Security of Medical Device Applications

ellumen

Expert IT Services for Healthcare Transformation

Dennis M. Seymour, CISSP, PMP
Senior Security Architect
Ellumen, Inc.

Prepared for

14th Semi-Annual Software Assurance Forum

- Objectives
- Recent Article – (ISC)2
- FDA Regulatory Requirements
- International Regulatory Requirements
- Health Information & Management Systems Society (HIMSS) Medical Device Security Task Force

Objectives

- How do medical data security requirements differ from other networked devices and applications?
- What regulations are specific to medical device security?
- What risks do medical devices bring to my networks?
- Who is responsible for mitigation of risks and addressing issues with these devices?

Recent Article – (ISC)2

- Issue 13 (February 2011)
- The State of Secure Software

THE STATE OF SECURE SOFTWARE

New research reveals a disconnect between the need for secure software and the policies and practices to make it so, writes Peter Fretty.

AS WE BECOME A MORE DIGITAL SOCIETY, it's important to recognize the increasing volume and kinds of data threats. While this may seem like common sense to information security professionals, according to a recent survey conducted by Creative Intellect Consulting (CIC) and partially sponsored by (ISC)², there is reason for concern.

"Organizations say they understand the dangers," says Bola Rotibi, research director at CIC. "However, when you look at the data, it suggests that we have serious issues as an industry, especially considering how many people do not follow their own policies. There are holes everywhere that are ripe for cyber attacks, and there is a need for organizations to take this more seriously."

Information security professionals—such as security architects, developers and IT leaders—in both private and public sectors across the globe participated in the State of Secure Application Lifecycle Management survey. The survey's goal was to establish a benchmark for security integration throughout the software development lifecycle.

"Before the industry can take a serious step forward, it's crucial to understand the capacity of organizations to achieve success," Rotibi says. "The results should enable us as a community to assess the capabil

- FDA Regulatory Requirements
  - Current
    - 510K
  - Upcoming Implementation Requirement
    - Plan of Action for Implementation

FDA 510(k)

- Under section 510(k) of the Act, a person who intends to introduce a device into commercial distribution is required to submit a premarket notification, or 510(k), to FDA at least 90 days before commercial distribution is to begin.
- Essentially a self-reporting standard
- FDA maintains a searchable database:

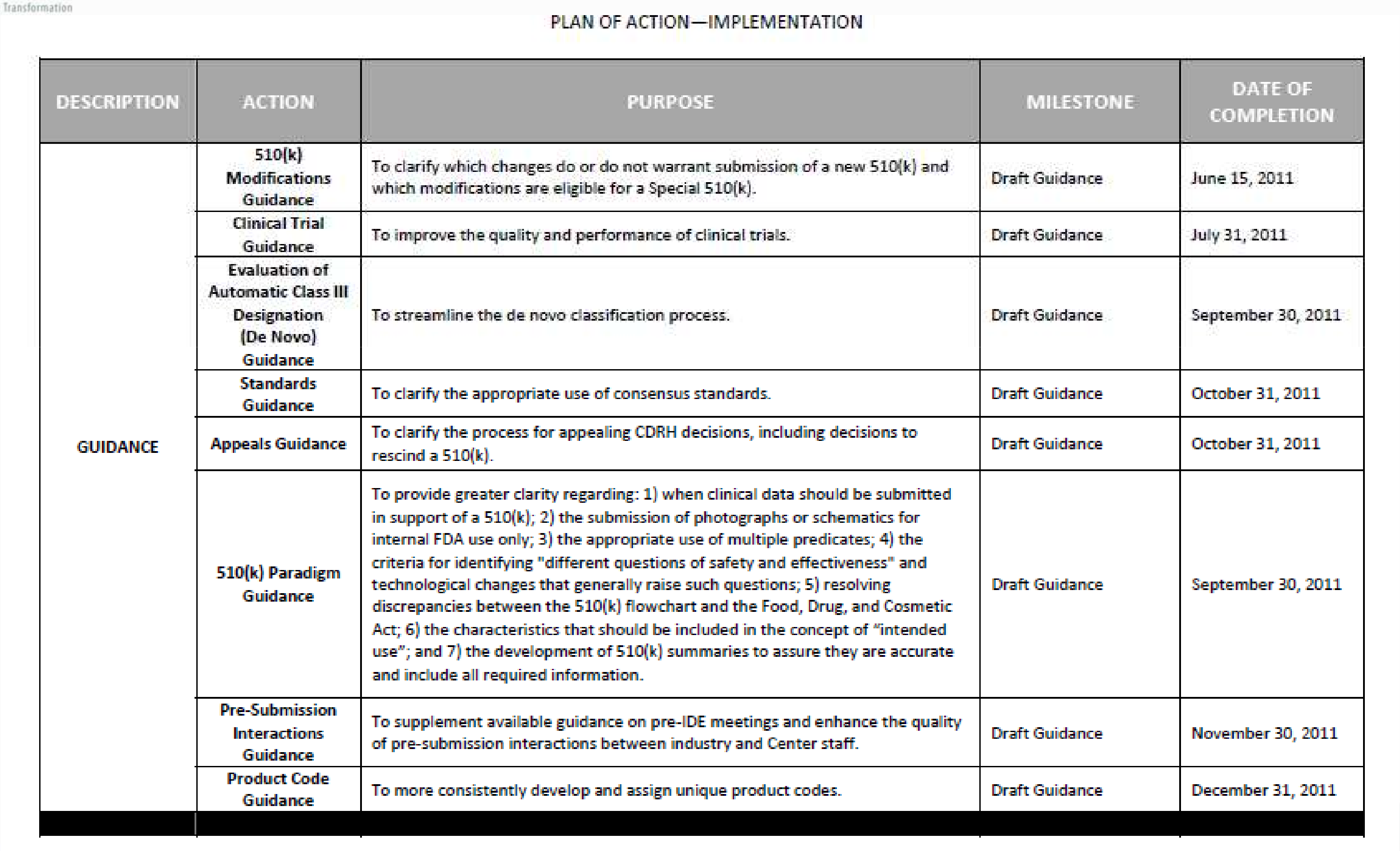
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/pmn.cfm

