

# HIMSS

2005 Annual Conference and Exhibition  
Dallas, TX

*ROUNDTABLE*

*New Tools & Initiatives for Addressing Medical Device Security*

## ***HIMSS Manufacturers Disclosure Statement for Medical Device Security (MDS<sup>2</sup>)***

Thursday, February 17, 2005 @ 9:45am



Stephen L. Grimes, FACCE  
Chair, Medical Device Security Workgroup  
Healthcare Information and Management Systems Society (HIMSS)  
Principal Associate  
Strategic Health Care Technology Associates (SHCTA)

# HIMSS Manufacturer Disclosure Statement for Medical Device Security (MDS<sup>2</sup>)



**Manufacturer Disclosure Statement for Medical Device Security - MDS<sup>2</sup>**

RECOMMENDED SECURITY PRACTICES

Document ID: \_\_\_\_\_ Document Release Date: \_\_\_\_\_  
 Software Release Date: \_\_\_\_\_ Department: \_\_\_\_\_

Device Category: \_\_\_\_\_ Manufacturer: \_\_\_\_\_  
 Device Model: \_\_\_\_\_ Software Version: \_\_\_\_\_ Telephone #: \_\_\_\_\_ Email: \_\_\_\_\_

Manufacturer or Representative Contact Information: Name: \_\_\_\_\_ Company Name: \_\_\_\_\_

**MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)** As defined by HIPAA Security Rule, 45 CFR Part 164.0

1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?  
 a. Demographic (e.g., name, address, location, unique identification number)?  
 b. Medical record (e.g., photos/radiograph, test results, or physiologic data with identifying characteristics)?  
 c. Diagnostic/therapeutic (e.g., photos/radiograph, test results, or physiologic data with identifying characteristics)?  
 d. Other, unstructured text entered by device user/operator?

2. Can this device transmit or maintain electronic Protected Health Information (ePHI) information (ePHI)?  
 a. Can this device transmit or maintain electronic Protected Health Information (ePHI) information (ePHI)?  
 b. Can this device transmit or maintain electronic Protected Health Information (ePHI) information (ePHI)?  
 c. Can this device transmit or maintain electronic Protected Health Information (ePHI) information (ePHI)?  
 d. Can this device transmit or maintain electronic Protected Health Information (ePHI) information (ePHI)?

3. Maintaining ePHI: Can the device  
 a. Maintain ePHI temporarily on local media?  
 b. Import/export ePHI with other systems?  
 c. Display ePHI (e.g., video capture)?  
 d. Generate ePHI from or import/export ePHI via dedicated cable connection (e.g., IEEE 1394, serial port, USB, FireWire)?  
 e. Retrieve ePHI from or import/export ePHI via network connection (e.g., LAN, WAN, VPN, internet, Intranet)?  
 f. Transmit/receive ePHI via a network connection (e.g., Wi-Fi, Bluetooth, infrared)?  
 g. Transmit/receive ePHI via an integrated wireless connection (e.g., Wi-Fi, Bluetooth, infrared)?  
 h. Other \_\_\_\_\_

4. Mechanisms used for the transmitting, importing/exporting of ePHI: Can the device  
 a. Import/export ePHI with other systems? Yes No N/A Note: #  
 b. Display ePHI (e.g., video capture)? Yes No N/A Note: #  
 c. Generate ePHI from or import/export ePHI via dedicated cable connection (e.g., IEEE 1394, serial port, USB, FireWire)? Yes No N/A Note: #  
 d. Retrieve ePHI from or import/export ePHI via network connection (e.g., LAN, WAN, VPN, internet, Intranet)? Yes No N/A Note: #  
 e. Transmit/receive ePHI via a network connection (e.g., Wi-Fi, Bluetooth, infrared)? Yes No N/A Note: #  
 f. Transmit/receive ePHI via an integrated wireless connection (e.g., Wi-Fi, Bluetooth, infrared)? Yes No N/A Note: #  
 g. Other \_\_\_\_\_

**ADMINISTRATIVE SAFEGUARDS**

5. Does manufacturer offer operator(s) (including version number) are used by the device? Yes No N/A Note: #  
 6. What underlying operating system(s) (including version number) are used by the device? Yes No N/A Note: #

