGEMENT. This technical report provides additional guidance in how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT PROCESS and stakeholder communications and agreements.

The informative set of common, high-level SECURITY CAPABILITIES presented here i intended to be the starting point for a security-centric discussion between vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sized RESPONSIBLE ORGANIZATIONS as each evaluates RISK under the capabilities and decides what to include or not include according to its RISK tolerance and resource planning. This technical report might be used in the preparation of documentation designed to communicate product SECURITY CAPABILITIES and options. This documentation could be used by the RESPONSIBLE ORGANIZATION as input to their IEC 80001 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. Other IEC-80001-1 technical reports will provide step-by-step guidance in the RISK MANAGEMENT PROCESS. Furthermore, the SECURITY CAPABILITIES encourage the disclosure of more detailed security controls – perhaps those specified in one or more security standards as followed by the RESPONSIBLE ORGANIZATION or the MEDICAL-DEVICE manufacturer (for example, ISO 27799:2008, ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2011, the ISO 22600 series, the ISO 13606 series, and ISO/HL7 10781:2009, which covers the Electronic Health Record System Functional Model). This report remains agnostic as to the underlying controls framework; it only proposes a structure for the disclosure and communication among the RESPONSIBLE ORGANIZATION (here called the healthcare delivery organization – HDO), the MEDICAL DEVICE manufacturer (MDM) and the IT-vendor.

The capabilities outlined here comprise a disclosure set of controls which support the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity or system/data availability. Capabilities can be added to or further elaborated as the need arises. Controls are intended to protect both data and systems but special attention is given to the protection of both PRIVATE DATA and its subset called HEALTH DATA. Both of these special terms have been defined to carefully avoid any law-specific references (e.g., EC Sensitive Data or USA ePHI).

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

1 Scope

This part of IEC 80001 creates a framework for the disclosure of security-related capabilities and RISKS necessary for managing the RISK in connecting MEDICAL DEVICES to IT-NETWORKS and for the security dialog that surrounds the IEC 80001-1 RISK MANAGEMENT of IT-NETWORK connection. This security report presents an informative set of common, high-level security-related capabilities useful in understanding the user needs, the type of security controls to be considered and the RISKS that lead to the controls. INTENDED USE and local factors determine which exact capabilities will be useful in the dialog about RISK.

The capability descriptions in this report are intended to supply:

a) health delivery organizations (HDOs),

b) MEDICAL DEVICE manufacturers (MDMs), and

c) IT vendors

with a basis for discussing RISK and their respective roles and responsibilities toward its management. This discussion among the RISK partners serves as the basis for one or more RESPONSIBILITY AGREEMENTS as specified in IEC 80001-1.

The present report provides broad descriptions of the security-related capabilities with the intent that any particular device or use of a device will have to have at least one additional level of specification detail under each capability. This will often be site and application-specific and may invoke RISK and security controls standards as applicable.

At this introductory stage of IEC 80001-1 standardization, the SECURITY CAPABILITIES in this report provide a common, simple classification of security controls particularly suited to MEDICAL IT NETWORKS and the incorporated devices. The list is not intended to constitute or to support rigorous IT security standards-based controls and associated programs of certification and assurance such as might be found in other ISO standards (e.g., ISO/IEC 15408 with its Common Criteria for Information Technology Security Evaluation). The present report does not contain sufficient detail for exact specification of requirements in a request for proposal or product security disclosure sheet. However, the classification and structure can be used to organize such requirements with underlying detail sufficient for communication during the purchase and integration PROCESS for a MEDICAL DEVICE or IT equipment component. Again, this report is intended to act as a basis for discussion and agreement sufficient to initial integration project RISK MANAGEMENT. Additionally, security only exists in the context of the organizational security policies. Both:

a) the security policies of the healthcare delivery organization (HDO), and

b) the product and services security policies of the MEDICAL DEVICE manufacturer (MDM)

are outside of the scope of this report. In addition, the Technical Report does not address clinical studies where there is a need for securing the selective disclosure of PRIVATE DATA or HEALTH DATA.

2 Normative references

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

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

3 Terms and definitions

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

[SOURCE: IEC 80001-1:2010, definition 2.5, modified — two notes integral to understanding the scope of the original definition have been deleted.]

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

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

3.3
EVENT MANAGEMENT
PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

[SOURCE: IEC 80001-1:2010, definition 2.7]

3.4
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY

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

3.5
HAZARD
potential source of HARM

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

3.6
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD(S)

[SOURCE: ISO 14971:2007, definition 2.4]

3.7
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

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

3.8
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

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

3.9
INTEROPERABILITY
a property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, definition 2.11]

3.10
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
a system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, definition 2.12, modified – the two notes to the original definition have not been retained.]

3.11
KEY PROPERTIES
three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, definition 2.13]

3.12
MEDICAL DEVICE
means any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

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

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

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

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

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

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

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

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

3.13
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

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

3.14
OPERATOR
person handling equipment

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

3.15
PRIVATE DATA
any information relating to an identified or identifiable person

3.16
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

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

3.17
RESIDUAL RISK
RISK remaining after RISK CONTROL measures have been taken

[SOURCE: IEC 80001-1:2010, definition 2.20]

3.18
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

[SOURCE: IEC 80001-1:2010, definition 2.21, modified – a note to the original definition, containg examples, has not been retained.]

3.19
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry: In this Technical Report, to avoid confusion associated with the notion of security responsibility, the RESPONSIBLE ORGANIZATION of IEC 80001-1 is given the name healthcare delivery organization (HDO).

[SOURCE: IEC 80001-1:2010, definition 2.22, modified — a note to the original definition, containing examples, has not been retained; a note to entry has been added.]

3.20
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

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

3.21
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

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

3.22
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

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

3.23
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: IEC 80001-1:2010, definition 2.26]

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

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

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

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

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

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

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

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

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

4 Use of SECURITY CAPABILITIES

4.1 Structure of a SECURITY CAPABILITY entry

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

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

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

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

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

The SECURITY CAPABILITIES address security RISK CONTROL options as follows:

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

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

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

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

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

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

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

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

5 SECURITY CAPABILITIES

5.1 Automatic logoff – ALOF

Applicable: **Standard:** N/A

Policies: Local HDO IT Policies

Reference material: N/A

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 log off 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.

5.2 Audit controls – AUDT

Applicable: **Profile:** IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)

IHE Radiology Technical Framework

Policies: Local HDO IT Policies

Reference material: NEMA: S&P Auditing

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 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.

