HIMSS/NEMA Standard HN 1-2013

Manufacturer Disclosure Statement for Medical Device Security

Published by

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

The National Electrical Manufacturers Association (NEMA) standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development **process**. This **process** brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the **process** and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEITHER THE HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY (HIMSS) NOR NEMA HAVE POWER, NOR DO THEY UNDERTAKE TO POLICE OR ENFORCE COMPLIANCE WITH THE CONTENTS OF THIS DOCUMENT. NEITHER HIMSS NOR NEMA CERTIFY, TEST, OR INSPECT PRODUCTS, DESIGNS, OR INSTALLATIONS FOR SAFETY OR HEALTH PURPOSES. ANY CERTIFICATION OR OTHER STATEMENT OF COMPLIANCE WITH ANY HEALTH OR SAFETY RELATED INFORMATION IN THIS DOCUMENT SHALL NOT BE ATTRIBUTABLE TO HIMSS OR NEMA AND IS SOLELY THE RESPONSIBILITY OF THE CERTIFIER OR MAKER OF THE STATEMENT.

CONTENTS

FOREWORD

This document consists of the Manufacturer Disclosure Statement for Medical Device Security (MDS^2) form and related instructions how to complete the form. The intent of the MDS^2 form is to supply healthcare providers with important information to assist them in assessing the **vulnerability** and risks associated with protecting **private data** transmitted or maintained by **medical devices** and systems. Because security **risk assessment** spans an entire organization, this document focuses on only those elements of the security **risk assessment process** associated with **medical devices** that maintain or transmit **private data**. A standardized form 1) allows manufacturers to quickly respond to a potentially large volume of information requests from providers regarding the security- related features of the **medical devices** they manufacture; and 2) facilitates the providers' review of the large volume of security-related information supplied by the manufacturers.

The manufacturer-completed MDS^2 should:

(1) Be useful to healthcare provider organizations worldwide. The information presented should be useful for any healthcare delivery organization that aspires to have an effective information security **risk management** program.

(2) Include **device**-specific information addressing the technical security-related attributes of the individual **device** model.

(3) Provide a simple, flexible way of collecting the technical, **device**-specific elements of the common/typical information needed by provider organizations (device **users/operators**) to begin **medical device** information security (i.e., confidentiality, integrity, availability) **risk assessments**.

PLEASE BE ADVISED—The MDS^2 form is not intended to nor should it be used as the sole basis for medical device procurement. Writing procurement specifications requires a deeper and more extensive knowledge of security (including the individual facility's/provider's situation) and the healthcare mission.

Using the information provided by the manufacturer in the MDS^2 form together with information collected about the care delivery environment (e.g., through tools such as ACCE, American College of Clinical Engineering/ECRI's *Guide for Information Security for Biomedical Technology*), the provider's multidisciplinary **risk assessment** team can review assembled information and make informed decisions on implementing a local security management plan.

This form was originally adapted from portions of the ACCE/ECRI Biomedical Equipment Survey Form, a key tool found in *Information Security for Biomedical Technology: A HIPAA* Compliance Guide* (ACCE/ECRI, 2004). This form was published originally in 2004, MDS^2 v. 1.0 (2004-11-01) and then as a joint HIMSS/NEMA standard in 2008, HIMSS/NEMA Standard HN 1-2008.

*Health Insurance Portability and Accountability Act.

In 2010, International Electrotechnical Commission standard IEC 80001-1, *Application of risk management for IT-networks incorporating medical devices*, was published. The standard deals with the application of **risk management** to IT-networks incorporating **medical devices** and provides the roles, responsibilities and activities necessary for **risk management**. In 2012, a Technical Report (TR) supplement to IEC 80001 was published, IEC/TR 80001-2-2, Guidance for the communication of **medical device** security needs, risks and controls. In this supplement, 19 relevant **security capabilities** of a **medical device** or IT component are defined. The 19 high-level **security capabilities** are "…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." Since this goal closely matches the primary objective of the MDS^2 initiative, HIMSS and NEMA have undertaken an expansion and re-categorization of the MDS^2 information provided by manufacturers in order to closely align with the 19 IEC/TR 80001-2-2 security categories.

HIMSS and NEMA recommend that the information in the MDS^2 form be used as part of each organization's security compliance and **risk assessment** efforts. In the preparation of this standards publication, input of **users** and other interested parties has been sought and evaluated.

Inquiries, comments, and proposed or recommended revisions should be submitted to the concerned NEMA product subdivision by contacting the:

Senior Technical Director, Operations
National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

CHANGES FROM PREVIOUS (2008) MDS^2 REVISION

1) Alignment of MDS^2 with International Electrotechnical Commission (IEC) standard 80001-1 supplement, IEC/TR 80001-2-2, *Guidance for the communication of medical device security needs, risks and controls.*

   a) The order and numbering of the (2008) MDS^2 questions has been changed and questions are now placed in either the MANAGEMENT OF PRIVATE DATA section or under the appropriate heading in one of the 19 categories in the SECURITY CAPABILITIES section of the MDS^2 form.

   b) The amount of MDS^2 data requested of **device** manufacturers has been increased to more adequately address the 19 **security capabilities** of IEC/TR 80001-2-2.

   c) MDS^2 term definitions have been added or updated to be consistent with definitions used in IEC 80001 when applicable.