FDA PLAN OF ACTION FOR IMPLEMENTATION OF 510(K)

- August 2010, the FDA’s Center for Devices and Radiological Health (CDRH or the Center) released for public comment the preliminary reports from the 510(k) Working Group and the Task Force on the Utilization of Science in Regulatory Decision Making.
  - The 510(k) Working Group was charged with evaluating the 510(k) program and exploring actions CDRH could take to enhance 510(k) decision making.
  - The Task Force was charged with making recommendations on how the Center can quickly incorporate new science, including evolving information, novel technologies, and new scientific methods, into its decision making in as predictable a manner as is practical. In addition, the Institute of Medicine (IOM) is conducting an independent evaluation of the 510(k) program
- FDA solicited and received a range of perspectives in developing these reports and on the recommendations contained in these reports at public and town hall meetings.

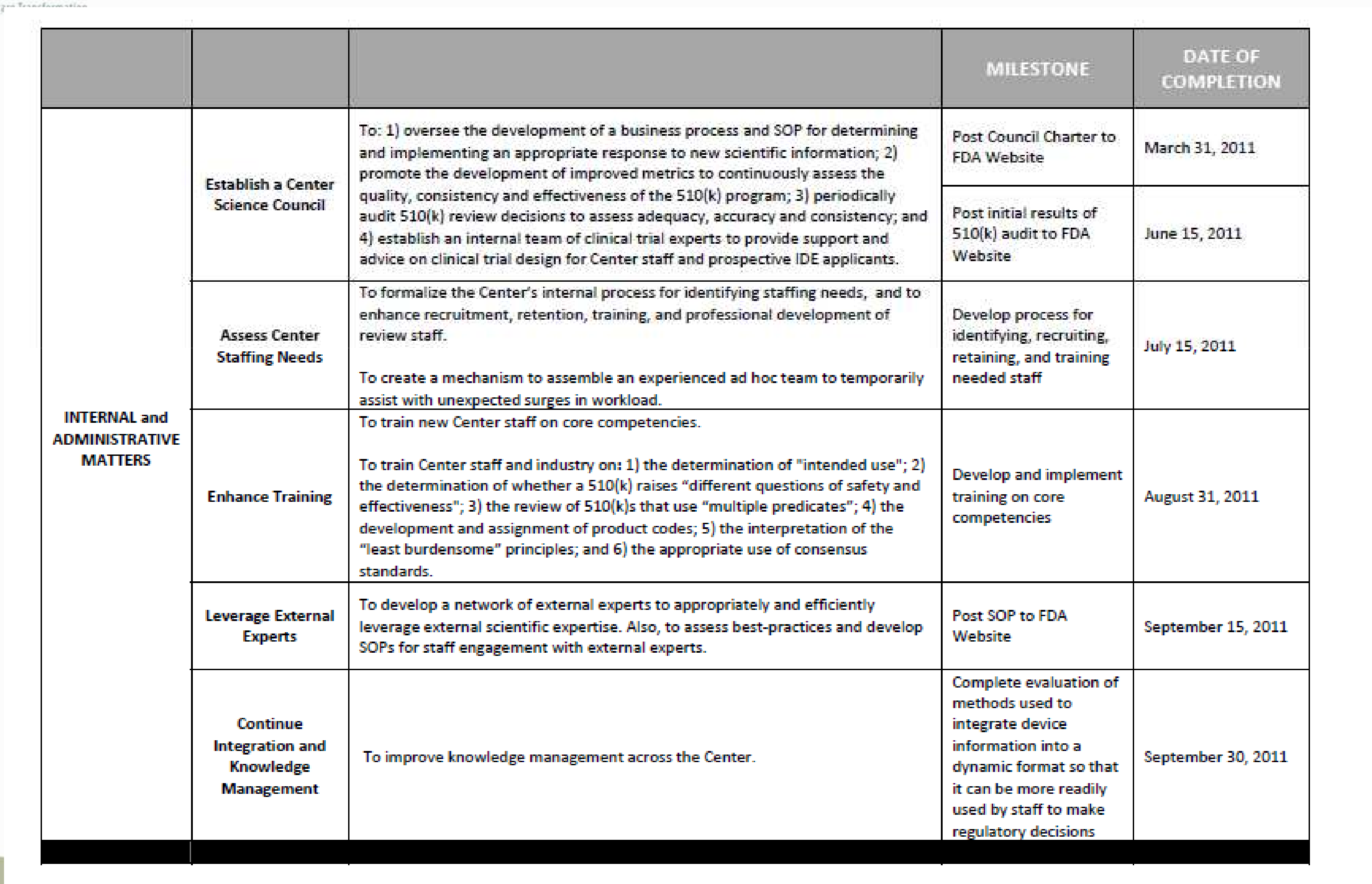
- CDRH developed 25 Action Items listed on the following slides
- CDRH may issue device-specific guidance on :
  - 1) when and what type of manufacturing data to submit;
  - 2) when a pre-clearance inspection would be conducted;
  - 3) when and what types of modifications should be periodically reported in lieu of submitting a 510(k); or
  - 4) when and what type of safety and effectiveness information for the device to be reviewed that is known to the manufacturer should be submitted as a brief description.
  - Because CDRH would only issue guidance on any of these four issues on a case-by-case basis there is no set timeframe for taking an action.
- FDA will post updates on the status of planned actions on CDRH's website.

