HIMSS

2005 Annual Conference and Exhibition
Dallas, TX

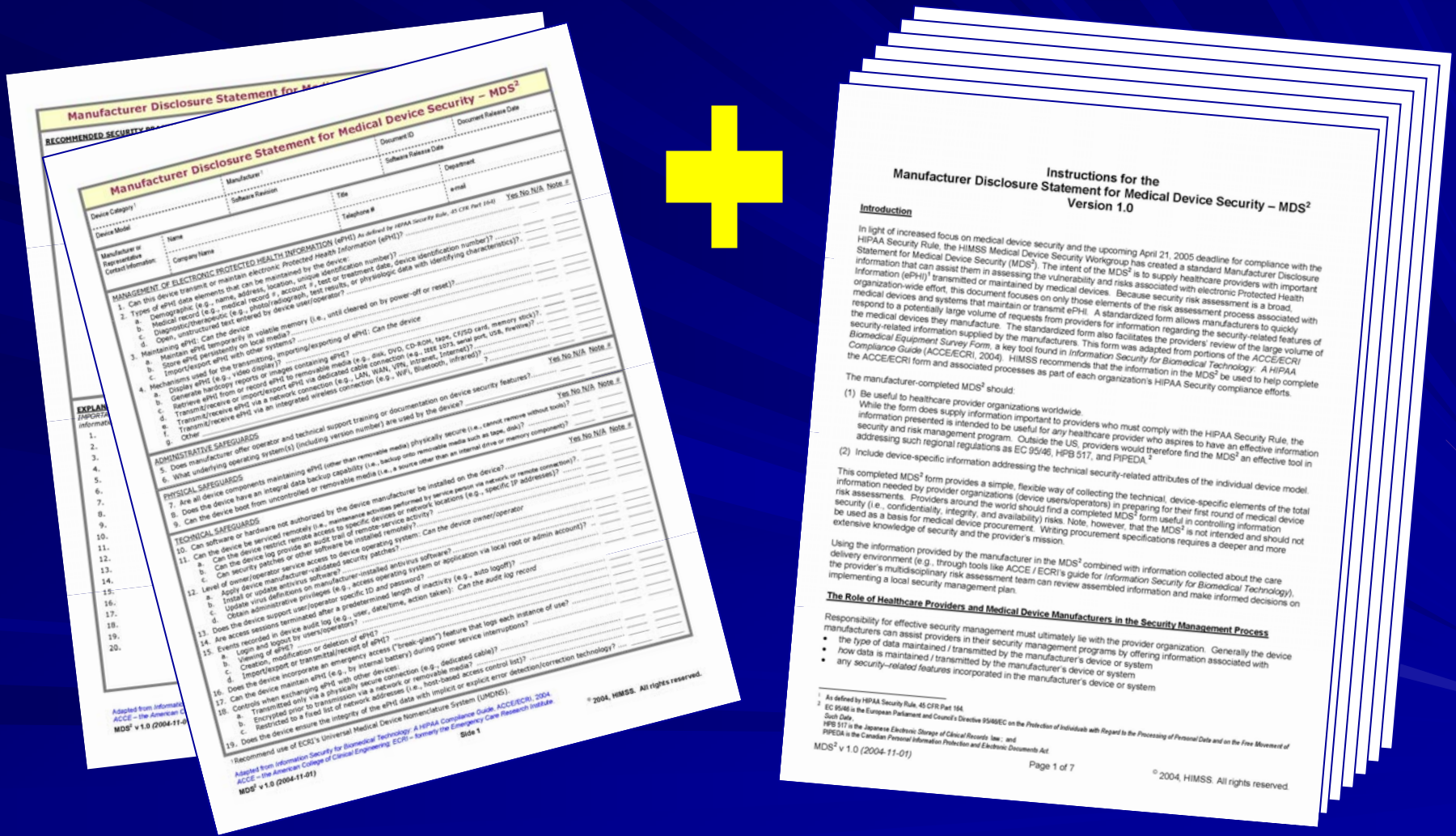
ROUNDTABLE
New Tools & Initiatives for Addressing Medical Device Security

HIMSS Manufacturers Disclosure Statement for Medical Device Security (MDS^2)

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 (MDS²)