   All of the MDS^2 security-related questions of previous MDS^2 revisions remain in this latest revision with no (or only minor) changes. A cross reference of the 2008 MDS^2 questions vs. 2013 MDS^2 questions is provided in the Annex.

2) De-localization

   Several region-specific references and standards have been removed or replaced with more generic/less region-specific references. The term “Protected Health Information” (PHI), defined in USA HIPAA legislation has been replaced in this MDS^2 revision by the term “**private data**,” as defined in IEC 80001.

Section 1
GENERAL

1.1 SCOPE

Information provided on the MDS^2 form is intended to assist professionals responsible for security **risk assessment processes** in their management of **medical device** security issues. The information on the MDS^2 form is not intended, and may be inappropriate, for other purposes.

1.1.1 The Role of Healthcare Providers in the Security Management Process

The provider organization has the ultimate responsibility for providing effective security management. **Device** manufacturers can assist providers in their security management programs by offering information describing:

- the type of data maintained/transmitted by the manufacturer's **device**;
- how data is maintained/transmitted by the manufacturer's **device**;
- any security-related features incorporated in the manufacturer's **device**.

In order to effectively manage medical information security and comply with relevant regulations, healthcare providers must employ **administrative**, **physical**, and **technical safeguards**—most of which are extrinsic to the actual **device**.

1.1.2 The Role of Medical Device Manufacturers in the Security Management Process

The greatest impact manufacturers can have on **medical device** security is to incorporate **technical safeguards** (i.e., security features) in their **devices** to facilitate healthcare providers' efforts in maintaining effective security programs and meeting any relevant regulatory requirements and/or standards. The **medical device** manufacturing industry is increasingly aware of the importance of having effective security functionality in their **devices**. Manufacturers are generally including such security-related requirements in the production of new **devices** based on provider needs and requirements.

1.2 REFERENCES

The following reference documents are included herein as suggested further reading, supportive material, and related publications:

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

Application of risk management...-- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples, IEC 80001-2-1:2012

Application of risk management...-- Part 2-2: Guidance for the communication of medical device security needs, risks and controls, IEC/TR 80001-2-2:2012

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191 (USA)

Health Insurance Reform: Security Standards; Final Rule, 45 CFR pts.160, 162, 164 (USA, 2003).

EC Data Protection Directive, 95/46/EC (EU 95/46), 1995.

Act on the Protection of Personal Information (Act No. 57 of 2003, Japan).

Personal Information Protection and Electronic Documents Act (PIPEDA), Statutes of Canada, 2000.

Guide for Information Security for Biomedical Technology: A HIPAA Compliance Guide, May 2004, American College of Clinical Engineering (ACCE)/ECRI.

1.3 DEFINITIONS

administrative safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect **private data** and to manage the conduct of an organization's workforce in relation to the protection of that information.

anti-malware: See **anti-virus software**.

anti-virus software: A program that monitors a computer or network to identify all major types of **malware** and prevent or contain **malware** incidents. See also **virus scanner**.

audit trail: Data collected and potentially used to facilitate a security audit.

biometric data: Identifies a human via a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, handwritten signature).

device: A product/system, including hardware, firmware and/or (only) software, etc. Unless otherwise clear from the context, in this MDS^2 document, "device" refers to the **medical device** (the manufacturer's product) which is being addressed by the manufacturer in the MDS^2 form. See also **medical device**.

electronic media: (1) Electronic storage media, including memory devices in computers (hard drives) and any removable/transportable digital memory media, such as magnetic tapes or disks, optical disks, or digital memory cards. (2) Transmission media used to exchange information already in electronic storage media, including, for example, the Internet (wide open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, and private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile and of voice via telephone, are not considered to be transmissions via **electronic media** because the information being exchanged did not exist in electronic form before the transmission.

electronic protected health information (ePHI): (As defined in U.S. HIPAA legislation, 45 CFR 160.103) **individually identifiable health information (IIHI)** that is (1) transmitted by or (2) maintained in **electronic media**.

emergency access: The **process** or mechanism by which a **device user** can quickly and easily access **private data** in urgent (emergency) situations, bypassing the device's established access controls.

individually identifiable health information (IIHI): Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

intended use: Use for which a product, **process** or service is intended according to the specifications, instructions and information provided by the manufacturer. (source: ISO 14971: 2007, *Application of risk management to medical devices*, definition 2.5).

malware: Malicious software. A software program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (source: NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*)

medical device: 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;
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.

operator: Person handling equipment. The person(s) using a **medical device** for its intended purpose.

personal identification number (PIN): A number or code assigned to an individual and used to provide verification of identity.

physical safeguards: The physical measures, policies, and procedures to protect an organization's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

private data: Any information relating to an identified or identifiable person.

process: A set of inter-related or interacting activities which transforms inputs into outputs.

remote service: A support service (e.g., testing, diagnostics, software upgrades) while not physically or directly connected to the device (e.g., remote access via modem, network, Internet).

removable media: **Electronic media** that can be removed from a system without the use of tools.

risk assessment: Conducting an accurate and thorough analysis of the potential risks and **vulnerabilities** to the integrity, availability, and confidentiality of **private data**.