Plan of Action for FDA



PLAN OF ACTION—IMPLEMENTATION

DESCRIPTION	ACTION	PURPOSE	MILESTONE	DATE OF COMPLETION
GUIDANCE	510(k) Modifications Guidance	To clarify which changes do or do not warrant submission of a new 510(k) and which modifications are eligible for a Special 510(k).	Draft Guidance	June 15, 2011
	Clinical Trial Guidance	To improve the quality and performance of clinical trials.	Draft Guidance	July 31, 2011
	Evaluation of Automatic Class III Designation (De Novo) Guidance	To streamline the de novo classification process.	Draft Guidance	September 30, 2011
	Standards Guidance	To clarify the appropriate use of consensus standards.	Draft Guidance	October 31, 2011
	Appeals Guidance	To clarify the process for appealing CDRH decisions, including decisions to rescind a 510(k).	Draft Guidance	October 31, 2011
	510(k) Paradigm Guidance	To provide greater clarity regarding: 1) when clinical data should be submitted in support of a 510(k); 2) the submission of photographs or schematics for internal FDA use only; 3) the appropriate use of multiple predicates; 4) the criteria for identifying "different questions of safety and effectiveness" and technological changes that generally raise such questions; 5) resolving discrepancies between the 510(k) flowchart and the Food, Drug, and Cosmetic Act; 6) the characteristics that should be included in the concept of "intended use"; and 7) the development of 510(k) summaries to assure they are accurate and include all required information.	Draft Guidance	September 30, 2011
	Pre-Submission Interactions Guidance	To supplement available guidance on pre-IDE meetings and enhance the quality of pre-submission interactions between industry and Center staff.	Draft Guidance	November 30, 2011
	Product Code Guidance	To more consistently develop and assign unique product codes.	Draft Guidance	December 31, 2011