The MDS^2 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

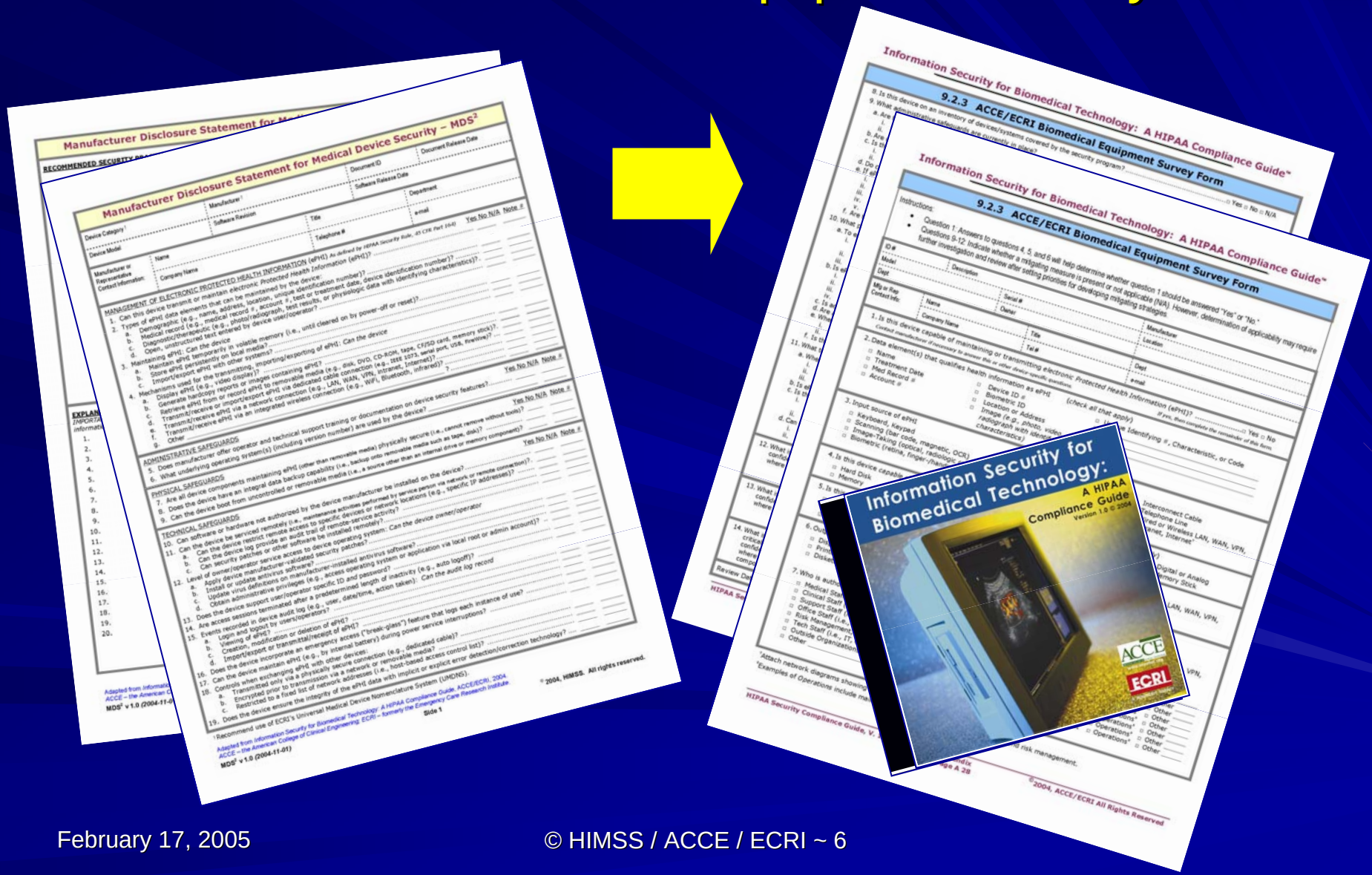
Key Benefits of the MDS^2

- 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^2

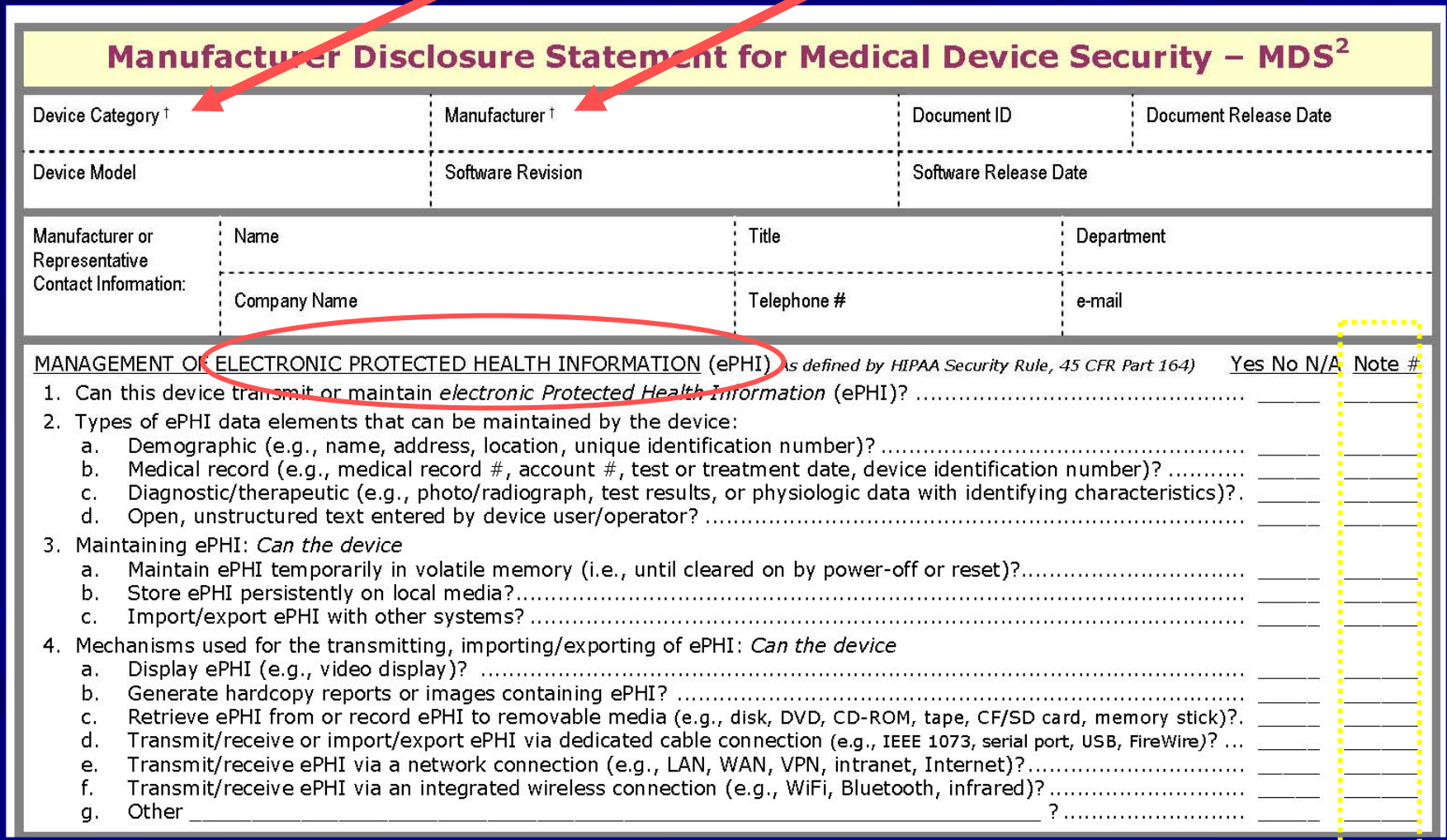
- HIMSS
  (Health Information and Management Systems Society)
- ACCE
  (American College of Clinical Engineering)
- ECRI
- NEMA
  (National Electrical Manufacturers Association)

MDS^2 supplies key data to the ACCE / ECRI Biomedical Equipment Survey Form



MDS² Form
Side 1

Standard Nomenclature (UMDNS)



Manufacturer Disclosure Statement for Medical Device Security – MDS²

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.

MDS² v 1.0 *(2004-11-01)* **Side 1**

MDS^2 Form

Side 2

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.