risk management: (1) The ongoing **process** of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. (2) Security measures sufficient to reduce risks and **vulnerabilities** to a reasonable and appropriate level.

security capability: The broad category of technical, administrative or organizational controls to manage risks of confidentiality, integrity, and availability and accountability of data and systems.

technical safeguards: The technology, policies, and procedures to protect data, including **private data** and control access to it.

token: A physical authentication **device** that the **user** carries (e.g., smartcard, SecureID^{tm}, etc.). Often combined with a **PIN** to provide a two-factor authentication method that is generally thought of as superior to simple password authentication.

user: See **operator**.

virus: See **malware**.

virus scanner: A computer program (**anti-virus software**) that detects a **virus** computer program, or other kind of **malware** (e.g., worms and Trojan horses), warns of its presence, and attempts to prevent it from affecting the protected computer. **Malware** often results in undesired side effects generally unanticipated by the **user**.

vulnerability: A flaw or weakness in **device** procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the **device**'s security policy.

1.4 ACRONYMS

CD	Compact Disk
CF	Compact Flash
COTS	Commercial Off-The-Shelf
DVD	Digital Versatile Disk
IP	Internet Protocol
LAN	Local Area Network
OS	Operating System
ROM	Read Only Memory
SD	Secure Digital
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity

Section 2
INSTRUCTIONS FOR OBTAINING, USING, AND COMPLETING MDS^2 FORM

2.1 OBTAINING THE MDS^2 FORM (PROVIDERS)

Completed MDS^2 forms for many **devices** may be available directly from the **device** manufacturer (e.g., manufacturer website).

NOTE—If a manufacturer does not have a completed MDS^2 form for the appropriate **device**(s), enter manufacturer and model information in the appropriate boxes on the top of a blank MDS^2 form, and submit the form(s) and these instructions to the manufacturer's compliance office for completion.

2.2 USING THE MDS^2 FORM (PROVIDERS)

2.2.1 Device Description

The first two sections of the MDS^2 form are used to identify the **device** (DEVICE DESCRIPTION) and describe the type of data maintained/transmitted by the **device** and how the data is maintained/transmitted, etc. (MANAGEMENT OF PRIVATE DATA).

PLEASE BE ADVISED—An indication of a device's ability to perform any listed function (i.e., a "Yes" answer) is not an implicit or explicit endorsement or authorization by the manufacturer to configure the device or cause the device to perform those listed functions.

It is important to distinguish between capability and permission. Unless otherwise indicated, the questions contained on the MDS^2 form generally refer to device capability. Permission is typically a contractual matter separate from the MDS^2 form. Making changes to a medical device without explicit manufacturer authorization may have significant contractual, safety and liability issues.

2.2.2 Explanatory Notes

The MDS^2 form contains space for explanatory notes if the manufacturer needs to explain specific details of the manufacturer's answers to questions.

NOTE—Manufacturers may elect to attach supplementary material if additional space for recommended practices or explanatory notes is necessary.

2.2.3 Security Capabilities

The final section of the MDS^2 (SECURITY CAPABILITIES) contains information on the specific security-related capabilities of the **device**. The information is organized into categories aligned with IEC 80001-2-2, *Guidance for the communication of medical device security needs, risks, and controls*.

2.3 COMPLETING THE MDS^2 FORM (MANUFACTURERS)

2.3.1 General

The manufacturer shall provide the information requested in the MDS^2 form to the appropriate requesting organization, including all requested descriptive information on the type of data maintained/transmitted by the **device**, how the data is maintained/transmitted, and other security-related features incorporated in the **device**, as appropriate.

2.3.2 MDS^2 Form Completion Guidance

DEVICE DESCRIPTION section:

Device Category: This is a free-text field. The manufacturer should use standard terminology that customers would reasonably understand to differentiate key modalities or **device** functionality.

Device Model: This is a free-text field. The manufacturer should fill in the name of the **device** under which it is placed on the market.

Document ID: The document ID is the manufacturer's unique tag used internally to track **device** documentation.

Manufacturer Contact Information: This information identifies how the person or department accountable for the final version of the form can be contacted.

Intended use of device in network-connected environment: This allows the manufacturer to describe the intended function and use of the **device** and, if relevant, how the **device** is expected to be used if connected to a customer's network environment.

MANAGEMENT OF PRIVATE DATA section:

The manufacturer shall answer all questions either "Yes," "No," "N/A" (not applicable), or "See Note."

If additional information is needed for proper interpretation of an answer, manufacturers are encouraged to provide information in explanatory notes.

The following clarifications and suggested guidance are provided to assist the manufacturer in answering the questions:

NOTE—the numbers in this subsection, below, correlate to the question numbers in the MDS^2 form.

A Can this **device** display, transmit or maintain **private data** (including **electronic Protected Health Information** [**ePHI**])?

B Types of **private data** elements that can be maintained by the **device**:

B.1 Demographic (e.g., name, address, location, unique identification number)?

B.2 Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?

B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?

B.4 Open, unstructured text entered by **device user/operator**?

B.5 **Biometric** data?

B.6 Personal financial information (e.g., credit card numbers, health insurance information, etc.)?

C Maintaining **private data** - Can the **device**:

C.1 Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?