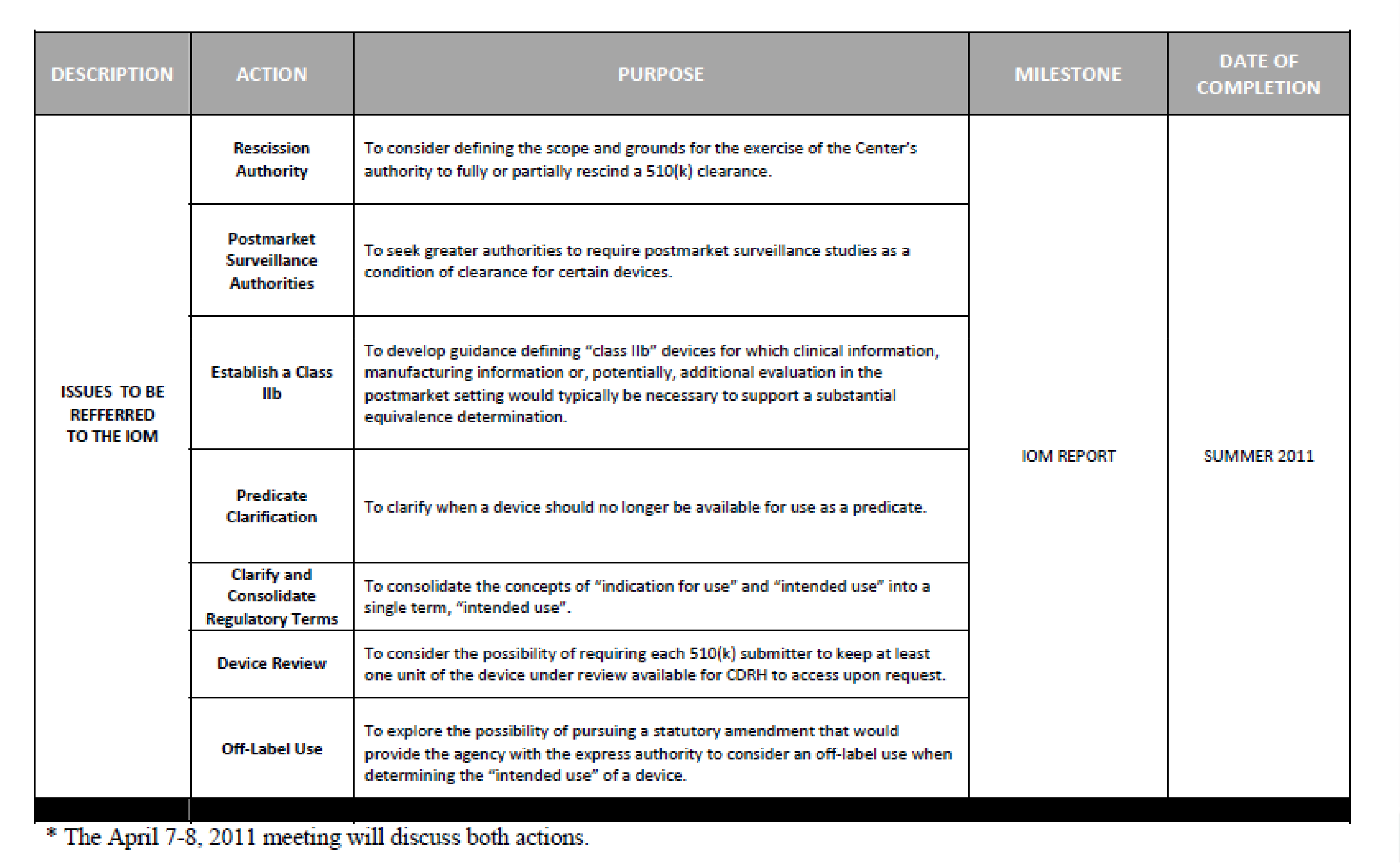


			MILESTONE	DATE OF COMPLETION
INTERNAL and ADMINISTRATIVE MATTERS	Establish a Center Science Council	To: 1) oversee the development of a business process and SOP for determining and implementing an appropriate response to new scientific information; 2) promote the development of improved metrics to continuously assess the quality, consistency and effectiveness of the 510(k) program; 3) periodically audit 510(k) review decisions to assess adequacy, accuracy and consistency; and 4) establish an internal team of clinical trial experts to provide support and advice on clinical trial design for Center staff and prospective IDE applicants.	Post Council Charter to FDA Website	March 31, 2011
			Post initial results of 510(k) audit to FDA Website	June 15, 2011
	Assess Center Staffing Needs	To formalize the Center's internal process for identifying staffing needs, and to enhance recruitment, retention, training, and professional development of review staff. To create a mechanism to assemble an experienced ad hoc team to temporarily assist with unexpected surges in workload.	Develop process for identifying, recruiting, retaining, and training needed staff	July 15, 2011
	Enhance Training	To train new Center staff on core competencies. To train Center staff and industry on: 1) the determination of "intended use"; 2) the determination of whether a 510(k) raises "different questions of safety and effectiveness"; 3) the review of 510(k)s that use "multiple predicates"; 4) the development and assignment of product codes; 5) the interpretation of the "least burdensome" principles; and 6) the appropriate use of consensus standards.	Develop and implement training on core competencies	August 31, 2011
	Leverage External Experts	To develop a network of external experts to appropriately and efficiently leverage external scientific expertise. Also, to assess best-practices and develop SOPs for staff engagement with external experts.	Post SOP to FDA Website	September 15, 2011
	Continue Integration and Knowledge Management	To improve knowledge management across the Center.	Complete evaluation of methods used to integrate device information into a dynamic format so that it can be more readily used by staff to make regulatory decisions	September 30, 2011