5.3 Authorization – AUTH

Applicable:

NOTE 1 Based on, but not to be confused with authenticating users.

Standard: ANSI/INCITS 359-2004 Role-Based Access Control

There are some frameworks that might prove useful here:

IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication (ATNA) / Enterprise User Authentication (EUA) / Cross-Enterprise User Assertion (XUA)

IETF: Transport Layer Security (TLS) 1.2 (RFC 5246)

ITU-T: Recommendation X.509. "Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks

Policies: Local HDO IT Policies

Reference material:

IHE White Paper – Access Control

IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication

ISO/TS 22600-1:2006 *Health informatics -- Privilege management and access control – Part 1: Overview and policy management*

ISO/TS 13606-4:2009 *Health informatics -- Electronic health record communication – Part 4: Security*

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 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 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 HDO to effectively deliver healthcare while (1) maintaining system and data security and (2) following the principle of appropriate data access minimization. Authorization may be managed locally or enterprise-wide (e.g., via centralized directory).

NOTE 2 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.

5.4 Configuration of security features – CNFS

Applicable:	**Standard:**	N/A
	Policies:	Local HDO IT Policies
Reference material:	N/A	
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.	

5.5 Cyber security product upgrades – CSUP

Applicable:	**Guideline:**	OIS Guidelines for Security Vulnerability Reporting and Response V2.0 1 September 2004
	Policies:	Local HDO IT Policies
Reference material:	NEMA SPC Patching off-the-shelf software used in medical information systems. October 2004.	
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.

5.6 HEALTH DATA de-identification – DIDT

Applicable:

Standard: NEMA DICOM Supplement 142: Clinical Trial De-identification Profiles.

NEMA DICOM Supplement 55: Attribute Level Confidentiality (including De-identification) 5 Sept 2002.

ISO 25237:2008, *Health Informatics – pseudonimization*,

NOTE Pseudonimization and use of any manner of patient-identifying keys permit data to be re-identified and, as such, are not de-identification methods.

Policies: Local HDO IT Policies

Reference material: Sweeney, L. 2002. *K*-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based systems, 10(5), 557-570.

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.

5.7 Data backup and disaster recovery – DTBK

Applicable:

Standard: N/A

Policies: Local HDO IT Policies

Reference material: ISO/IEC 20000-2:2012, Service continuity planning and testing

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 may not be appropriate for smaller, low-cost devices and may, 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)

5.8 Emergency access – EMRG

Applicable:

Standard: N/A

Policies: Local HDO IT Policies

Reference material: NEMA SPC White paper: *Breakglass*

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.

5.9 HEALTH DATA integrity and authenticity – IGAU

Applicable:	**Standard:**	N/A.
	Policies:	Local HDO IT Policies
Reference material:	NEMA Security and Privacy Auditing	
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.	

5.10 Malware detection/protection – MLDP

Applicable:	**Standard:**	N/A.
	Policies:	Local HDO IT Policies
Quote from regulation:	Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	
Reference material:	NEMA Defending Medical Information Systems Against Malicious Software	
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.	

5.11 Node authentication – NAUT

Applicable:	**Profile:**	IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)
	Policies:	NEMA/COCIR/JIRA Joint Security and Privacy Committee draft White Paper: *Management of Machine Authentication Certificates,* 10 February 2005

SANS Security Policy Project

Local HDO IT Policies

Reference material: N/A

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 industry standards.

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

5.12 `Person authentication – PAUT

Applicable: **Profile:** IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)

IHE PWP profile (Personal White Pages)

IHE EUA (Enterprise User Authentication)

IHE XUA (Cross-Enterprise User Assertion)

Policies: SANS Security Policy Project
Local HDO IT Policies

Reference material: N/A

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: Creation and use of unique accounts for users and role based access control (RBAC,local and remote) for a network connected device to control and monitor network access and activity.

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

Users might need to associate personal preferences with user accounts. This might help devices and systems used by multiple OPERATORS, departments or even multiple HDOs. 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).

5.13 Physical locks on device – PLOK

Applicable: **Standard:** N/A

Policies: Local HDO IT Policies

Reference material: none

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.

5.14 Third-party components in product lifecycle roadmaps – RDMP

Applicable: **Standard:** N/A

Policies: Local HDO IT Policies

Quote from regulation: N/A

Reference material: N/A

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, MIP components etc. (assumption is that existing PCP already manages hardware component obsolescence). 3rd 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 vendor 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.

5.15 System and application hardening – SAHD

Applicable: **Standard:** N/A

Policies: Local HDO IT Policies

SANS Policy Project

Reference material: SANS Information Security Reading Room (Step-by-step Guides)

CIS Benchmarks and Security Tools

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.

5.16 Security guides – SGUD

Applicable:
Standard: N/A
Policies: Local HDO IT Policies

Reference material: Manufacture Disclosure Statement for Medical Device Security (MDS2)

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.

5.17 HEALTH DATA storage confidentiality – STCF

Applicable:
Standard: NEMA DICOM Part 15: Security and System Management Profiles

NEMA DICOM Supplement 51: Media security

NEMA DICOM Supplement 55: Attribute level confidentiality (including De-identification) 5 Sept 2002 (Final text)

Policies: Local HDO IT Policies

Reference material: Schneier B. 1996. Applied Cryptography, Second Edition. John Wiley & Sons, New York, NY.

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.

5.18 Transmission confidentiality – TXCF

Applicable:	**Profile:**	IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)
	Policies:	Local HDO IT Policies
Reference material:	NEMA SPC Certificates white paper.	
	NEMA DICOM Part 15: Security and System Management Profiles	
	IETF: Transport Layer Security in Network Working Group RFC 5246 August 2008: The TLS Protocol Version 1.2	
	ITU-T: Recommendation X.509. “Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks"	
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.	

5.19 Transmission integrity – TXIG

Applicable:	**Profile:**	IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)
	Policies:	Local HDO IT Policies
Reference material:	NEMA SPC Certificates white paper	
	NEMA DICOM Part 15: Security and System Management Profiles	
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.	

6 Example of detailed specification under SECURITY CAPABILITY: Person authentication – PAUT

The previous “Security Capabilities” clause provided a description of the basic capability along with user need and source material. In actual use, a capability will be more detailed by the MDM in a security statement or the HDO in a request for product security information. The following is an example of a MDM’S disclosure under the “Person Authentication” capability. For the target MEDICAL DEVICE, the disclosure would indicate presence or absence of that SECURITY CAPABILITY.

PAUT: Person authentication
The term user is considered to refer to the caregiver and/or the network and security management roles in the healthcare delivery environment.

