HIMSS/NEMA Standard HN 1-2008

Manufacturer Disclosure Statement for Medical Device Security

Published by

National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
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 HEALTHCARE INFORMATION 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 ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) transmitted or maintained by medical devices. 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 and systems that maintain or transmit ePHI. 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 form should:

(1) Be useful to healthcare provider organizations worldwide. While the form does supply information important to providers who must comply with HIPAA privacy and security rules, the information presented may be useful for any healthcare provider who aspires to have an effective information security RISK MANAGEMENT program. Outside the US, providers would therefore find the MDS^2 form an effective tool to address regional regulations such as EU 95/46 (Europe), Act on the Protection of Personal Information (Act No. 57 of 2003, Japan), and PIPEDA (Canada).

(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.

(4) HIMSS and NEMA grant permission to make copies and use this form.

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 like ACCE / 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). The initial form was published in 2004, "MDS^2 v. 1.0 (2004-11-01)" and is now published for the first time as a joint HIMSS/NEMA standard. HIMSS and NEMA recommend that the information in the MDS^2 form be used to help complete the ACCE / ECRI form and associated processes as part of each organization's HIPAA security compliance 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 sub-division by contacting the:

Vice President, Engineering
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209

<This page is intentionally left blank.>

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

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 and systems. Manufacturers are generally including such security-related requirements in the production of new devices and systems 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.

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

Health Insurance Reform: Security Standards; Final Rule, 45 CFR pts.160, 162, 164 (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 ELECTRONIC PROTECTED HEALTH INFORMATION and to manage the conduct of the covered entity's workforce in relation to the protection of that information. [45 CFR Part 164]

anti-virus software: See VIRUS SCANNER

audit trail: Data collected and potentially used to facilitate a security audit [45 CFR Part 142]

biometric ID: A biometric identification system identifies a human from 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). [45 CFR Part 142]

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. [45 CFR Part 160.103]

electronic protected health information (ePHI): INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI) that is (1) transmitted by or (2) maintained in ELECTRONIC MEDIA. [45 CFR Part 160.103]

individually identifiable health information (IIHI): INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION is 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. [45 CFR Part 160.103].

personal identification number (PIN): A number or code assigned to an individual and used to provide verification of identity. [45 CFR Part 142]

physical safeguards: The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. [45 CFR Part 164]

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: See ELECTRONIC MEDIA

risk analysis: Conducting an accurate and thorough assessment of the potential risks and VULNERABILITIES to the integrity, availability, and confidentiality of ELECTRONIC PROTECTED HEALTH INFORMATION. [45 CFR Part 164]

risk management: (1) The ongoing process of assessing risk, taking steps to reduce risk to an

acceptable level, and maintaining that level of risk. [NIST SP 800-26] (2) Security measures sufficient to reduce risks and VULNERABILITIES to a reasonable and appropriate level. [45 CFR Part 164]

technical safeguards: The technology, policies, and procedures to protect ELECTRONIC PROTECTED HEALTH INFORMATION and control access to it. [45 CFR Part 164]

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.

virus: In general, computer code that is either:

(1) A type of programmed threat—a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

(2) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs; in addition to propagation, the VIRUS usually performs some unwanted function. [45 CFR Part 164]

virus scanner: A computer program ("ANTI-VIRUS SOFTWARE") that detects a VIRUS computer program, or other kind of malware (e.g., worms and Trojans), 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 system 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 system's security policy. [NIST SP 800-30]

1.4 ACRONYMS

CD: Compact Disk

CF: Compact Flash

DVD: Digital Versatile Disk

IP: Internet Protocol

LAN: Local Area Network

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 and systems 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)/system(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 Section 1 – Questions 1-19

Section 1 of the MDS^2 form contains 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. The field "Other Security Considerations" allows the manufacturer to add some general security considerations.

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. The questions contained on the MDS^2 form refer to device capability. Permission is a contractual matter separate from the MDS^2 form and is not covered by the MDS^2 form. Making changes to a device without explicit manufacturer authorization may have significant contractual and liability issues.

