Manufacturer Disclosure Statement for Medical Device Security – MDS^2

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

Manufacturer or Representative Contact Information:	Name	Title	Department
	Company Name	Telephone #	e-mail

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) *As defined by HIPAA Security Rule, 45 CFR Part 164)*	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 such as 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?				
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 log 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 ID *and* password?				
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?				
15. Events recorded in device audit log (e.g., user, date/time, action taken): *Can the audit log 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 logs each instance of use?				
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?				
18. Controls when exchanging ePHI with other devices:				
a. Transmitted only via a physically secure connection (e.g., dedicated cable)?				
b. Encrypted prior to transmission via a network or removable media?				
c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?				
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?				

†Recommend use of ECRI's Universal Medical Device Nomenclature System (UMDNS).

Adapted from *Information Security for Biomedical Technology: A HIPAA Compliance Guide*, ACCE/ECRI, 2004.
ACCE – the American College of Clinical Engineering; ECRI – formerly the Emergency Care Research Institute.

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

RECOMMENDED SECURITY PRACTICES

EXPLANATORY NOTES *(from questions 1 – 19):*
IMPORTANT: Refer to Instructions for the Manufacturers Disclosure Statement for Medical Device Security for the proper interpretation of information provided in this form.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.

Instructions for the Manufacturer Disclosure Statement for Medical Device Security – MDS^2 Version 1.0

Introduction

In light of increased focus on medical device security and the upcoming April 21, 2005 deadline for compliance with the HIPAA Security Rule, the HIMSS Medical Device Security Workgroup has created a standard Manufacturer Disclosure Statement for Medical Device Security (MDS^2). The intent of the MDS^2 is to supply healthcare providers with important information that can assist them in assessing the vulnerability and risks associated with electronic Protected Health Information (ePHI)[1] transmitted or maintained by medical devices. Because security risk assessment is a broad, organization-wide effort, this document focuses on only those elements of the risk assessment process associated with medical devices and systems that maintain or transmit ePHI. A standardized form allows manufacturers to quickly respond to a potentially large volume of requests from providers for information regarding the security-related features of the medical devices they manufacture. The standardized form also facilitates the providers' review of the large volume of security-related information supplied by the manufacturers. This form was 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). HIMSS recommends that the information in the MDS^2 be used to help complete the ACCE/ECRI form and associated processes as part of each organization's HIPAA Security compliance efforts.

The manufacturer-completed MDS^2 should:

(1) Be useful to healthcare provider organizations worldwide.
While the form does supply information important to providers who must comply with the HIPAA Security Rule, the information presented is intended to be useful for *any* healthcare provider who aspires to have an effective information security and risk management program. Outside the US, providers would therefore find the MDS^2 an effective tool in addressing such regional regulations as EC 95/46, HPB 517, and PIPEDA.[2]

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

This completed MDS^2 form provides a simple, flexible way of collecting the technical, device-specific elements of the total information needed by provider organizations (device users/operators) in preparing for their first round of medical device risk assessments. Providers around the world should find a completed MDS^2 form useful in controlling information security (i.e., confidentiality, integrity, and availability) risks. Note, however, that the MDS^2 is not intended and should not be used as a basis for medical device procurement. Writing procurement specifications requires a deeper and more extensive knowledge of security and the provider's mission.

Using the information provided by the manufacturer in the MDS^2 combined 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.

The Role of Healthcare Providers and Medical Device Manufacturers in the Security Management Process

Responsibility for effective security management must ultimately lie with the provider organization. Generally the device manufacturers can assist providers in their security management programs by offering information associated with

- 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

---

[1] As defined by HIPAA Security Rule, 45 CFR Part 164.

[2] EC 95/46 is the European Parliament and Council's Directive 95/46/EC on the *Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* ,
HPB 517 is the Japanese *Electronic Storage of Clinical Records* law ; and
PIPEDA is the Canadian *Personal Information Protection and Electronic Documents Act.*

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 (other than some technical safeguards) must be adopted and employed on-site extrinsic to the actual device. Other than some general recommendations with regard to medical devices:

- there are few ADMINISTRATIVE safeguards manufacturers can address beyond providing assistance in security training
- there are few PHYSICAL safeguards manufacturers can address beyond incorporating physical security features (e.g., component lock & key, theft/intrusion alarms) in their devices

The greatest impact manufacturers can have on medical device security is to incorporate TECHNICAL Safeguards (i.e., security features) in their devices to facilitate the providers efforts in maintaining an effective security program and meeting any relevant regulations. The medical device manufacturing industry is increasingly aware of the importance of having effective security features in their devices and systems. Manufacturers are generally including such features in the production of new devices and systems based provider needs and requirements.

Instructions for Obtaining and Using the MDS^2

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

Completed MDS^2 forms for many devices and systems may be available directly from the device manufacturer. Check the manufacturer's web site first for relevant forms and, when not available there, contact a manufacturer's representative to request a MDS^2 for the appropriate device(s)/system(s). If a manufacturer does not have a completed MDS^2 for the appropriate device(s)/system(s), enter the device category, manufacturer and model information in the appropriate boxes on the top of a blank form[3] and submit the form(s) and these instructions to the manufacturer's compliance office for their completion.

Note that HIMSS suggests that a standard naming convention be used for the device category terms and manufacturer names listed on the form. This assists providers in matching information from the form to their equipment inventories. ECRI's Universal Medical Device Nomenclature System (UMDNS) is the most widely used. Adopted by thousands of healthcare providers worldwide, UMDNS has been adopted by the National Library of Medicine into its Universal Medical Language System, and has been recommended by the Institute of Medicine for inclusion in the US Department of Health and Human Services (HHS) National Committee on Vital and Health Statistics (NCVHS) core terminology group. For more information about UMDNS contact ECRI at www.ecri.org.