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:	Creation and use of unique accounts for users and role-based access control (RBAC,local and remote) for a network connected device to control and monitor network access and activity. Capability of managing accounts on a modality to protect HEALTH DATA access. Users might need to associate personal preferences with user accounts. This might help devices and systems used by multiple OPERATORS, departments or even multiple HDOs. 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).
PAUT.1	Product supports locally administered (on the device) User accounts operation. Capability for HDO IT and optionally the service engineer to manage the local User accounts.
PAUT.2	Use of HDO central administration of User accounts according the IHE EUA profile.
PAUT.3	Support for identifying multiple simultaneous users (e.g. OPERATOR + clinician) for role based access control.
PAUT.4	Single sign-on for modalities with multiple workspots or single workspots running multiple applications.
PAUT.5	Visible indication of who is the current user to make it easier to identify who is using the system, and determine if it is necessary to close the session.
PAUT.6	Support fast user switching. By supporting this, signing off and on is not a time-consuming task.

7 References

This section describes the detail behind the abbreviated references used in the security capabilities clause above.

Reference Document	Title
CIS	The Center for Internet Security Benchmarks and Security Tools http://cisecurity.org/
DICOM	Digital Imaging and Communications in Medicine sponsored by NEMA Standards: NEMA DICOM Part 15: Security and System Management Profiles NEMA DICOM *Supplement 55: Attribute level confidentiality (including De-identification)* 5 Sept 2002 (Final text) NEMA DICOM *Supplement 51: Media security* NEMA DICOM *Supplement 142: Clinical Trial De-identification profiles*
IETF	The Internet Engineering Task Force Papers:

Reference Document	Title
	Network Working Group RFC 5246 August 2008: *The TLS Protocol Version 1.2*: http://www.ietf.org/rfc/rfc5246.txt
IHE	Integrated Healthcare Enterprise: http://www.ihe.net/Technical_Framework/ Note on ATNA: (see http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication) *Audit Trail and Node Authentication (ATNA) Integration Profile* is designed to support access control by limiting network access between nodes and limiting access to each node to authorized users (locally authenticated). It involves User Authentication, Connection Authentication, and Audit Trails. It supports actors including • Secure Nodes, • Audit Repository, and • Time Server. The actions are to maintain time, authenticate nodes, and recording audit events. It is based upon standards established by the IETF IT Infrastructure Technical Framework including standards for Secure Communications, Audit Log Transport, Audit Log Message. Among these standards are RFC 5246, WS-I Basic Security Profile 1.1, RFC 5424, RFC 5425, RFC 5426, RFC 3164,RFC 3881, DICOM: Supplement 95 (ISO 12052 ftp://medical.nema.org/medical/dicom/final/sup95_ft.pdf).
Local HDO IT Policies	Policies created by our product user's organization specifying the acceptable use of information technology.
NEMA SPC	Joint Security and Privacy Committee of NEMA/COCIR/JIRA: http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/ White papers: SPC Security and Privacy Auditing in Health Care Information Technology. SPC Break-Glass: An approach to granting emergency access to health care systems. December 2004. SPC Defending medical information systems against malicious software. December 2003.SPC *Patching off-the-shelf software used in medical information systems*, October 2004. SPC *Remote Service Interface - Solution (A) - Version 2: IPSec over the Internet Using Digital Certificates*, December 2003.
ITU	International Telecommunication Union Telecommunication Standardization Section (ITU-T) Recommendation X.509 (11/2008) ISO/IEC 9594-8:2008: http://www.itu.int/itu-t/recommendations/index.aspx?ser=X
OIS	Organization for Internet Safety http://www.oisafety.org/ publication: OIS *Guidelines for Security Vulnerability Reporting and Response V2.0* 1 September 2004: http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclo

Reference Document	Title
	sure.pdf
SANS	The SANS (SysAdmin, Audit, Network, Security) Institute: http://www.sans.org The SANS Security Policy Project – "…everything you need for rapid development and implementation of information security policies.": http://www.sans.org/resources/policies/ SANS Information *Security Reading Room*: http://www.sans.org/reading_room/
Schneier	Bruce Schneier. 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition. J Wiley & Sons. N.B., if you use this book, please search the web for errata as there are some well-known errors present.
WEDI	Workgroup for Electronic Data Interchange Security and Privacy Workgroup (SNIP) White papers: WEDI-SNIP Introduction to Security Final Rule Final Version – January 2004: (membership required) http://www.wedi.org WEDI-SNIP SECURITY: Audit Trail Clarification White Paper Version 5.0 November 7, 2003: (membership required) http://www.wedi.org

8 Other resources

8.1 General

This clause contains some description and reference to standards and resources that also itemize the security capabilities of MEDICAL DEVICES or applications. The focus of each of these resources is slightly different and therefore they should be carefully applied according to their original context.

8.2 Manufacture disclosure statement for medical device security (MDS2)

Manufacture Disclosure Statement for Medical Device Security—developed by HIMSS to capture MEDICAL DEVICE SECURITY CAPABILITIES. This form is currently going through an international open consensus PROCESS under NEMA and HIMSS.

http://www.himss.org/content/files/MDS2FormInstructions.pdf

8.3 Application security questionnaire (ASQ)

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

http://www.himss.org/asp/topics_FocusDynamic.asp?faid=212

8.4 The Certification Commission for Healthcare Information Technology (CCHIT)

The Certification Commission for Healthcare Information Technology or CCHIT is a recognized certification body (RCB) for electronic health records and their networks, and an independent, voluntary, private-sector initiative. It is our mission to accelerate the adoption of health information technology by creating an efficient, credible and sustainable certification program.

8.5 http://www.cchit.org/get_certifiedHL7 Functional Electronic Health Record (EHR)

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

http://www.hl7.org/ehr/

8.6 Common criteria – ISO/IEC 15408

Common criteria – ISO/IEC 15408 (all parts) that would describe the capabilities of a system.