C.2 Store **private data** persistently on local media?

C.3 Import/export **private data** with other systems?

C.4 Maintain **private data** during power service interruptions?

D Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:

D.1 Display **private data** (e.g., video display, etc.)?

D.2 Generate hardcopy reports or images containing **private data**?

D.3 Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?

D.4 Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?

D.5 Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?

D.6 Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?

D.7 Import **private data** via scanning?

D.8 Other?

SECURITY CAPABILITIES Section:

The Security Capabilities section of the MDS^2 form contains questions regarding the specific security-related features of the **device**. The questions are organized into the **security capabilities** categories of IEC 80001-2-2, Guidance for the communication of **medical device** security needs, risks and controls.

The manufacturer shall answer all questions either "Yes," "No," "N/A" (not applicable), or "See Note" unless the applicable question requires otherwise.

If additional information is needed for proper interpretation of these answers, manufacturers are encouraged to provide information in explanatory notes.

The following clarifications and suggested guidance are provided to assist the manufacturer in answering the questions:

NOTE—the numbers in this subsection, below, correlate to the question numbers in the MDS^2 form.

1 AUTOMATIC LOGOFF (ALOF): The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.

1-1 Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?

GUIDANCE: Does the **device**, by default or by configuration, always:
- enforce reauthorization after a specified period of inactivity;
- activate a password-protected screen saver after a preselected period of inactivity that effectively prevents **user** access even without logging the **user** off?

The notes section may be used to indicate if/how an auto-logoff or screen lock function can be disabled (e.g., per session or globally with appropriate **user** security warnings/notification?)

1-1.1 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)

GUIDANCE: Can the **user** or administrator configure the amount of time that must lapse before auto-logoff or screen lock occurs? The notes section should be used to indicate whether a **device** with adjustable auto-logoff/screen lock can be configured:
- to a **user** determined time;
- by specific role (e.g., administrator, **user**).

1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key) by the **user**?

GUIDANCE: Can the **user**/**operator** manually invoke the auto-logoff/screen lock via a shortcut key combination (e.g., CTRL-ALT-DELETE)?

2 AUDIT CONTROLS (AUDT): The ability to reliably audit activity on the **device**.

2-1 Can the **medical device** create an **audit trail**?

GUIDANCE: If the answer is no, then answers to 2.2.1 ~ 2.3.2 should be "N/A" and move to question 3-1. Indicate in the notes if the **audit trail** can differentiate between the creation/display/export etc. of **private data** vs. other data. If so, indicate in the notes if the data subject (e.g., patient) is identified for each **private data** event in the log.

2-2 Indicate which of the following events are recorded in the audit log:

2-2.1 Login/Logout?

2-2.2 Display/presentation of data?

GUIDANCE: Does the **audit trail** track the display, printing or other means of presenting data?

2-2.3 Creation/modification/deletion of data?

GUIDANCE: If yes, indicate in notes which (creation and/or modification and/or deletion) of these forms of data manipulation are tracked.

2-2.4 Import/export of data from **removable media**?

GUIDANCE: If yes, indicate in notes which of these forms of data manipulation are tracked.

2-2.5 Receipt/transmission of data from/to external (e.g., network) connection?

GUIDANCE: If yes, indicate in notes which of these forms of data manipulation are tracked.

2-2.5.1 **Remote service** activity?

2-2.6 Other events? (Describe in the notes section.)

GUIDANCE: If yes, indicate in notes which other forms of data manipulation are tracked.

2-3 Indicate what information is used to identify individual events recorded in the audit log:

2-3.1 **User** ID?

2-3.2 Date/time?

GUIDANCE: Indicate in the notes how the **device** time is set. e.g., indicate if the **device** can synchronize time to a Network Time Server (NTP, SNTP, etc.)

3 AUTHORIZATION (AUTH): The ability of the **device** to determine the authorization of **users**.

3-1 Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?

GUIDANCE: If the **device** can prevent unauthorized access, indicate in the notes what physical or **technical safeguards** the **device** uses to prevent access (password, biometrics, keycard, etc.)

3-2 Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?

3-3 Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?

GUIDANCE: Indicate in the notes if the **device** supports more than one privileged account (e.g., administrator, root).
Indicate in the notes if the manufacturer imposes any restrictions on **users** regarding the use of administrator accounts.

4 CONFIGURATION OF SECURITY FEATURES (CNFS): The ability to configure/re-configure **device security capabilities** to meet **users'** needs.

4-1 Can the **device** owner/**operator** reconfigure product **security capabilities**?

GUIDANCE: Indicate in the notes if the manufacturer imposes any restrictions on **users** regarding the reconfiguring of product **security capabilities**.

5 CYBER SECURITY PRODUCT UPGRADES (CSUP): The ability of on-site service staff, **remote service** staff, or authorized customer staff to install/upgrade **device**'s security patches.

5-1 Can relevant OS and **device** security patches be applied to the **device** as they become known/available?

GUIDANCE: If the manufacturer does not authorize **users** to apply OS and **device** security patches, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note. The manufacturer may optionally choose to describe any restrictions directly in the note or reference external documents where a description of these restrictions can be found or simply write, "Information on manufacturer restrictions/limitations can be provided upon request," for example.