**PHYSICAL SAFEGUARDS**

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

**TECHNICAL SAFEGUARDS**

10. Can the device be serviced remotely (i.e., remote access performed by service person via network or remote connection)? Yes No N/A Note: #  
 a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)? Yes No N/A Note: #  
 b. Can the device log provide an audit trail of remote-service activity? Yes No N/A Note: #  
 c. Can security patches or other software to device operating system or application via local root or admin account? Yes No N/A Note: #  
 d. Can security patches or other software to device operating system or application via local root or admin account? Yes No N/A Note: #

11. Level of device manufacturer-installed antivirus software?  
 a. Apply or update definitions on manufacturer-specific ID and password?  
 b. Install or update definitions on manufacturer-specific ID and password?  
 c. Update administrative privileges (e.g., access operating system or application via local root or admin account)? Yes No N/A Note: #  
 d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? Yes No N/A Note: #

12. Does the device support user/operator specific ID and password?  
 a. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? Yes No N/A Note: #  
 b. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? Yes No N/A Note: #

13. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #  
 14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #

15. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #  
 16. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #

17. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #  
 18. Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logout)? Yes No N/A Note: #

19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?  
 a. Implicit or explicit error detection/correction technology? Yes No N/A Note: #  
 b. Implicit or explicit error detection/correction technology? Yes No N/A Note: #  
 c. Implicit or explicit error detection/correction technology? Yes No N/A Note: #

20. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?  
 a. Implicit or explicit error detection/correction technology? Yes No N/A Note: #  
 b. Implicit or explicit error detection/correction technology? Yes No N/A Note: #  
 c. Implicit or explicit error detection/correction technology? Yes No N/A Note: #

Adapted from Information Security for Biomedical Technology: A HIPAA Compliance Guide, ACCE/ECRI, 2004  
 MDS<sup>2</sup> v 1.0 (2004-11-01)

© 2004, HIMSS. All rights reserved.

**Instructions for the Manufacturer Disclosure Statement for Medical Device Security - MDS<sup>2</sup> 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<sup>2</sup>). The intent of the MDS<sup>2</sup> is to supply healthcare providers with important information (ePHI) 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<sup>2</sup> 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<sup>2</sup> 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<sup>2</sup> an effective tool in addressing such regional regulations as EC 95/46, HFB 017, and PIPEDA.<sup>2</sup>
- (2) Include device-specific information addressing the technical security-related attributes of the individual device model. This completed MDS<sup>2</sup> form provides a simple, flexible way of collecting the technical, device-specific elements of the risk assessments. Providers around the world should find a completed MDS<sup>2</sup> form useful in controlling information security (i.e., confidentiality, integrity, and availability) risks. Note, however, that the MDS<sup>2</sup> 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<sup>2</sup> combined with information collected about the care delivery environment (e.g., through tools like ACCE/ECRI's guide for Information Security for Biomedical Technology), 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

<sup>1</sup> As defined by HIPAA Security Rule, 45 CFR Part 164.  
<sup>2</sup> 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.  
 HFB 017 is the Japanese Electronic Storage of Clinical Records Law, and PIPEDA is the Canadian Personal Information Protection and Electronic Documents Act.

MDS<sup>2</sup> v 1.0 (2004-11-01) Page 1 of 7 © 2004, HIMSS. All rights reserved.

# The MDS<sup>2</sup> provides the Manufacturer's Model-specific Description of

- Device ability to maintain/transmit ePHI
  - ✓ Is the device capable of maintaining or transmitting ePHI?
  - ✓ For those devices capable of maintaining/transmitting ePHI, a description of
    - type of ePHI (e.g., demographic info, diagnostic/therapeutic info, etc.)
    - device mechanisms for maintaining ePHI
    - device mechanisms for transmitting ePHI
- Security features associated with the device
  - ✓ Safeguards provided with or incorporated in the device, including
    - Administrative
    - Physical
    - Technical
  - ✓ A list of any manufacturer-optional recommended safety practices