9 Standards and frameworks

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

NSA	US National Security Agency NSA Security Configuration Guides http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
IETF	The Internet Engineering Task Force Papers: Network Working Group RFC 5246 August 2008: *The TLS Protocol Version 1.2*. http://www.ietf.org/rfc/rfc5246.txt
SANS	The SANS (SysAdmin, Audit, Network, Security) Institute: http://www.sans.org/ The SANS Security Policy Project – "…everything you need for rapid development and implementation of information security policies." http://www.sans.org/resources/policies SANS Information *Security Reading Room* http://www.sans.org/rr/ SANS security glossary http://www.sans.org/security-resources/glossary.php
WEDI	Workgroup for Electronic Data Interchange Security and Privacy Workgroup (SNIP) White papers: WEDI-SNIP Introduction to Security Final Rule Final Version – January 2004: (membership required) WEDI-SNIP SECURITY: Audit Trail Clarification White Paper Version 5.0 November 7, 2003: (membership required)
IHE	Integrated Healthcare Enterprise http://www.ihe.net/Technical_Framework/ IHE ATNA profile (Audit Trail and Node Authentication Integration Profile) IHE EUA (Enterprise User Authentication) IHE RAD TF (*Radiology Audit Trail)* draft version for public comment.

Annex A
(informative)

Sample scenario showing the exchange of security information

A.1 Introduction to the security characteristics scenario

This annex contains documents shared in the first round of the exchange of security characteristics information between a hypothetical MEDICAL DEVICE manufacturer (MDM – The Widget Corporation) and a healthcare delivery organization (HDO – The New Town Hospital). The product under consideration is a DICOM Workstation called “FOOBAR 2.0”.

The MDM has received a request for IEC-80001 information on the FOOBAR 2.0 from the HDO. Section 2 contains the MDM’s initial communication about the SECURITY CAPABILITIES of the FOOBAR 2.0. This is followed by the HDO’s review of the security characteristics “offering” with their comments and additional questions.

This annex gives a simplified example of what the MDM of the FOOBAR would provide to a healthcare delivery organization who is contemplating the purchase or integration of the FOOBAR. It might be shared by the MDM under a non-disclosure agreement with the HDO or, perhaps, the MDM would publish the capabilities to their HDO Internet site. Either way, it is the first “offering” of information about the detailed SECURITY CAPABILITIES of a MEDICAL DEVICE under consideration. Likewise, the HDO’s reply is a first-response back to the MDM intended to identify areas of general agreement and understanding, issues that were not apparent in the document, and questions that need to be resolved in subsequent communications.

Of course, there is much more to a purchase, installation, and maintenance arrangement. As an overall context for this example of a simplified MEDICAL DEVICE purchase and later FOOBAR medical IT-NETWORK connection project, we outline some basic steps that might be followed during security RISK MANAGEMENT (see IEC 80001-1 for full details):

a) The HDO requests or locates the MDM security characteristics summary (Section 2 below).

b) The HDO examines the FOOBAR security characteristics report and responds in writing (Section 3 below).

c) The HDO contacts the MDM and obtains answers to some details not present in the FOOBAR report.

d) A decision is made by the HDO to complete a purchase and the MDM decides to accept the purchase pending some elements of the purchase to be worked out. The HDO uses the security input and dialog with the MDM to decide if this is a partner who will work in good faith.

e) Various elements of project planning and execution are carried out including an explicit RESPONSIBILITY AGREEMENT with regard to RISK MANAGEMENT in the IT-NETWORK connection. The HDO and the MDM are clear about how various RISKS are managed. Some are managed intrinsically by the device security characteristics, some have to be mitigated by HDO security controls (technical and/or administrative).Preliminary estimates of RESIDUAL RISK are made. This step may be included in the purchase or may be preliminary to purchase.

f) The HDO purchases the FOOBAR system and contracts for support for the connection/integration project.

g) RISKS are analyzed and RESIDUAL RISK is surfaced and understood by the HDO and, where it is found acceptable in light of the benefits of the FOOBAR connection, the integration project is executed with the device connected to the HDO’s MEDICAL IT-NETWORK.

h) The FOOBAR operates in a RISK managed manner as part of the HDO’s MEDICAL IT-NETWORK.

i) Sustainable activities relating to emerging vulnerabilities, monitoring, EVENT MANAGEMENT are all put in place with necessary agreements with FOOBAR service providers.

j) Decommissioning of storage devices and systems are considered in local procedures that contain requirements for data destruction, logging and auditing the decommissioning PROCESS.

NOTE This is a simple scenario with an agreement between two parties only. In real-life situations there may be other parties involved such as IT vendors, third-party integrators, etc. The actual steps will be decided on a case-by-case basis.

To be clear that these are sample pages from a hypothetical exchange, the security characteristics document from the manufacturer (MDM) has pages highlighted with a blue box border. The security characteristics document that contains the response from the hospital (HDO) back to the MDM has pages with an orange box border.

***Disclaimer**: this scenario is provided without warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability, completeness and fitness for a particular purpose. The entire RISK as to the quality and performance of the provided information is with you.*

The example describes a fictional device (FOOBAR 2.0) and is intended to provide a suggested way of beginning a security dialog between the MDM and the HDO.

A.2 Manufacturer (MDM) Security Characteristics Report – "The Offering"

The following pages are the FOOBAR 2.0 MDM's statement of the security of the product arranged in a manner consistent with the advice of the IEC 80001-1 Security Technical Report (this document). This starts with an expression of interest by a healthcare deliver organization. The MDM responds with an email/letter and an attached FOOBAR 2.0 Security Characteristics Document.

Joan Kowalski, CISSP

IT Security Officer

New Town General Hospital

Dear Ms. Kowalski,

Thank you for your interest in the FOOBAR 2.0 DICOM PACS Workstation. We have received your signed non-disclosure agreement and please find attached for your records a copy signed by us.

You will also find attached the detailed security information about the FOOBAR 2.0 in a form consistent with IEC 80001-1 Security Technical Report. We always try to be clear and consistent in our communications with customer about security risk and I trust that this confidential document meets your needs.

Of course, security can be a highly complex issue when attaching a new medical device to a hospital IT-network. We look forward to working with you to resolve any questions or issues you see in considering our product for purchase and integration into your Medical IT-network.

Thank you for considering Widget Corporation's products in your technology plans and we look forward to working with you this important purchase and the full integration of our product into your operational network.

Please let me know if you have any questions on our security capabilities and/or risks that might be present in this state-of-the-art product.

Best regards,

Jose Armas

FOOBAR Product Sales Manager,

Widget Corporation

cc:

1. Doubly signed Non-disclosure Agreement dated May 1, 2010
2. FOOBAR 2.0 Security Characteristics Report (IEC80001-1)

FOOBAR 2.0 Security Characteristics Document per IEC 80001-1
– MANUFACTURER'S OFFERING –

A. Brief Intended Purpose definition of the device FOOBAR 2.0

The Advanced DICOM Viewing Station "FOOBAR 2.0" is connected to the DICOM network and enables its users to access DICOM 3.0 images and data outside the radiology department or imaging center in order to review these medical reports and medical images.