ellumen
Expert IT Services for Healthcare Transformation

			MILESTONE	DATE OF COMPLETION
PROGRAMMATIC and REGULATORY	Implement an "Assurance Case" Pilot Program	To explore the use of an "assurance case" framework for 510(k) submissions.	Start pilot program	March 31, 2011
	Provide Additional Information About Regulated Products	To make device photographs available in a public database without disclosing proprietary information.	Public Meeting *	April 7 - 8, 2011 *
	Improve Collection and Analysis of Postmarket Information	To develop better data sources, methods and tools for collecting and analyzing meaningful postmarket information, and to enhance the Center's capabilities to support evidence synthesis and quantitative decision making.	Determine system requirements and select the platform for a new adverse event database	June 30, 2011
	Establish "Notice to Industry Letters" as a Standard Practice	To clarify and more quickly inform stakeholders when CDRH has changed its regulatory expectations on the basis of new scientific information.	Post SOP to FDA Website	June 15, 2011
	Improve the IDE Process	To better characterize the root causes of existing challenges and trends in IDE decision making. Assess, characterize and mitigate challenges in reviewing IDE's.	Complete program assessment	June 30, 2011
	Implement a Unique Device Identification (UDI) System	To permit the rapid and accurate identification of devices, to facilitate and improve adverse event reporting and identification of device-specific problems.	Issue proposed regulation	June 30, 2011
	Multiple Predicate Analysis	To conduct additional analyses to determine the basis for the apparent association between citing more than five predicates and a greater mean rate of adverse event reports.	Complete analysis and make results public	October 31, 2011

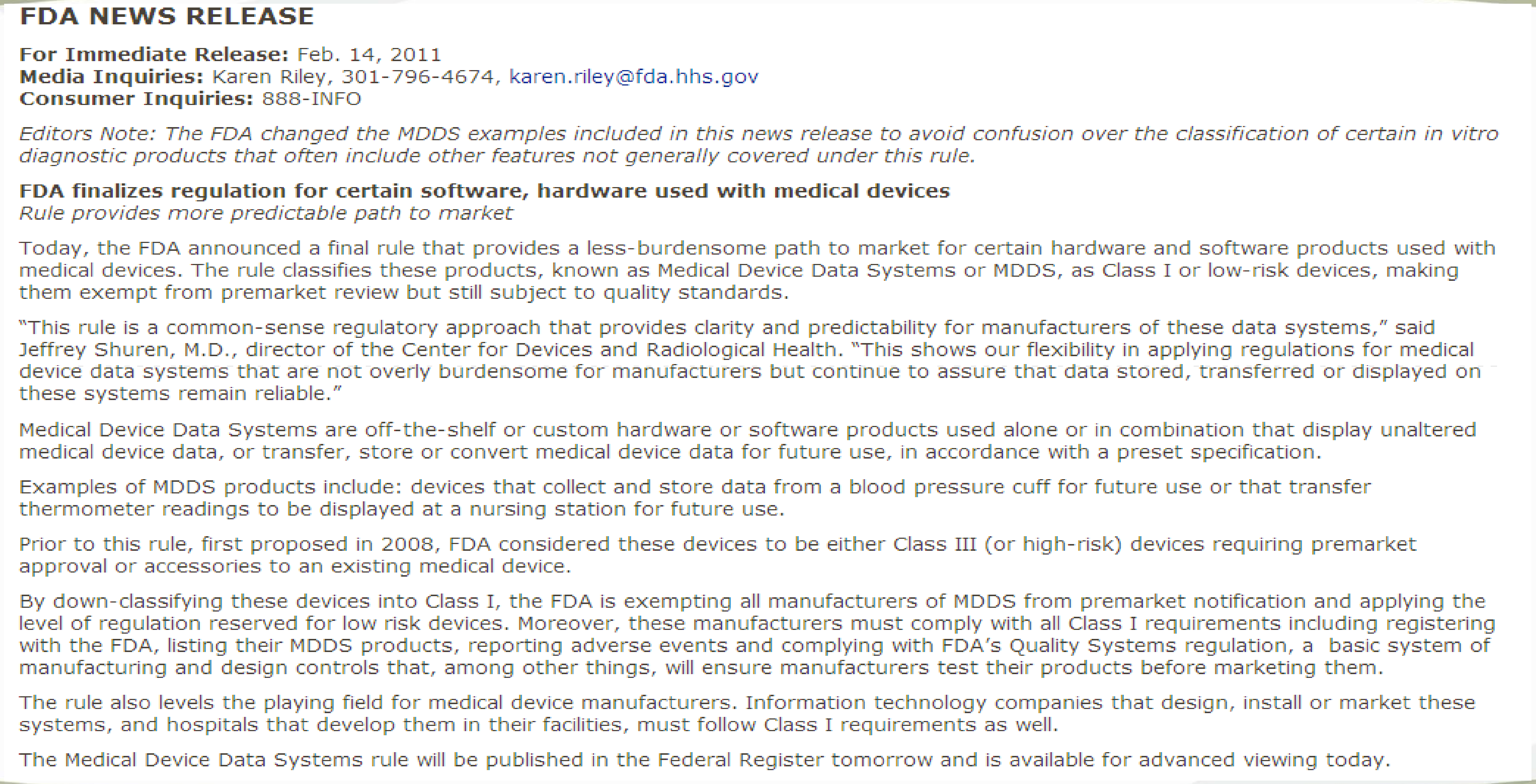
			MILESTONE	DATE OF COMPLETION
PROGRAMMATIC and REGULATORY (cont.)	Clarify and Improve Third-Party Review	To develop a process for regularly evaluating the list of device types eligible for third-party review and to enhance third-party reviewer training.	Post SOP to FDA Website	September 30, 2011
	Streamline Guidance and Regulation Development Process	To provide greater clarity, predictability, and efficiency in the guidance and regulation development process.	Post SOPs to FDA Website	July 31, 2011
	Draft 510(k) Transfer of Ownership Regulation	To better document 510(k) transfers of ownership.	Issue proposed regulation	December 31, 2011
	Improve Medical Device Labeling	To develop an on-line labeling repository.	Public Meeting *	April 7 - 8, 2011 *
		To clarify the statutory listing requirements for the submission of labeling.	Issue proposed regulation	December 31, 2011