Side 1 of the MDS^2 contains descriptive information on the *type* of data maintained/transmitted by device, *how* the data is maintained/transmitted, and any *security–related features* incorporated in the device. Side 2 contains manufacturer-optional recommended security practices and space for numbered explanatory notes that may expand on answers to questions 1 through 19. Manufacturers may elect to attach supplementary material if additional space for recommended practices or explanatory notes is necessary.

Question-specific notes.

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.

[3] Additional form copies and instructions may be downloaded from http://www.himss.org/asp/medicalDeviceSecurity.asp

2. The four sections of this question relate directly to the 18 data elements referred to in HIPAA, any of which, if present, render the entire electronically transmitted/maintained data set as ePHI. The 18 data elements included in the Rule are:

   - *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*

   The *open, unstructured text* question (2d) is intended to indicate an additional element where a provider might put further identifying information.

3. Here the manufacturer provides more detail on how ePHI is maintained. Note that a fully networked device is likely to have all three items with a 'Yes' response.
   - Persistently on local media refers to media created or directly attached to the device under consideration (e.g., MR Scanner, 3-D workstation), not a remote archive.
   - Import/export ePHI refers to data that is sourced or destined to remote storage devices (e.g., an MR scanner that relies on an image server in a PACS system).

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.

5. This question includes either explicit security training or 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 if there is no 3rd party platform (i.e., proprietary system created for this manufacturer alone).

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

8. Refers to an integrated feature that supports information backup onto removable media (e.g., optical disk, magnetic disk, tape).

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).

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)?

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. A MANUFACTURER ANSWERING 'YES' TO ANY OF THESE QUESTIONS DOES NOT MEAN THAT THE MANUFACTURER AUTHORIZES THE OWNER TO PERFORM THESE FUNCTIONS. THE OWNER ASSUMES ALL RESPONSIBILITY FOR UNAUTHORIZED INSTALLATION or REPAIRS. UNAUTHORIZED INSTALLATION or REPAIRS MAY VOID APPLICABLE WARRANTIES AND SERVICE AGREEMENTS. Authorization to perform these security-related services or changes to a medical device should be obtained in writing from the device manufacturer. Unauthorized changes to a medical device may remove it from government regulatory controls (e.g., FDA) and render the device an experimental medical device.

13. Self-explanatory.

14. Self-explanatory.

15. Clarifications:
    - Controlled viewing refers to operations that have to do with the display, printing, or other use of ePHI (e.g., image display, record print-out).
    - 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. Self-explanatory.
18. Clarifications:
    - *Physically secure connection* is a cabling system that is not accessible to the general public. (i.e., it is in a physically controlled space such as examining rooms, 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. Is such a method available for use as part of the device under consideration (either in transmission or receipt of ePHI)?

Disclaimer

This document is intended to assist healthcare providers in meeting their regulatory obligations regarding medical device security. It is the obligation of the users of this document (e.g., the healthcare provider) to employ all necessary and appropriate safeguards to meet their regulatory and organizational requirements. HIMSS does not assume any responsibility for the application or the content of this form.

Glossary

Term	Definition
Access	Read, write, modify, or transmit/receive data or otherwise make use of any system resource *[45 CFR Part 164]*
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 Checking*
Archive	Store (data) for extended period of time (e.g., years)
Audit Trail	Data collected and potentially used to facilitate a security audit *[45 CFR Part 142]*
Availability	The property that data or information is accessible and usable on demand by an authorized person *[45 CFR Part 164]*
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]*
Compact Disk (CD)	Optical storage media
Compact Flash (CF) Card™	Any of a family of solid-state memory cards
Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes *[45 CFR Part 164]*
Digital Versatile Disk (DVD)	Optical storage media
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]*
EPHI	*Individually Identifiable Health Information* that is (1) transmitted or (2) maintained by *electronic media* *[45 CFR Part 160]*

Term	Definition
Individually Identifiable Health Information (IIHI)	Any information, including demographic data collected from an *individual*, that (1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and a. identifies the individual, or b. with respect to which there is a reasonable basis to believe that the information can be used to identify the individual *[45 CFR Part 160]*
Integrity	The property that data or information has not been altered or destroyed in an unauthorized manner *[45 CFR Part 164]*
Local Area Network (LAN)	See *Networks*
Memory Stick™	One of a family of solid-state memory cards
Networks	A communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system; examples of networks include local area or wide area networks, including public networks such as the Internet *[NIST SP 800-26]*
Operating System	A collection of computer programs that manages the hardware for other computer applications; examples include Microsoft Windows, Novell Netware, Unix, Linux, Mac OS
Password	Confidential authentication information composed of a string of characters *[45 CFR Part 164]*
PC Card	A standard laptop personal computer device that plugs into a personal computer slot approximately the size of a credit card (formerly known as PCMCIA^{tm} card)
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	Provide 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	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]* Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level *[45 CFR Part 164]*
Secure Digital (SD) Card™	One of a family of solid-state memory cards

Term	Definition
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™, etc.). Often combined with a PIN to provide a two-factor authentication method that is generally thought of as superior to simple password authentication
Virtual Private Network (VPN)	See *Networks*
Virus	A computer program 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 142]*
Virus Checking	A computer program ("anti-virus software") that identifies and disables another "virus" computer program, typically hidden, that attempts to attach itself to other programs and has the ability to replicate (unchecked virus programs result in undesired side effects generally unanticipated by the user) *[45 CFR Part 142]*
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]*
Wide Area Network (WAN)	See *Networks*