FOOBAR 2.0 is able to retrieve the medical data either from the dedicated remote archive present on the DICOM network or from a local hard drive.

Because of the internal storage capabilities, FOOBAR 2.0 is able to display the medical data even outside the boundaries of the DICOM network.

Security options are included in order to control access to medical imaging data, depending upon user privileges; access is logged in audit logs.

B. Detailed Specification of SECURITY CAPABILITIES

In the security capabilities detailed below, each capability is tagged with the four-level-acronym of the SECURITY CAPABILITY. To assist in communication about specific characteristics under a SECURITY CAPABILITY, each is tagged with an identifier composed of the identifier and a two digit sequential number. This is intended to help in discussions and written communication about specific characteristics.

ALOF: Automatic logoff

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.

Identifier	Capability
/ALOF.01/	A screen-saver starts automatically 5 min after last keystroke / mouse movement operation. ***Remark:*** *the local authorized IT administrator can set the delay for this action and even disable the screen-saver.*
/ALOF.02/	The screen-saver clears all displayed HEALTH DATA from the screen.
/ALOF.03/	The screen-saver does not log-off the user / does not terminate the session.
/ALOF.04/	User has to log-in after occurrence of the screen-saver.
/ALOF.05/	The user-session terminates automatically 60 min after last keystroke / mouse movement / touchscreen operation. ***Remark:*** *the local authorized IT administrator can set the delay for this action and even disable the automatic log-off.*

AUDT: Audit controls

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.

Identifier	Capability
/AUDT.01/	Access, modification or deletion to any HEALTH DATA is recorded and stored on the dedicated remote DICOM archive.
/AUDT.02/	Download of HEALTH DATA (to the internal storage of the device) is recorded and stored on the dedicated remote DICOM archive.
/AUDT.03/	In case the device is used outside the boundaries of the DICOM network, access to any HEALTH DATA is stored on the internal storage of the device.
/AUDT.04/	After re-connecting the device back to the DICOM-Network, the audit-trails recorded on the internal storage of the device during offline-use are synchronized with the dedicated remote DICOM archive.
/AUDT.05/	Refers to /CNFS.01/: all changes to the SECURITY CAPABILITIES are included to the audit-trail of the device.

CNFS: Configuration of security features

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

Identifier	Capability
/CNFS.01/	The local authorized IT administrator can set / disable the available SECURITY CAPABILITIES of the device.
/CNFS.02/	Refers to /AUDT.05/: in case the local authorized IT administrator set / disables / changes the settings of the available SECURITY CAPABILITIES of the device, the action is logged in an audit-trail.

DTBK: Data backup and disaster recovery

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

Identifier	Capability
/DTBK.01/	FOOBAR 2.0 provides a back-up (built-in) to store the system-settings to an externally connected mass-storage-device (e.g. an USB-Stick).
/DTBK.02/	FOOBAR 2.0 provides a back-up (built-in) to store the audit-trails to an externally connected mass-storage-device (e.g. an USB-Stick).
/DTBK.03/	The audit-trails are encrypted accordingly in order to prevent loss of confidential information, contained in HEALTH DATA (like patient name, DOB, etc.).
/DTBK.04/	Backup of locally stored HEALTH DATA can only be done back to the dedicated remote DICOM archive. ***Rationale:*** *this restrictive functionality is required in order to ensure that the HEALTH DATA remains consistent.*

DIDT: HEALTH DATA de-identification

Goal: Ability of equipment (application software or additional tooling) to directly remove information that allows identification of PATIENT.

Identifier	Capability
/DIDT.01/	FOOBAR 2.0 does not support any means to directly remove information that allows identification of PATIENT.

STCF: HEALTH DATA storage confidentiality

Goal: MANUFACTURER ensures that unauthorized access does not compromise the integrity and confidentiality of HEALTH DATA stored on products or removable media.

Identifier	Capability
/STCF.01/	HEALTH DATA, stored on the internal storage of FOOBAR 2.0 is encrypted. Used algorithm: AES (Rijndael), Encryption strength: 256 BIT. ***Remark:*** *this setting cannot be changed by local IT administrator.*
/STCF.02/	The secured / encrypted HEALTH DATA is accessible after successful boot only. See also /MLDP.04/.
/STCF.03/	Only the required HEALTH DATA is decrypted (required for the current interaction / usage / display). Currently not used HEALTH DATA remains encrypted.
/STCF.04/	Boot partition, operating system, temporary data on internal mass storage device, etc. is also encrypted. Used algorithm: AES (Rijndael), Encryption strength: 256 BIT. ***Remark:*** *this setting cannot be changed by local IT administrator.*
/STCF.05/	Accidental power-down of the system does not affect the encryption of the HEALTH DATA on the mass storage device. In no circumstance of operation is unencrypted HEALTH DATA present on the internal mass storage device.
/STCF.06/	Connection to the dedicated remote archive present on the DICOM network can be established via VPN.

EMRG: Emergency access

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

Identifier	Capability
/EMRG.01/	Break-glass functionality provided: even without personal user id and authentication clinical user can gather access to HEALTH DATA. ***Remark:*** *remember that this functionality may be changed / disabled by local IT administrator.*

Identifier	Capability
/EMRG.02/	Usage of the break-glass functionality /EMRG.01/ requires the usage of a general user id and authentication (in order to prevent patients or bystanders to access HEALTH DATA).
/EMRG.03/	Each use of the break-glass functionality /EMRG.01/ will be recorded in the audit-trail.
/EMRG.04/	Each use of the break-glass functionality /EMRG.01/ can be reported automatically to a defined user account, e.g. by means of eMail.

SGUD: Security guides

Goal: Ensure that security guidance for OPERATOR and administrator of the system and MANUFACTURER sales and service is available. Separate manuals are desirable as they allow understanding of full administrative functions to be kept only by administrators.

Identifier	Capability
/SGUD.01/	Security guidance for OPERATOR is included in the instructions for use of FOOBAR 2.0. See chapter 13.
/SGUD.02/	Security guidance for administrator is included in the technical information of FOOBAR 2.0. See chapter 17.

IGAU: HEALTH DATA integrity and authenticity

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.

Identifier	Capability
/IGAU.01/	HEALTH DATA, stored on the mass storage of FOOBAR 2.0 in order to display the medical data outside the boundaries of the DICOM network, is secured by adequate checksum (SHA1) in order to assure integrity of data.
/IGAU.02/	Backup-capabilities are provided. See chapter DTBK: Data backup and disaster recovery

MLDP: Malware detection/protection

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 defense in depth approach to security.