DESCRIPTION	ACTION	PURPOSE	MILESTONE	DATE OF COMPLETION
ISSUES TO BE REFFERRED TO THE IOM	**Rescission Authority**	To consider defining the scope and grounds for the exercise of the Center's authority to fully or partially rescind a 510(k) clearance.	IOM REPORT	SUMMER 2011
	Postmarket Surveillance Authorities	To seek greater authorities to require postmarket surveillance studies as a condition of clearance for certain devices.		
	Establish a Class IIb	To develop guidance defining "class IIb" devices for which clinical information, manufacturing information or, potentially, additional evaluation in the postmarket setting would typically be necessary to support a substantial equivalence determination.		
	Predicate Clarification	To clarify when a device should no longer be available for use as a predicate.		
	Clarify and Consolidate Regulatory Terms	To consolidate the concepts of "indication for use" and "intended use" into a single term, "intended use".		
	Device Review	To consider the possibility of requiring each 510(k) submitter to keep at least one unit of the device under review available for CDRH to access upon request.		
	Off-Label Use	To explore the possibility of pursuing a statutory amendment that would provide the agency with the express authority to consider an off-label use when determining the "intended use" of a device.		

* The April 7-8, 2011 meeting will discuss both actions.

Medical Device Data Systems



FDA NEWS RELEASE

For Immediate Release: Feb. 14, 2011
Media Inquiries: Karen Riley, 301-796-4674, karen.riley@fda.hhs.gov
Consumer Inquiries: 888-INFO

Editors Note: The FDA changed the MDDS examples included in this news release to avoid confusion over the classification of certain in vitro diagnostic products that often include other features not generally covered under this rule.

FDA finalizes regulation for certain software, hardware used with medical devices
Rule provides more predictable path to market

Today, the FDA announced a final rule that provides a less-burdensome path to market for certain hardware and software products used with medical devices. The rule classifies these products, known as Medical Device Data Systems or MDDS, as Class I or low-risk devices, making them exempt from premarket review but still subject to quality standards.

"This rule is a common-sense regulatory approach that provides clarity and predictability for manufacturers of these data systems," said Jeffrey Shuren, M.D., director of the Center for Devices and Radiological Health. "This shows our flexibility in applying regulations for medical device data systems that are not overly burdensome for manufacturers but continue to assure that data stored, transferred or displayed on these systems remain reliable."

Medical Device Data Systems are off-the-shelf or custom hardware or software products used alone or in combination that display unaltered medical device data, or transfer, store or convert medical device data for future use, in accordance with a preset specification.

Examples of MDDS products include: devices that collect and store data from a blood pressure cuff for future use or that transfer thermometer readings to be displayed at a nursing station for future use.

Prior to this rule, first proposed in 2008, FDA considered these devices to be either Class III (or high-risk) devices requiring premarket approval or accessories to an existing medical device.