# Key Benefits of the MDS<sup>2</sup>

## ■ For Manufacturers

- ✓ Facilitates the manufacturers' common response to a potentially large volume of requests from providers for information regarding the ePHI capability and security-related features of the devices they manufacture

## ■ For Healthcare Providers

- ✓ Facilitates the providers' review & analysis of the large volume of security-related information supplied by manufacturers for devices on the providers' inventories

# Industry Endorsements for the MDS<sup>2</sup>

- HIMSS  
(Health Information and Management Systems Society)
- ACCE  
(American College of Clinical Engineering)
- ECRI
- NEMA  
(National Electrical Manufacturers Association)

# MDS<sup>2</sup> supplies key data to the ACCE / ECRI Biomedical Equipment Survey Form

**Manufacturer Disclosure Statement for Medical Device Security - MDS<sup>2</sup>**

**RECOMMENDED SECURITY INFORMATION**

**Manufacturer Disclosure Statement for Medical Device Security**

Device Category: \_\_\_\_\_ Manufacturer: \_\_\_\_\_ Document ID: \_\_\_\_\_ Document Release Date: \_\_\_\_\_  
 Software Version: \_\_\_\_\_ Software Release Date: \_\_\_\_\_ Department: \_\_\_\_\_  
 Name: \_\_\_\_\_ Title: \_\_\_\_\_ Email: \_\_\_\_\_  
 Telephone #: \_\_\_\_\_ Fax: \_\_\_\_\_

**MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)** As defined by HIPAA Security Rule, 45 CFR Part 164.2

1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?  
 a. Demographic (e.g., name, address, location, unique identification number)?  
 b. Medical record (e.g., photos/radiograph, test results, or physiologic data with identifying characteristics)?  
 c. Diagnostic/therapeutic (e.g., photos/radiograph, test results, or physiologic data with identifying characteristics)?  
 d. Open/structured text entered by device user/operator?

2. Can this device transmit or maintain electronic Protected Health Information (ePHI) on local media?  
 a. Can this device transmit or maintain electronic Protected Health Information (ePHI) on removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?  
 b. Can this device transmit or maintain electronic Protected Health Information (ePHI) on other systems?  
 c. Can this device transmit or maintain electronic Protected Health Information (ePHI) on other systems?  
 d. Can this device transmit or maintain electronic Protected Health Information (ePHI) on other systems?

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 permanently on local media?  
 c. Import/export ePHI to other systems?  
 d. Import/export ePHI to other systems?

4. Mechanisms used for the transmitting, importing/exporting of ePHI:  
 a. Display ePHI (e.g., video display)?  
 b. Generate ePHI from or record ePHI via dedicated cable connection (e.g., IEEE 1394, serial, USB, FireWire)?  
 c. Retrieve ePHI from or import/export ePHI via dedicated cable connection (e.g., LAN, WAN, VPN, Intranet, Internet)?  
 d. Transmit/receive ePHI via a network connection (e.g., WiFi, Bluetooth, infrared)?  
 e. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?  
 f. Other: \_\_\_\_\_

**ADMINISTRATIVE SAFEGUARDS**

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**

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 into 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**

10. Can the device be serviced remotely (i.e., remote activities performed by service person via network or remote connection)?  
 11. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?  
 12. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 13. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 14. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?

15. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 16. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 17. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 18. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?  
 19. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?

**Information Security for Biomedical Technology: A HIPAA Compliance Guide\***

**9.2.3 ACCE/ECRI Biomedical Equipment Survey Form**

Instructions:  
 • Question 1: Answers to questions 4, 5, and 6 will help determine whether question 1 should be answered 'Yes' or 'No'.  
 • Questions 9-12: Indicate whether a mitigating measure is present or not applicable (N/A). However, determination of applicability may require further investigation and review after setting priorities for developing mitigating strategies.