Identifier	Capability
/MLDP.01/	All unnecessary network-ports of FOOBAR 2.0 are closed. ***Remark 01:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details. See /SGUD.02/.* ***Remark 02:*** *this capability cannot be changed by local IT-administrator.*

Identifier	Capability
/MLDP.02/	The operating-system on the boot-device of FOOBAR 2.0 is protected against authorized / unauthorized changes. After re-boot, the system is back in the initial state. ***Remark:*** *this capability cannot be changed by local IT-administrator.*
/MLDP.03/	All relevant files are secured by adequate checksum (SHA1) and checked during boot-sequence. In case of error detection, system does not start but displays an error message. ***Remark:*** *this capability cannot be changed by local IT-administrator.*
/MLDP.04/	The secured / encrypted HEALTH DATA is accessible after successful boot only. See also /STCF.01/. ***Remark:*** *this capability cannot be changed by local IT-administrator.*

PAUT: Person authentication

Goal: Authentication policies need to be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when communicating HEALTH DATA.

Identifier	Capability
/PAUT.01/	FOOBAR 2.0 supports local and global management of accounts. ***Remark:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details.*
/PAUT.02/	FOOBAR 2.0 supports withdrawal of accounts. ***Remark:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details.*
/PAUT.03	FOOBAR 2.0 supports fast user switching. By supporting this, signing off and on is not a time-consuming task.

PLOK: Physical locks on device

Goal: Assure that unauthorized access does not compromise the integrity and confidentiality of HEALTH DATA stored on products or removable media.

Identifier	Capability
/PLOK.01/	Because of the chosen encryption, FOOBAR 2.0 does not require physical lock-outs.

CSUP: Cyber security Product upgrades

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).

Identifier	Capability
/CSUP.01/	We herewith confirm that internal procedures for market surveillance are in place in order to determine current threads, concerning cyber security. In case patches are necessary, technical support can be addressed. ***Remark:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details.*
/CSUP.02/	Based on the internal design of the device, we (the manufacturer) do not allow the HDO to install any unauthorized patches.

RDMP: 3rd party components in product lifecycle roadmaps

Goal: Manufacturer plans such that products are sustainable throughout their life cycle according to internal quality systems and external regulations.

Identifier	Capability
/RDMP.01/	We herewith confirm that we maintain/support the system during estimated product life. In case maintenance / repair / patches are necessary, technical support can be addressed. ***Remark:*** *refer to the technical information of FOOBAR 2.0 (chapter 42) for further details.*

SAHD: System and application hardening

Goal: Minimize attack vectors and surface area via port closing; service removal, etc.

Identifier	Capability
/SAHD.01/	All capabilities to ensure that a system that is stable and provides just those services specified and required according to its INTENDED USE with a minimum of maintenance activities and to allow healthcare providers / HDOs to connect FOOBAR 2.0 to their network are addressed in chapter MLDP: Malware detection/protection in *the technical information of FOOBAR 2.0 (chapter 38)*.

AUTH: Authorization

Goal: Provide access to MEDICAL DEVICE data and functions only as necessary to perform the tasks required by the HDO consistent with the INTENDED USE of the device.

Identifier	Capability
/AUTH.01/	Despite the administrative functions listed below, only personnel authorized by us (the manufacturer) have access to service functions and capabilities. Besides administrative tasks, allowed in the technical documentation, we do not allow further repair by unauthorized personnel. ***Remark:*** *refer to the technical information of FOOBAR 2.0 for further details.*

Identifier	Capability
/AUTH.02/	So-called Administrator logins are provided with FOOBAR 2.0 for – general server administration; – installation of updates/fixes; – adding more FOOBAR clients; – master user administration; – backup operations.
/AUTH.03/	So-called Master User logins are pre-configured and can be added to – fix/join reports/patient data; – recover lost reports; – general user administration; – edit and maintain general FOOBAR application configuration.

TXDF: Transmission confidentiality

Goal: MANUFACTURER demonstrates that its equipment meets multiple national standards or regulations (USA HIPAA, EU 95/46/EC, HBP 517, etc.) according to HDO needs to ensure the confidentiality of transmitted HEALTH DATA.

Identifier	Capability
/TXDF.01/	See /STCF.06/: connection to the dedicated remote archive present on the DICOM network can be established via VPN. ***Remark:*** *refer to the technical information of FOOBAR 2.0 (chapter 33) for further details.*
/TXDF.02/	Upon request: we (the manufacturer) will provide certificates to demonstrate compliance with applicable national regulation. As these certificates vary, depending on the country, please contact technical service for further details.

TXIG: Transmission integrity

Goal: Device protects the integrity of transmitted HEALTH DATA

Identifier	Capability
/TXIG.01/	See /STCF.06/: connection to the dedicated remote archive present on the DICOM network can be established via VPN. This capability assures that integrity of HEALTH DATA is maintained during transmission and allows FOOBAR 2.0 transmission of HEALTH DATA over relatively open networks or environment where strong policies for HEALTH DATA integrity are in use. ***Remark:*** *refer to the technical information of FOOBAR 2.0 (chapter 33) for further details.*

A.3 HDO's reply to the MDM Security Characteristics Report – "The Response"

The following pages are the New Town Hospital's (HDO) response to the FOOBAR 2.0 Widget Corporation (MDM) statement of the SECURITY CAPABILITIES of the product (given in Section 3). Overall New Town is pleased with the security information as presented but there a few things missing and a few questions to be resolved before the New Town Security Officer can give a "proceed" message to the purchasing committee. The New Town Hospital's Security Officer responds with an annotated (right-most column added – in blue) FOOBAR 2.0 Security Characteristics Document. The response is started with an email/letter.

Jose Armas
FOOBAR Product Sales Manager,
Widget Corporation

Dear Mr. Armas,

Thank you for your detailed response to my request for security information on Widget Corporation's FOOBAR 2.0 DICOM PACS Workstation. We find your IEC 80001-1 based document highly informative and a good start to our purchase and installation project prior to connecting the PACS Workstation to New Town Hospital's Medical IT-network

Although I appreciate your attempts at clarity and risk transparency, I have some comments and questions. I have taken the liberty of adding a column to your document and placing my comments to the right of your description of the security characteristics. Where I found a security feature lacking, I have added a row in the appropriate section. Further, where I recognized the security capability and where it seemed likely to meet our needs, my comment reads "Acknowledged." Although not yet ready to "Accept" at this early date, I thought it useful to use this term so we could focus on other, more important issues, in our first discussion.