5-1.1 Can security patches or other software be installed remotely?

GUIDANCE: If the manufacturer does not authorize **users** to install OS/**device** security patches or other software remotely, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note.
The manufacturer may optionally choose to describe any restrictions directly in the note or reference external documents where a description of these restrictions can be found or simply write, "Information on manufacturer restrictions/limitations can be provided upon request," for example.

6 HEALTH DATA DE-IDENTIFICATION (DIDT): The ability of the **device** to directly remove information that allows identification of a person.

6-1 Does the **device** provide an integral capability to de-identify **private data**?

GUIDANCE: Mention in the notes if the de-identification **process** references/adheres to any specific de-identification standard/guideline. Also mention if the de-identification procedure is configurable.

7 DATA BACKUP AND DISASTER RECOVERY (DTBK): The ability to recover after damage or destruction of **device** data, hardware, or software.

7-1 Does the **device** have an integral data backup capability (e.g., backup to remote storage or **removable media** such as tape, disk)?

GUIDANCE: This refers to an integrated feature or option that supports information backup to remote storage or **removable media** (e.g., optical disk, magnetic disk, tape, etc.) If appropriate, mention in a note any limitations or restrictions on data backup/disaster recovery.

8 EMERGENCY ACCESS (EMRG): The ability of the **device user** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.

8-1 Does the **device** incorporate an **emergency access** (“break-glass”) feature?

GUIDANCE: See “Definitions” section for a description of the term **emergency access**. If applicable, describe in the notes for section 2 (e.g., question 2-2.6) the **device**’s ability to log instances of **emergency access**. The manufacturer may also choose to mention in the notes for question 8-1:

- If/how the **device** prompts an emergency **user** for a (temporary/"emergency") **user** name and/or hospital/clinic ID # that is then recorded in the audit log.
- If/how the **device** identifies or "flags" data acquired during an "emergency" session (e.g., data acquired without an authorized **user** logged in).

9 HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU): How the **device** ensures that data processed by the **device** has not been altered or destroyed in a non-authorized manner and is from the originator.

9-1 Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?

GUIDANCE: This question refers only to the integrity of stored data. Information regarding system controls intended to prevent unauthorized changes to the application program or system in general should be provided in the notes to the System and Application Hardening (SAHD) section.

10 MALWARE DETECTION/PROTECTION (MLDP): The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).

10-1 Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?

GUIDANCE: The manufacturer may optionally choose to describe any restrictions on **malware** support (purchase/installation/configuration) directly in the note or reference external documents where a description of these restrictions can be found.

10-1.1 Can the **user** independently (re-)configure **anti-malware** settings?

10-1.2 Does notification of **malware** detection occur in the **device user** interface?

GUIDANCE: Optionally, in the notes describe how the **user** is notified when **malware** is detected.

10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected?

GUIDANCE: Optionally, in the notes describe any restrictions on who is or is not authorized by the manufacturer to repair **malware** infected systems, or reference external documents where a description of these restrictions can be found.

10-2 Can the **device** owner install or update **anti-virus software**?

GUIDANCE: Answer “Yes” if the **device user**/owner has the ‘technical’ ability to install or update **anti-virus software**. However, If the manufacturer does not authorize **users** to install or update **anti-virus software**, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note.

10-3 Can the **device** owner/**operator** (technically/physically) update **virus** definitions on manufacturer-installed **anti-virus** software?

GUIDANCE: Answer “Yes” if the system **user**/owner has the technical ability to update **virus** definitions/**virus** signature files. However, if the manufacturer does not authorize **users** to update these **virus** signature files or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note. For whitelisting

solutions, indicate in the notes if the **device** manufacturer restricts the owner's/**user**'s ability to modify the list of authorized applications (the white list).

11 NODE AUTHENTICATION (NAUT): The ability of the **device** to authenticate communication partners/nodes.

11-1 Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?

12 PERSON AUTHENTICATION (PAUT): The ability of the **device** to authenticate **users**.

12-1 Does the **device** support **user**/**operator**-specific username(s) and password(s) for at least one **user**?

GUIDANCE: If the **device** supports identification beyond username and password, describe it briefly in the notes (e.g., "uses XYZ secure **token** mechanism").

12-1.1 Does the **device** support unique **user**/**operator**-specific IDs and passwords for multiple **users**?

12-2 Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?

GUIDANCE: If yes, please specify which mechanism in the notes section.

12-3 Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?

GUIDANCE: If yes, provide any detail in notes as desired.

12-4 Can default passwords be changed at/prior to installation?

GUIDANCE: If the manufacturer imposes specific restrictions, please explain in the notes.

12-5 Are any shared user IDs used in this system?

GUIDANCE: Answer "Yes" if, by design, the **device** is intended to be used with shared IDs. If yes, specify if the shared IDs are for service and/or **user** mode. Additionally, indicate if the IDs/passwords are common across multiple instances of the same model(s) of the **device**. (This excludes "emergency" or "break glass" accounts.)

12-6 Can the **device** be configured to enforce creation of **user** account passwords that meet established (organization specific) complexity rules? If there are any limitations to password constraints please list in the notes section.

GUIDANCE: Answer "Yes" if password complexity is configurable. Answer "No" if password complexity is not configurable, regardless of complexity requirements. Indicate complexity rules and limits in the notes.