1. Is this device capable of maintaining or transmitting electronic Protected Health Information (ePHI)?  
 a. Name: \_\_\_\_\_ Title: \_\_\_\_\_ Manufacturer: \_\_\_\_\_  
 b. Treatment Date: \_\_\_\_\_ Location: \_\_\_\_\_  
 c. Med Record #: \_\_\_\_\_ Dept: \_\_\_\_\_  
 d. Account #: \_\_\_\_\_ Email: \_\_\_\_\_

2. Data element(s) that qualifies health information as ePHI (check all that apply):  
 a. Device ID # \_\_\_\_\_  
 b. Biometric ID \_\_\_\_\_  
 c. Location or Address \_\_\_\_\_  
 d. Image (e.g., photo, video, radiograph with identifying characteristics) \_\_\_\_\_  
 e. Identifying #, Characteristic, or Code \_\_\_\_\_

3. Input source of ePHI (check all that apply):  
 a. Keyboard, keypad \_\_\_\_\_  
 b. Scanning (bar code, magnetic, OCR) \_\_\_\_\_  
 c. Biometric (retina, finger/thumbprint) \_\_\_\_\_  
 d. Hard Disk \_\_\_\_\_  
 e. Memory \_\_\_\_\_

4. Is this device capable of:  
 a. Hard Disk \_\_\_\_\_  
 b. Memory \_\_\_\_\_  
 c. Other: \_\_\_\_\_

5. Is this device capable of:  
 a. Hard Disk \_\_\_\_\_  
 b. Memory \_\_\_\_\_  
 c. Other: \_\_\_\_\_

6. Other: \_\_\_\_\_

7. Who is authorized to access ePHI?  
 a. Medical Staff \_\_\_\_\_  
 b. Clinical Staff \_\_\_\_\_  
 c. Support Staff \_\_\_\_\_  
 d. Office Staff (i.e., IT, Risk Management) \_\_\_\_\_  
 e. Tech Staff (i.e., IT, Risk Management) \_\_\_\_\_  
 f. Outside Organization \_\_\_\_\_  
 g. Other: \_\_\_\_\_

8. Attach network diagrams showing Examples of Operations include:  
 a. Other: \_\_\_\_\_  
 b. Other: \_\_\_\_\_  
 c. Other: \_\_\_\_\_  
 d. Other: \_\_\_\_\_  
 e. Other: \_\_\_\_\_  
 f. Other: \_\_\_\_\_  
 g. Other: \_\_\_\_\_

ACCE  
 ECRI

© 2004, ACCE/ECRI All Rights Reserved

# MDS<sup>2</sup> Form

## Side 1

Standard Nomenclature (UMDNS)

### Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

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 <u>ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)</u> <small>As defined by HIPAA Security Rule, 45 CFR Part 164</small>	Yes	No	N/A	Note #
1. Can this device transmit or maintain <i>electronic Protected Health Information</i> (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: <i>Can the device</i>				
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: <i>Can the device</i>				
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.

# MDS<sup>2</sup> Form

## Side 2

### Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

#### 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.

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.

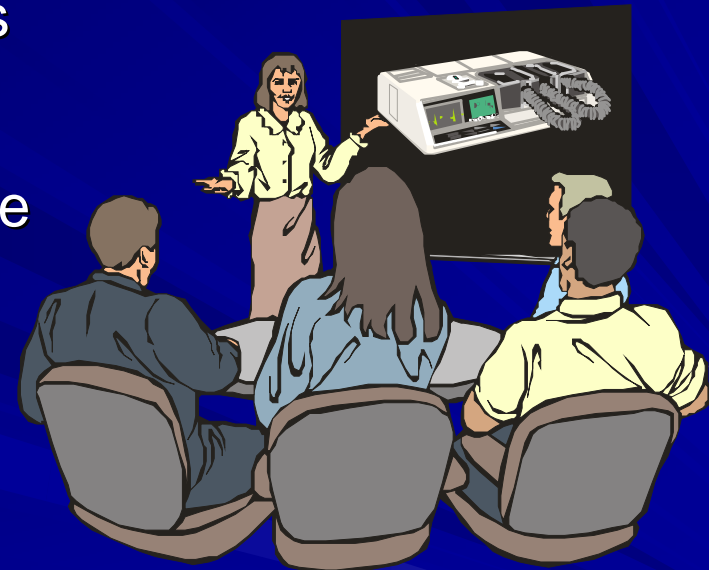
MDS<sup>2</sup> v 1.0 (2004-11-01)

Side 2

© 2004, HIMSS. All rights reserved.