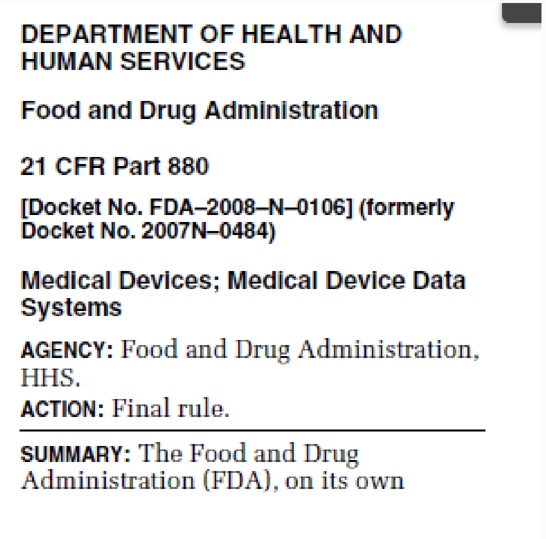
By down-classifying these devices into Class I, the FDA is exempting all manufacturers of MDDS from premarket notification and applying the level of regulation reserved for low risk devices. Moreover, these manufacturers must comply with all Class I requirements including registering with the FDA, listing their MDDS products, reporting adverse events and complying with FDA's Quality Systems regulation, a basic system of manufacturing and design controls that, among other things, will ensure manufacturers test their products before marketing them.

The rule also levels the playing field for medical device manufacturers. Information technology companies that design, install or market these systems, and hospitals that develop them in their facilities, must follow Class I requirements as well.

The Medical Device Data Systems rule will be published in the Federal Register tomorrow and is available for advanced viewing today.

MDDS Federal Register

ellumen
Expert IT Services for Healthcare Transformation



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 880

[Docket No. FDA–2008–N–0106] (formerly Docket No. 2007N–0484)

Medical Devices; Medical Device Data Systems

AGENCY: Food and Drug Administration, HHS.

ACTION: Final rule.

SUMMARY: The Food and Drug Administration (FDA), on its own

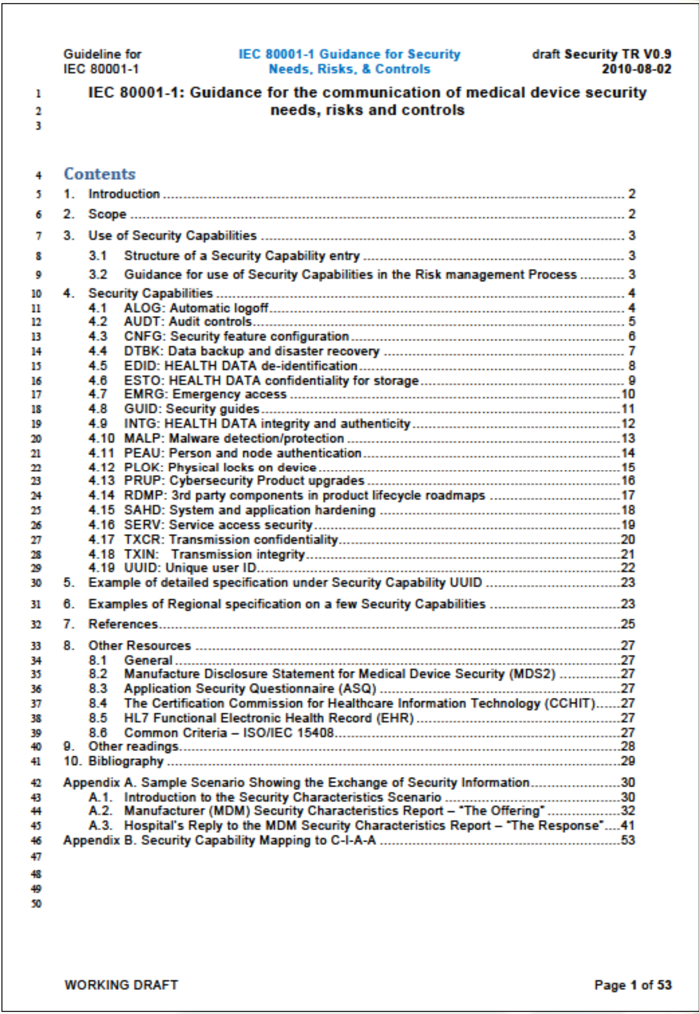
The Food and Drug Administration (FDA), on its own initiative, is issuing a final rule to reclassify Medical Device Data Systems (MDDSs) from class III (premarket approval) into class I (general controls).