Once you have reviewed the attached document, I suggest that we have a teleconference to resolve items that can easily be clarified by telephone. If New Town Hospital Radiology and Purchasing decide to go forward with the purchase of your equipment and installation, we will have ample opportunity to further detail the security risks and mitigations in the integration project planning and implementation.

My office will contact you regarding the follow-up phone discussion.

Sincerely, Joan Kowalski, CISSP
IT Security Officer
New Town General Hospital

Cc: New Town Hospital Response to FOOBAR 2.0 Security Characteristics Report (IEC80001-1)

FOOBAR 2.0 security characteristics
– New Town Hospital RESPONSE to Proposal from Widget Corporation –

The example contains a first reaction of a fictional health delivery organization New Town General Hospital. This HDO is considering the purchase of several FOOBAR 2.0 devices. This document section describes reaction/questions/issues on the security statement of the manufacturer of the FOOBAR 2.0 MEDICAL DEVICE.

A. Short description of the hospital

The New Town General Hospital consists of multi-medical disciplines. Additional technical staff positions support the clinicians in the fields of privacy and security. The FOOBAR workstation will be placed into the Pulmonary Intensive Care Unit for use by Pulmonologists and Radiology consultants.

B. Short description of the network

The network is divided into a general network and special network segments for medical products.

System and network administration is done by a local team of well-trained network administrators. A training program on medical product judicial aspects exists.

C. Short description of security aspects

The network security strategy relies on a mixed protection and sensor strategy.

Certain network areas are protected by security equipment to prevent infections by malicious software. The whole network is monitored by sensor networks which reports malware infections exceeding a threshold level.

Please note that the text in **BLACK** in Section 4 below was provided by Widget Corporation for their FOOBAR 2.0 device. The text comments in ***BLUE*** *italic* below are the response by New Town Hospital's security staff.

D. Detailed Specification of SECURITY CAPABILITIES

ALOF: Automatic logoff

Goal: Reduce the RISK of unauthorized access to HEALTH DATA from an unattended workspots. Prevent misuse by other users if a system or workspot is left idle for a period of time.

Identifier	Capability	*HDO Comments/needs*

Identifier	Capability	*HDO Comments/needs*
/ALOF.01/	A screen-saver starts automatically 5 minutes after last keystroke / mouse movement operation. ***Remark:*** *the local authorized IT administrator can set the delay for this action and even disable the screen-saver.*	*acknowledged by HDO* *desirable would be a longer time period since diagnostics has pauses with inactivity*
/ALOF.02/	The screen-saver clears all displayed HEALTH DATA from the screen.	*acknowledged by HDO*
/ALOF.03/	The screen-saver does not log-off the user / does not terminate the session.	*acknowledged by HDO*
/ALOF.04/	User has to log-in after occurrence of the screen-saver.	*acknowledged by HDO*
/ALOF.05/	The user-session terminates automatically 60 minutes after last keystroke / mouse movement / touchscreen operation. ***Remark:*** *the local authorized IT administrator can set the delay for this action and even disable the automatic log-off.*	*acknowledged by HDO*
		additional: a master account would be desirable to override a user account and log in a screen-saved box

AUDT: Audit controls

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.

Identifier	Capability	*HDO Comments/needs*
/AUDT.01/	Access, modification or deletion to any HEALTH DATA is recorded and stored on the dedicated remote DICOM archive.	*Feature not needed in this application.*
/AUDT.02/	Download of HEALTH DATA (to the internal storage of the device) is recorded and stored on the dedicated remote DICOM archive.	*Feature not needed in this application.*
/AUDT.03/	In case the device is used outside the boundaries of the DICOM network, access to any HEALTH DATA is stored on the internal storage of the device.	*Feature not needed in this application.*
/AUDT.04/	After re-connecting the device back to the DICOM-Network, the audit-trails recorded on the internal storage of the device during offline-use are synchronized with the dedicated remote DICOM archive.	*Feature not needed in this application.*

Identifier	Capability	*HDO Comments/needs*
/AUDT.05/	Refers to /CNFS.01/: all changes to the SECURITY CAPABILITIES are included to the audit-trail of the device.	*Feature not needed in this application.*

CNFS: Configuration of security features

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

Identifier	Capability	*HDO Comments/needs*
/CNFS.01/	The local authorized IT administrator can set / disable the available SECURITY CAPABILITIES of the device.	*HDO acknowledges*
/CNFS.02/	Refers to /AUDT.05/: in case the local authorized IT administrator set / disables / changes the settings of the available SECURITY CAPABILITIES of the device, the action is logged in an audit-trail.	*HDO acknowledges*
		HDO misses an important security feature (e.g., port blocking). An investment plan is created to calculate the costs for additional equipment which compensates these deficiencies.

DTBK: Data backup and disaster recovery

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

Identifier	Capability	*HDO Comments/needs*
/DTBK.01/	FOOBAR 2.0 provides a back-up (built-in) to store the system-settings to an externally connected mass-storage-device (e.g. a USB-stick).	*Feature not needed in this application.*
/DTBK.02/	FOOBAR 2.0 provides a back-up (built-in) to store the audit-trails to an externally connected mass-storage-device (e.g. a USB-stick).	*Feature not needed in this application.*
/DTBK.03/	The audit-trails are encrypted accordingly in order to prevent loss of confidential information, contained in HEALTH DATA (like patient name, DOB, etc.).	*Feature not needed in this application.*

Identifier	Capability	*HDO Comments/needs*
/DTBK.04/	Backup of locally stored HEALTH DATA can only be done back to the dedicated remote DICOM archive. ***Rationale:*** *this restrictive functionality is required in order to ensure that the HEALTH DATA remains consistent.*	*Feature not needed in this application.*

DIDT: HEALTH DATA de-identification

Goal: Ability of equipment (application software or additional tooling) to directly remove information that allows identification of PATIENT.

Identifier	Capability	*HDO Comments/needs*
/DIDT.01/	FOOBAR 2.0 does not support any means to directly remove information that allows identification of PATIENT.	*HDO acknowledges* ***Note to HDO Purchasing:*** *This device capability prevents use in research and teaching*
		HDO needs to receive from the MDM an exact specification of all data put into the DICOM 3.0 files. This is essential to write its own file format manipulators (e.g., deidentification, transfer to research archive).

STCF: HEALTH DATA storage confidentiality

Goal: Manufacturer ensures that unauthorized access does not compromise the integrity and confidentiality of HEALTH DATA stored on products or removable media.