12-7 Can the **device** be configured so that account passwords expire periodically?

GUIDANCE: If yes, provide in the notes the expiration frequency or administration controls available.

13 PHYSICAL LOCKS (PLOK): Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.

13-1 Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e. cannot remove without tools)?

GUIDANCE: This question refers to the typical installation and configuration of the manufacturer's **device**.
Consider internal data storage drives and any other storage media that maintain **private data**. Answer "Yes," if any such media can be physically accessed and removed without tools. In this context, a physical key required for access is considered a tool.

14 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP): Manufacturer's plans for security support of third-party components within the **device**'s life cycle.

14-1 In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).

14-2 Is a list of other third party applications provided by the manufacturer available?

GUIDANCE: In the notes section, list the other third-party applications used by the **device** and provided by the manufacturer. If components are proprietary, please specify whether this information is available upon request prior to sale.

15 SYSTEM AND APPLICATION HARDENING (SAHD): The **device**'s inherent resistance to cyber-attacks and **malware**.

15-1 Does the **device** employ any hardening measures?

15-2 Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?

GUIDANCE: Optionally describe in the notes section the mechanism(s) used to protect changes to the application programs, system configuration and/or **device** data.

15-3 Does the **device** have external communication capability? (network, modem, etc.)

GUIDANCE: If yes, indicate in the notes if the **device** must initiate the external connection or accepts incoming connections.

15-4 Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?

GUIDANCE: Provide a summary in the notes section of the file-level access controls (e.g., **user** access versus administrator access, remote versus local access, etc.)

15-5 Are all accounts which are not required for the intended use of the **device** disabled or deleted, for both **users** and applications?

GUIDANCE: Indicate in the notes if any accounts are closed/disabled by the manufacturer (at or prior to the installation of the **device**) or are expected to be disabled by the end **user**.

15-6 Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?

GUIDANCE: Indicate in the notes if any shared resources are closed/disabled by the manufacturer (at or prior to the installation of the **device**) or are expected to be disabled by the end **user**.

15-7 Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?

GUIDANCE: Indicate in the notes if the ports are closed/disabled by the manufacturer (at or prior to the installation of the **device**) or are expected to be disabled by the end **user**.

15-8 Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?

GUIDANCE: Indicate in the notes if the unneeded services are deleted/disabled by the manufacturer (at or prior to the installation of the **device**) or are expected to be disabled by the end **user**.

15-9 Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?

GUIDANCE: Indicate in the notes if the unneeded applications are deleted/disabled by the manufacturer (at or prior to the installation of the **device**) or are expected to be disabled by the end **user**.

15-10 Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?

GUIDANCE: Describe in the notes what external media is accepted by the **device**.

15-11 Can software or hardware not authorized by the **device** manufacturer be installed on the **device** without the use of tools?

GUIDANCE: Answer "Yes" if the **device user**/owner has the 'technical' ability to install hardware or software. However, If the manufacturer does not authorize **users** to install hardware or software, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note.

16 SECURITY GUIDES (SGUD): Availability of security guidance for **operator** and administrator of the **device** and manufacturer sales and service.

16-1 Are security-related features documented for the **device user**?

GUIDANCE: Answer "Yes" if the manufacturer provides a dedicated security document or security documentation within the **user** manual, service manual, or other documentation available to **users**.

16-2 Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data.)?

GUIDANCE: Answer "Yes" if the manufacturer provides such instructions within any documentation available to **users**.

17 HEALTH DATA STORAGE CONFIDENTIALITY (STCF): The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.

17-1 Can the **device** encrypt data at rest?

GUIDANCE: See also section 18 for specific questions regarding encryption of data prior to network transmission or media export.

18 TRANSMISSION CONFIDENTIALITY (TXCF): The ability of the **device** to ensure the confidentiality of transmitted **private data**.

18-1 Can **private data** be transmitted only via a point-to-point dedicated cable?

GUIDANCE: Clarification: a point-to-point dedicated cable is a cabling system that is not accessible to the general public (e.g., it is in physically controlled space such as examining rooms or communication closets or building plenum).

18-2 Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes section to which standard the encryption mechanism adheres.)

18-3 Is **private data** transmission restricted to a fixed list of network destinations?

GUIDANCE: Clarification: a fixed list is an explicit mechanism that limits the connections and nature of connections on a per-**device** basis.

19 TRANSMISSION INTEGRITY (TXIG): The ability of the **device** to ensure the integrity of transmitted **user**.

19-1 Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)

20 OTHER SECURITY CONSIDERATIONS (OTHR): Additional security considerations/notes regarding **medical device** security.

20-1 Can the **device** be serviced remotely?

GUIDANCE: **Remote service** refers to **device** maintenance activities performed by a service person via network or other remote connection. Describe in the notes any manufacturer restrictions on **remote service**.

20-2 Can the **device** restrict remote access to/from specified **devices** or **users** or network locations (e.g., specific IP addresses)?

20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access?

Section 3
MDS^2 FORM

To access and download the current HN 1 MDS^2 *Worksheet*, type the following into your web browser:
http://www.nema.org/Standards/ComplimentaryDocuments/MDS2-Worksheet.xls
or double click on the icon below.