2.2.2 Section 2 – Explanatory notes

The optional section 2 of the MDS^2 form contains space for explanatory notes if the manufacturer needs more space to explain specific details to the answers on questions 1-19. .

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

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

Header Information:

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

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

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

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

Questions 1-19:

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

If additional information is needed for proper interpretation of these answers, it shall be provided in Section 2, Explanatory Notes.

The manufacturer shall answer questions 1-19 in accordance with the following guidance:

NOTE—the numbers in this subsection, below, correlate to the question numbers in Section 1 of the MDS[2] form.

1. Maintaining ePHI includes storage on an internal disk, REMOVABLE MEDIA, short-term computer memory, etc. Transmitting ePHI includes receiving / sending external to the device via network, telephone, direct connect cable, REMOVABLE MEDIA, etc.

2. The definition of ePHI varies based on national regulations and local experience. In general it includes any form of protected health information that can be identified as being associated with a particular patient. As an example, in the US, the HIPAA regulation lists the following 18 elements as nominal identifiers of ePHI in the absence of better local experience:

- *Name*
- *Geographic data (e.g., address)*
- *Dates (e.g., date of birth, admission, discharge, death, treatment)*
- *Telephone No.*
- *Fax No.*
- *E-mail address*
- *Social Security No.*
- *Medical record No.*
- *Health plan beneficiary No.*
- *Account No.*
- *Certificate/license numbers*
- *Vehicle identifiers*
- *Device identifiers*
- *Universal Resource Locators (URLs)*
- *IP address numbers*
- *Biometric identifiers*
- *Full face (or comparable) photographic images*
- *Any unique identifying number, characteristic or code*

Question 2d regarding unstructured text is intended to cover any additional (possibly ePHI) data maintained by the device that a provider could enter via open, unstructured text capability.

3. The manufacturer provides detail on how ePHI is maintained.

4. Import and export refer to movement of information via published open protocols to devices outside of the medical device under consideration (e.g., medical information bus (IEEE 1073), serial port and published protocol that allows general access to ePHI).

Dedicated cable here refers to communication via a point-to-point cable to a device or system outside of the device under consideration. A device might use a dedicated cable internally within its structure, but that need not be mentioned unless it is also accessible externally.

5. Training and documentation include explicit sections of administrator or user manuals that detail the device security features and their use.

6. This question identifies the underlying 3rd party system software platform (operating system) name or indicates that there is no 3rd party platform (i.e., proprietary system created for this manufacturer alone).

7. Refers to the typical installation configuration of the manufacturer's device.

8. Refers to an integrated feature or option that supports information backup onto REMOVABLE MEDIA (e.g., optical disk, magnetic disk, tape, etc.).

9. Identifies whether it is possible to start the device with software from any source other than the manufacturer's normal startup device (e.g., an integral hard disk or ROM) without the use of tools.

10. Does the device allow, through root access, administrative privilege, or other non-intrusive method, a local user and/or IT staff to install software not provided and not explicitly authorized by the manufacturer (e.g., email client, office applications, VIRUS SCANNER, browsers, games, etc.)? If the normal device configuration permits this, but it is not permitted by contract or service policy, answer this question yes and clarify the policy in the associated Section 2 notes.

11. REMOTE SERVICE refers to device maintenance activities performed by a service person via network or other remote connection.

12. Level of owner/operator access to device operating system. Here the manufacturer details what is technically possible if the device owner (generally the healthcare provider) has the technical ability to install security controls on the medical device under consideration. If the owner is able to do any of these steps, the answer is yes. This does not mean that contracts or service policies permit this. It is important to distinguish between capability and permission. This question is about capability. Permission is a contractual matter separate from the MDS^2 form and is not covered by the MDS^2 form.

13. If the device supports identification beyond username and password, describe it briefly in the associated notes (e.g., “uses XYZ secure TOKEN mechanism”).