Identifier	Capability	*HDO Comments/needs*
/STCF.01/	HEALTH DATA, stored on the internal storage of FOOBAR 2.0 is encrypted. Used algorithm: AES (Rijndael), Encryption strength: 256 BIT. ***Remark:*** *this setting cannot be changed by local IT administrator.*	*HDO needs more information of the key generation PROCESS.* *When the key generation is done by the manufacturer, a PROCESS must exist that makes a separation of those parties that generate the key and those doing a hardware support case, to prevent legal privacy issues when a defect harddrive is returned to the manufacturer to get a replacement device. How is key management done?*

Identifier	Capability	*HDO Comments/needs*
/STCF.02/	The secured / encrypted HEALTH DATA is accessible after successful boot only. See also /MLDP.04/.	*HDO acknowledges* *During reboot, does the device require a special password (other than user logon) to proceed to operational state?*
/STCF.03/	Only the required HEALTH DATA is de-crypted (required for the current interaction / usage / display). Currently not used HEALTH DATA remains encrypted.	*HDO acknowledges*
/STCF.04/	Boot partition, operating system, temporary data on internal mass storage device, etc. is also encrypted. Used algorithm: AES (Rijndael), Encryption strength: 256 BIT. ***Remark:*** *this setting cannot be changed by local IT administrator.*	*HDO acknowledges*
/STCF.05/	Accidental power-down of the system does not affect the encryption of the HEALTH DATA on the mass storage device. In no circumstance of operation is unencrypted HEALTH DATA present on the internal mass storage device.	*HDO acknowledges*
/STCF.06/	Connection to the dedicated remote archive present on the DICOM network can be established via VPN.	*HDO acknowledges*

EMRG: Emergency access

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

Identifier	Capability	*HDO Comments/needs*
/EMRG.01/	Break-glass functionality provided: even without personal user id and authentication clinical user can gather access to HEALTH DATA. ***Remark:*** *remember that this functionality may be changed / disabled by local IT administrator.*	*HDO acknowledges*
/EMRG.02/	Usage of the break-glass functionality /EMRG.01/ requires the usage of a general user id and authentication (in order to prevent patients or bystanders to access HEALTH DATA).	*HDO acknowledges*
/EMRG.03/	Each use of the break-glass functionality /EMRG.01/ will be recorded in the audit-trail.	*HDO acknowledges*

Identifier	Capability	*HDO Comments/needs*
/EMRG.04/	Each use of the break-glass functionality /EMRG.01/ can be reported automatically to a defined user account, e.g. by means of eMail.	*HDO acknowledges*

SGUD: Security guides

Goal: Ensure that security guidance for OPERATOR and administrator of the system and MANUFACTURER sales and service is available. Separate manuals are desirable as they allow understanding of full administrative functions to be kept only by administrators.

Identifier	Capability	*HDO Comments/needs*
/SGUD.01/	Security guidance for OPERATOR is included in the instructions for use of FOOBAR 2.0. See chapter 13.	*HDO acknowledges*
/SGUD.02/	Security guidance for administrator is included in the technical information of FOOBAR 2.0. See chapter 17.	*HDO acknowledges*

IGAU: HEALTH DATA integrity and authenticity

Goal: Assure that HEALTH DATA has not been altered or destroyed in nonauthorized manner and is from the originator. Assure integrity of HEALTH DATA.

Identifier	Capability	*HDO Comments/needs*
/IGAU.01/	HEALTH DATA stored on the mass storage of FOOBAR 2.0 in order to display the medical data outside the boundaries of the DICOM network, is secured by adequate checksum (SHA1) in order to assure integrity of data.	*HDO knows of weaknesses of SHA1 algorithm and needs a policy statement how manufacturer reacts on cryptographic security issues.*
/IGAU.02/	Backup-capabilities are provided. See chapter DTBK: Data backup and disaster recovery	*HDO acknowledges*

MLDP: Malware detection/protection

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 defense in-depth approach to security.

Identifier	Capability	*HDO Comments/needs*

Identifier	Capability	*HDO Comments/needs*
/MLDP.01/	All unnecessary network-ports of FOOBAR 2.0 are closed. ***Remark 01:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details. See /SGUD.02/.* ***Remark 02:*** *this capability cannot be changed by local IT-administrator.*	*HDO acknowledges*
/MLDP.02/	The operating-system on the boot-device of FOOBAR 2.0 is protected against authorized / unauthorized changes. After re-boot, the system is back in the initial state. ***Remark:*** *this capability cannot be changed by local IT-administrator.*	*HDO needs a statement from the manufacturer how malicious run time modifications are detected.*
/MLDP.03/	All relevant files are secured by adequate checksum (SHA1) and checked during boot-sequence. In case of error detection, system does not start but displays an error message. ***Remark:*** *this capability cannot be changed by local IT-administrator.*	*HDO acknowledges*
/MLDP.04/	The secured / encrypted HEALTH DATA is accessible after successful boot only. See also /STCF.01/. ***Remark:*** *this capability cannot be changed by local IT-administrator.*	*HDO acknowledges*

PAUT: Person authentication

Goal: Authentication policies need to be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when communicating HEALTH DATA.

Identifier	Capability	*HDO Comments/needs*
/PAUT.01/	FOOBAR 2.0 supports local and global management of accounts. ***Remark:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details.*	*HDO needs exact specification of connection to central authentication structures (e.g., PKI, IEEE 802.1X).* *NOTE Please provide Guidance Documents ASAP.*
/PAUT.02/	FOOBAR 2.0 supports withdrawal of accounts. ***Remark:*** *refer to the security guidance for administrator in the technical information of FOOBAR 2.0 (chapter 17) for further details.*	*Can this be done remotely or does the IT Administrator have to be at the FOOBAR device?*

Identifier	Capability	*HDO Comments/needs*
/PAUT.03	FOOBAR 2.0 supports fast user switching. By supporting this, signing off and on is not a time-consuming task.	*HDO acknowledges*

PLOK: Physical locks on device

Goal: Assure that unauthorized access does not compromise the integrity and confidentiality of HEALTH DATA stored on products or removable media.

Identifier	Capability	*HDO Comments/needs*
/PLOK.01/	Because of the chosen encryption, FOOBAR 2.0 does not require physical lock-outs.	*HDO acknowledges*
		HDO asks if keyboard is protected or a illegal key-logger device can easily be attached between the keyboard and cabinet.
		Does the computer cabinet use a lock? Can disk drives be easily removed or replaced?

CSUP: Cyber security Product upgrades

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).

Identifier	Capability	*HDO Comments/needs*