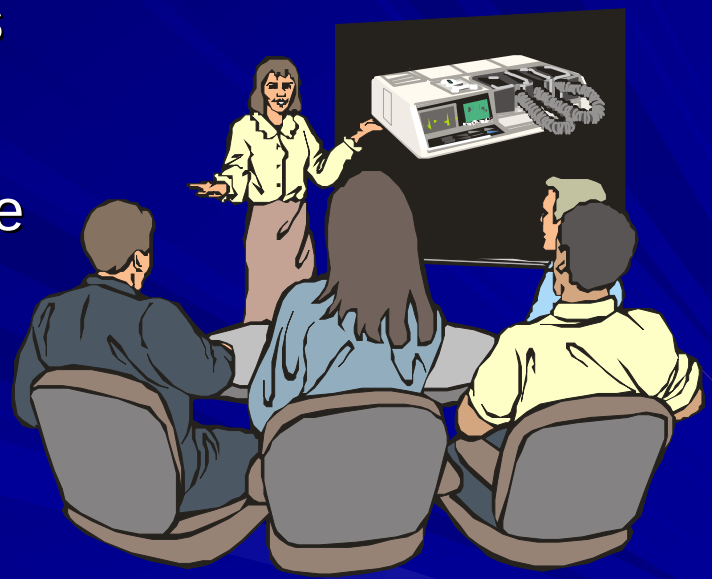
1.
2.

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^2 v 1.0 *(2004-11-01)* **Side 2**

Healthcare Providers Use MDS^2

- Information Security Committee
  - ✓ Reviews manufacturer-supplied MDS^2 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^2 to identify common classes of technology with common vulnerabilities
  - ✓ Uses MDS^2 to take common approaches to mitigating risks with those common classes where possible



Future of MDS^2 - *Automation*

- The MDSW is developing and plans to publish an MDS^2 schema and reference toolkit with open source software. The schema and toolkit would
  - ✓ unambiguously define a structured representation of the MDS^2 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^2
  - ✓ large-scale distribution of MDS^2 data by manufacturers to major healthcare providers
  - ✓ large-scale analysis of MDS^2 data by healthcare providers
  - ✓ establishing a central repository of MDS^2 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

- HIMSS November 8, 2004 Press Release on MDS^2
  http://www.himss.org/pressroom/ASP/releaseDetail.asp?ContentID=59072

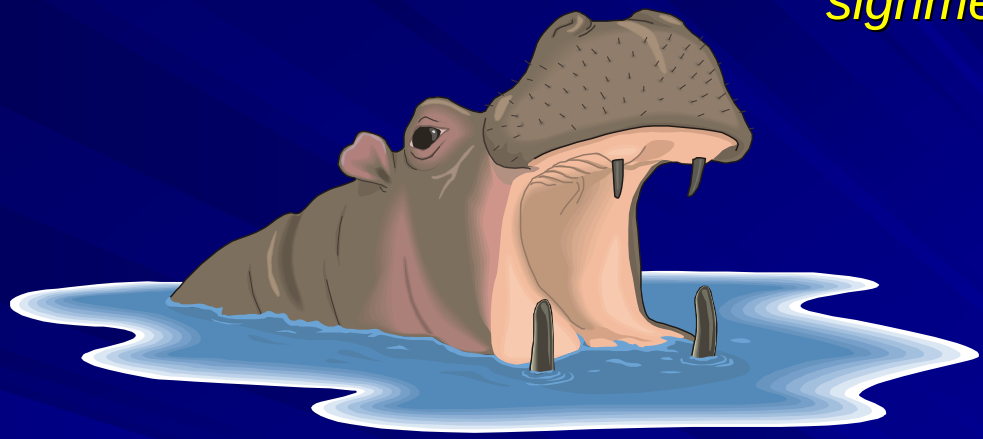
- Manufacturer's Disclosure Statement for Medical Device Security (MDS2) Form & Instructions
  http://www.himss.org/content/files/MDS2FormInstructions.pdf

Free Download

- Manufacturers obtain *free* UMDNS (nomenclature) listing of their products by e-mailing ECRI at himss-mds@ecri.org

Questions?

Stephen L. Grimes, FACCE
slgrimes@shcta.com



Strategic Health Care Technology Associates
www.shcta.com
Health Information and Management Systems Society
www.himms.org
American College of Clinical Engineering (ACCE)
www.accenet.org
ECRI
www.ecri.org

A NONPROFIT AGENCY