14. If the answer is yes, summarize briefly in the associated notes.

15. Clarifications: viewing refers to operations that have to do with the display, printing, or other use of ePHI (e.g., image display, record print-out, etc.); creation, modification, or deletion would mean that all these events are tracked in the log file; export or transmittal refers to the movement of ePHI outside of the device under consideration.

16. Emergency access features allow operators emergency access to the device in cases where the normal authentication cannot be successfully completed or is not working properly.

17. If the device has non-volatile storage, such as a disk drive, this also should be answered yes. If a power loss results in partial loss of ePHI, briefly summarize the characteristics of this behavior in the notes.

18. Clarifications: via a point-to-point dedicated cable is a cabling system that is not accessible to the general public (i.e., it is in physically controlled space such as examining rooms or communication closets or building plenum); fixed list is an explicit mechanism that limits the connections and nature of connections on a per-device basis.

19. Ensure integrity refers to methods that can detect and/or correct differences between the source makeup of an ePHI message and the ePHI message received by an external device.

Section 3
MDS^2 FORM

To access and download the HN 1 MDS^2 *Worksheet*, type the following into your web browser:
http://www.nema.org/stds/complimentary-docs/upload/MDS2%20Worksheet.xls
or double click on the icon below.

MDS^2 Worksheet

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

SECTION 1

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	

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	Yes	No	N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?				
2. Types of ePHI data elements that can be maintained by the device:				
a. Demographic (e.g., name, address, location, unique identification number)?				
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?				
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?				
d. Open, unstructured text entered by device user/operator?				
3. Maintaining ePHI - Can the device				
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?				
b. Store ePHI persistently on local media?				
c. Import/export ePHI with other systems?				
4. Mechanisms used for the transmitting, importing/exporting of ePHI – Can the device				
a. Display ePHI (e.g., video display)?				
b. Generate hardcopy reports or images containing ePHI?				
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?				
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?				
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?				
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?				
g. Other?_____				

ADMINISTRATIVE SAFEGUARDS	Yes	No	N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?				
6. What underlying operating system(s) (including version number) are used by the device? _____				

PHYSICAL SAFEGUARDS	Yes	No	N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e. cannot remove without tools)?				
8. Does the device have an integral data backup capability (i.e., backup onto removable media like tape, disk)?				
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?				

TECHNICAL SAFEGUARDS	Yes	No	N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?				
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?				
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?				
b. Can the device provide an audit trail of remote-service activity?				
c. Can security patches or other software be installed remotely?				
12. Level of owner/operator service access to device operating system: Can the device owner/operator				
a. Apply device manufacturer-validated security patches?				
b. Install or update antivirus software?				
c. Update virus definitions on manufacturer-installed antivirus software?				
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?				
13. Does the device support user/operator specific username *and* password?				
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?				

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

SECTION 1

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	

15. Events recorded in device audit trail (e.g., user, date/time, action taken): Can the audit trail record
    a. Login and logout by users/operators? ..... _____ _____
    b. Viewing of ePHI? ..... _____
    c. Creation, modification or deletion of ePHI? ..... _____ _____
    d. Import/export or transmittal/receipt of ePHI? ..... _____ _____
16. Does the device incorporate an emergency access ("break-glass") feature that is logged? ..... _____ _____
17. Can the device maintain ePHI during power service interruptions? ..... _____ _____
18. Controls when exchanging ePHI with other devices:
    a. Transmitted only via a point-to-point dedicated cable? ..... _____ _____
    b. Encrypted prior to transmission via a network or removable media? ..... _____ _____
    c. Restricted to a fixed list of network destinations ..... _____ _____
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?..... _____ _____

Other Security Considerations

Manufacturer Disclosure Statement for Medical Device Security – MDS[2]			
SECTION 1			
Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	
Manufacturer or Representative Contact Information:	Company Name Representative Name/ Position	Manufacturer Contact Information	
SECTION 2			
EXPLANATORY NOTES (from questions 1 – 19) **IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form).**			

§