# Healthcare Providers Use MDS<sup>2</sup>


- Information Security Committee
  - ✓ Reviews manufacturer-supplied MDS<sup>2</sup> forms along with the hospital's medical device inventory & *survey forms* to assess risks and determine what (if any) safeguards are available with the device
  - ✓ Uses MDS<sup>2</sup> to identify common classes of technology with common vulnerabilities
  - ✓ Uses MDS<sup>2</sup> to take common approaches to mitigating risks with those common classes where possible



# Future of MDS<sup>2</sup> - *Automation*

- The MDSW is developing and plans to publish an MDS<sup>2</sup> schema and reference toolkit with open source software. The schema and toolkit would
  - ✓ unambiguously define a structured representation of the MDS<sup>2</sup> data in XML
  - ✓ be made freely available (unlimited license to manufacturers/vendors & providers) with no implicit or explicit warranty
- The benefits of the toolkit are that it would facilitate
  - ✓ data entry & validation (of structure & content)
  - ✓ creation of templates for “common device categories”
  - ✓ populating data into subsequent versions of the MDS<sup>2</sup>
  - ✓ large-scale distribution of MDS<sup>2</sup> data by manufacturers to major healthcare providers
  - ✓ large-scale analysis of MDS<sup>2</sup> data by healthcare providers
  - ✓ establishing a central repository of MDS<sup>2</sup> data with an independent organization

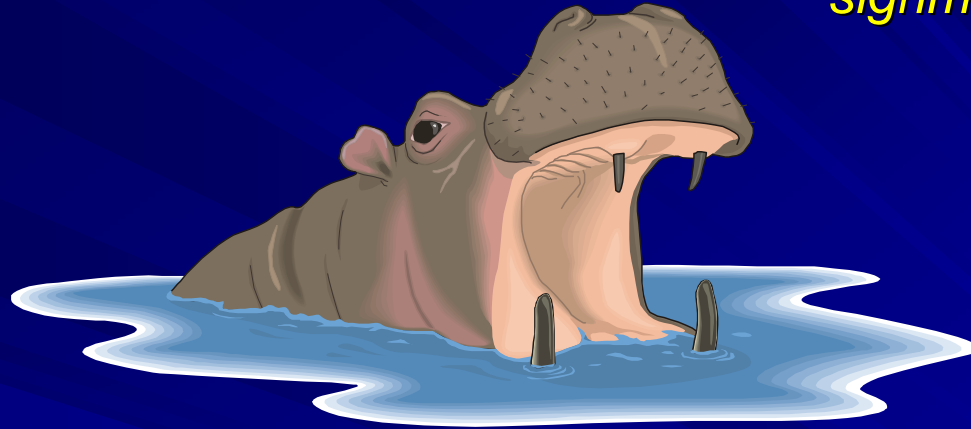
# HIMSS on Medical Device Security

- Web Site for HIMSS Medical Device Security Workgroup  
*with Bibliography of relevant source material*  
[http://www.himss.org/ASP/topics\\_medicalDevice.asp](http://www.himss.org/ASP/topics_medicalDevice.asp)
- HIMSS November 8, 2004 Press Release on MDS<sup>2</sup>  
<http://www.himss.org/pressroom/ASP/releaseDetail.asp?ContentID=59072>
- Manufacturer's Disclosure Statement for Medical Device Security (MDS2) Form & Instructions  
<http://www.himss.org/content/files/MDS2FormInstructions.pdf> 
- Manufacturers obtain *free* UMDNS (nomenclature) listing of their products by e-mailing ECRI at [himss-mds@ecri.org](mailto:himss-mds@ecri.org)

# Questions?



Stephen L. Grimes, FACCE  
*slgrimes@shcta.com*



Strategic Health Care Technology Associates  
[www.shcta.com](http://www.shcta.com)

Health Information and Management Systems Society  
[www.himms.org](http://www.himms.org)

American College of Clinical Engineering (ACCE)  
[www.accenet.org](http://www.accenet.org)



ECRI  
[www.ecri.org](http://www.ecri.org)



A NONPROFIT AGENCY