MDS2-Worksheet.xls

< This page is intentionally left blank >

Manufacturer Disclosure Statement for Medical Device Security – MDS[2]

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

Manufacturer or Representative Contact Information	Company Name	Manufacturer Contact Information
	Representative Name/Position	

Intended use of device in network-connected environment:

MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [**ePHI**])?	_____	__
B	Types of **private data** elements that can be maintained by the **device**:		
	B.1 Demographic (e.g., name, address, location, unique identification number)?	_____	__
	B.2 Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	_____	__
	B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	_____	__
	B.4 Open, unstructured text entered by **device user/operator**?	_____	__
	B.5 **Biometric data**?	_____	__
	B.6 Personal financial information?	_____	__
C	Maintaining **private data** - Can the **device**:		
	C.1 Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	_____	__
	C.2 Store **private data** persistently on local media?	_____	__
	C.3 Import/export **private data** with other systems?	_____	__
	C.4 Maintain **private data** during power service interruptions?	_____	__
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1 Display **private data** (e.g., video display, etc.)?	_____	__
	D.2 Generate hardcopy reports or images containing private data?	_____	__
	D.3 Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	_____	__
	D.4 Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	_____	__
	D.5 Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	_____	__
	D.6 Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	_____	__
	D.7 Import **private data** via scanning?	_____	__
	D.8 Other?	_____	__

Management of **private data** notes:

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

SECURITY CAPABILITIES

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

1 AUTOMATIC LOGOFF (ALOF)
The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.

1-1 Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? ..... _____ __

1-1.1 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.) ..... _____ __

1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**? ..... _____ __

ALOF notes:

2 AUDIT CONTROLS (AUDT)
The ability to reliably audit activity on the **device**.

2-1 Can the **medical device** create an **audit trail**? ..... _____ __

2-2 Indicate which of the following events are recorded in the audit log:

2-2.1 Login/logout ..... _____ __

2-2.2 Display/presentation of data ..... _____ __

2-2.3 Creation/modification/deletion of data ..... _____ __

2-2.4 Import/export of data from **removable media** ..... _____ __

2-2.5 Receipt/transmission of data from/to external (e.g., network) connection ..... _____ __

2-2.5.1 **Remote service** activity ..... _____ __

2-2.6 Other events? (describe in the notes section) ..... _____ __

2-3 Indicate what information is used to identify individual events recorded in the audit log:

2-3.1 **User** ID ..... _____ __

2-3.2 Date/time ..... _____ __

AUDT notes:

3 AUTHORIZATION (AUTH)
The ability of the **device** to determine the authorization of **users**.

3-1 Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism? _____ __

3-2 Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)? ..... _____ __

3-3 Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)? ..... _____ __

AUTH notes:

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

4 CONFIGURATION OF SECURITY FEATURES (CNFS)
The ability to configure/re-configure **device security capabilities** to meet **users'** needs.

4-1 Can the **device** owner/**operator** reconfigure product **security capabilities**? ..... _____ __

CNFS notes:

5 CYBER SECURITY PRODUCT UPGRADES (CSUP)
The ability of on-site service staff, **remote service** staff, or authorized customer staff to install/upgrade **device**'s security patches.

5-1 Can relevant OS and **device** security patches be applied to the **device** as they become available? ..... _____ __

5-1.1 Can security patches or other software be installed remotely? ..... _____ __

CSUP notes:

6 HEALTH DATA DE-IDENTIFICATION (DIDT)
The ability of the **device** to directly remove information that allows identification of a person.

6-1 Does the **device** provide an integral capability to de-identify **private data**? ..... _____ __

DIDT notes:

7 DATA BACKUP AND DISASTER RECOVERY (DTBK)
The ability to recover after damage or destruction of **device** data, hardware, or software.

7-1 Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)? ..... _____ __

DTBK notes:

8 EMERGENCY ACCESS (EMRG)
The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.

8-1 Does the **device** incorporate an **emergency access** ("break-glass") feature? ..... _____ __

EMRG notes:

9 HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)
How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.

9-1 Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology? ..... _____ __

IGAU notes:

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

10 MALWARE DETECTION/PROTECTION (MLDP)
The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).

10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	_____	__
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	_____	__
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	_____	__
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	_____	__
10-2	Can the **device** owner install or update **anti-virus software**?	_____	__
10-3	Can the **device** owner/**operator** (technically/physically) update **virus** definitions on manufacturer-installed **anti-virus software**?	_____	__

MLDP notes:

11 NODE AUTHENTICATION (NAUT)
The ability of the **device** to authenticate communication partners/nodes.

11-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	_____	__

NAUT notes:

12 PERSON AUTHENTICATION (PAUT)
Ability of the **device** to authenticate **users**

12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	_____	__
12-1.1	Does the **device** support unique **user/operator**-specific IDs and passwords for multiple **users**?	_____	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	_____	__
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	_____	__
12-4	Can default passwords be changed at/prior to installation?	_____	__
12-5	Are any shared **user** IDs used in this system?	_____	__
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	_____	__
12-7	Can the **device** be configured so that account passwords expire periodically?	_____	__

PAUT notes:

13 PHYSICAL LOCKS (PLOK)
Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.

13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	_____	__

PLOK notes:

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

14 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)
Manufacturer's plans for security support of 3rd party components within **device** life cycle.

14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	_____	__
14-2	Is a list of other third party applications provided by the manufacturer available?	_____	__

RDMP notes:

15 SYSTEM AND APPLICATION HARDENING (SAHD)
The **device**'s resistance to cyber attacks and **malware**.

15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	_____	__
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	_____	__
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	_____	__
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	_____	__
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both users and applications?	_____	__
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	_____	__
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	_____	__
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	_____	__
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	_____	__
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	_____	__
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	_____	__

SAHD notes:

16 SECURITY GUIDANCE (SGUD)
The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.

16-1	Are security-related features documented for the **device user**?	_____	__
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	_____	__

SGUD notes:

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

17 HEALTH DATA STORAGE CONFIDENTIALITY (STCF)
The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.

17-1 Can the **device** encrypt data at rest? ..... _____ __

STCF notes:

18 TRANSMISSION CONFIDENTIALITY (TXCF)
The ability of the **device** to ensure the confidentiality of transmitted **private data**.

18-1 Can **private data** be transmitted only via a point-to-point dedicated cable? ..... _____ __

18-2 Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.) ..... _____ __

18-3 Is **private data** transmission restricted to a fixed list of network destinations? ..... _____ __

TXCF notes:

19 TRANSMISSION INTEGRITY (TXIG)
The ability of the **device** to ensure the integrity of transmitted **private data**.

19-1 Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.) ..... _____ __

TXIG notes:

20 OTHER SECURITY CONSIDERATIONS (OTHR)
Additional security considerations/notes regarding **medical device** security.

20-1 Can the **device** be serviced remotely? ..... _____ __

20-2 Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)? ..... _____ __

20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access? ..... _____ __

OTHR notes:

Annex
COMPARISON OF PREVIOUS (2008) AND CURRENT (2013) MDS^2 (Informative)

Table A-1
MDS^2 question number changes cross-reference: HN 1-2008 vs. HN 1-2013

2013		2008
A	Can this **device** display, transmit or maintain **private data** (including **electronic Protected Health Information** (**ePHI**))?	1
B	Types of **private data** elements that can be maintained by the **device**:	2
B.1	Demographic (e.g., name, address, location, unique identification number)?	2a
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	2b
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	2c
B.4	Open, unstructured text entered by **device user/operator**?	2d
B.5	**Biometric data**?	…
B.6	Personal financial information?	…
C	Maintaining **private data** - Can the **device**:	3
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	3a
C.2	Store **private data** persistently on local media?	3b
C.3	Import/export **private data** with other systems?	3c
C.4	Maintain **private data** during power service interruptions?	17
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:	4
D.1	Display **private data** (e.g., video display, etc.)?	4a
D.2	Generate hardcopy reports or images containing **private data**?	4b
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	4c
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	4d
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	4e
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	4f
D.7	Import **private data** via scanning?	…
D.8	Other?	4g
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	14
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	…
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	…
2-1	Can the **medical device** create an **audit trail**?	15
2-2	Indicate which of the following events are recorded in the audit log:	
2-2.1	Login/logout	15a

Table continues on next page

Table A-1 Continued

2013		2008
2-2.2	Display/presentation of data	15b
2-2.3	Creation/modification/deletion of data	15c
2-2.4	Import/export of data from **removable media**	15d
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	
2-2.5.1	**Remote service** activity	11b
2-2.6	Other events? (describe in the notes section)	…
2-3	Indicate what information is used to identify individual events recorded in the audit log:	…
2-3.1	**User** ID	…
2-3.2	Date/time	…
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	…
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	…
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	12d
4-1	Can the **device** owner/**operator** reconfigure product **security capabilities**?	…
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	12a
5-1.1	Can security patches or other software be installed remotely?	11c
6-1	Does the **device** provide an integral capability to de-identify **private data**?	…
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** like tape, disk)?	8
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	16
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	19
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	…
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	…
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	…
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	…
10-2	Can the **device** owner install or update **anti-virus software**?	12b
10-3	Can the **device** owner/**operator** (technically/physically) update **virus** definitions on manufacturer-installed **anti-virus software**?	12c
11-1	Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	11a
12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	13
12-1.1	Does the **device** support unique **user/operator** -specific IDs and passwords for multiple users?	…
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	…
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	…
12-4	Can default passwords be changed at/prior to installation?	…

Table continues on next page

Table A-1 Continued

2013		2008
12-5	Are any shared **user** IDs used in this system?	…
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	…
12-7	Can the **device** be configured so that account passwords expire periodically?	…
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	7
14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	6
14-2	Is a list of other third party applications provided by the manufacturer available?	…
15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	…
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	…
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	…
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	…
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	…
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	…
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	…
15-8	Are all services (e.g., Telnet, File Transfer Protocol [FTP], Internet Information Server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	…
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	…
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	9
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the **device** without the use of tools?	10
16-1	Are security-related features documented for the **device user**?	5
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	…
17-1	Can the **device** encrypt data at rest?	…
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	18a
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	18b
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	18c
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	…
20-1	Can the **device** be serviced remotely?	11
20-2	Can the **device** restrict remote access to/from specified **device**s or **users** or network locations (e.g., specific IP addresses)?	11a
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	…

§