MDDS devices are intended to transfer, store, convert from one format to another according to preset specifications, or display medical device data. MDDSs perform all intended functions without controlling or altering the function or parameters of any connected medical devices. An MDDS is not intended to be used in connection with active patient monitoring. FDA is exempting MDDSs from the premarket notification requirements.

DATES: This rule is effective April 18, 2011.

International Regulatory Requirements

- The IEC 80001 - *The Application of Risk Management to IT-Networks Incorporating Medical Devices,* provides:
  - Roles,
  - Responsibilities, and
  - Activities necessary for risk management.
- This security report provides:
  - Additional guidance in how security capabilities might be referenced in both the Risk Management process and stakeholder communications and agreements.
  - Presents an informative set of common, high-level security capabilities for many IT-network connected products and services.



Guideline for IEC 80001-1 | IEC 80001-1 Guidance for Security Needs, Risks, & Controls | draft Security TR V0.9 2010-08-02

IEC 80001-1: Guidance for the communication of medical device security needs, risks and controls

Contents

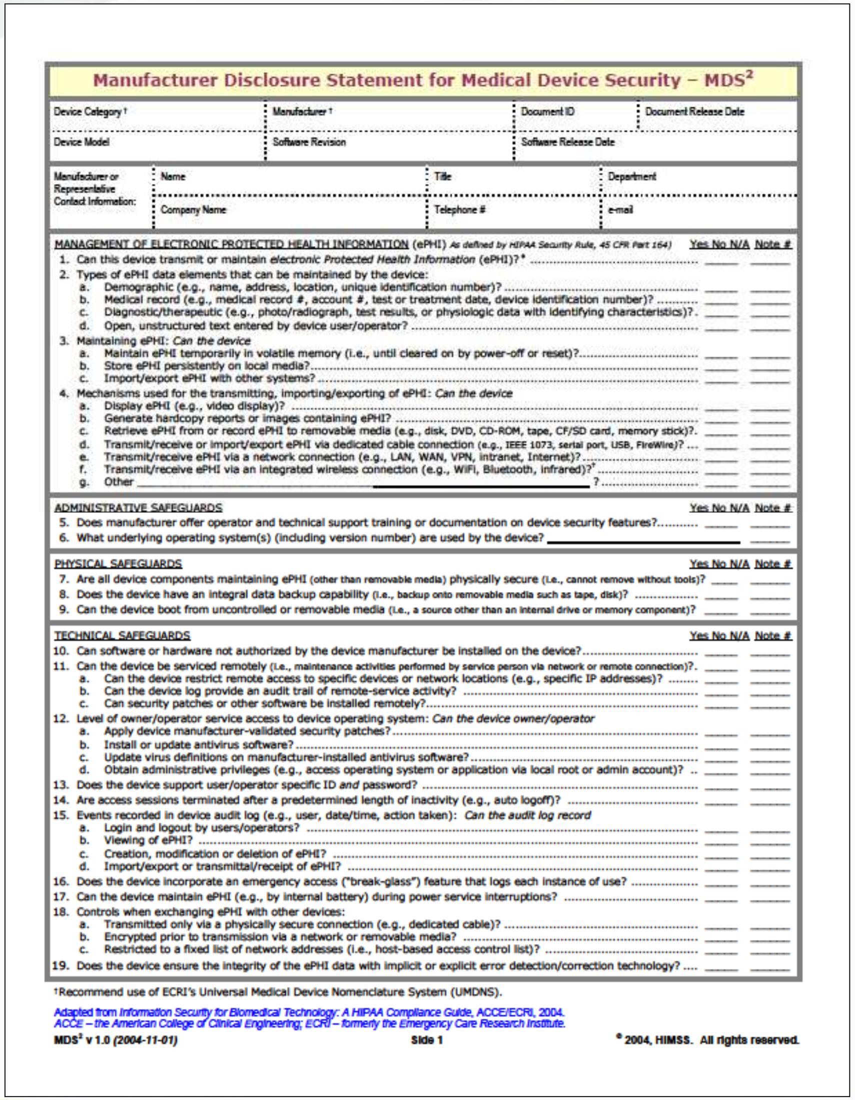
WORKING DRAFT | Page 1 of 53

HIMSS Medical Device Security Task Force

- Health Information & Management Systems Society (HIMSS) Medical Device Security Task Force
  - Manufacturers Disclosure Statement for Medical Device Security (MDS2)
    - Current Version – based solely on HIPAA requirements
    - Draft Revision to address IEC 80001 and HITECH

Current MDS2 Form

ellumen
Expert IT Services for Healthcare Transformation



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

<u>MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION</u> (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 ________________________ ? .... ____ ____

<u>ADMINISTRATIVE SAFEGUARDS</u> 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? ________________ ____

<u>PHYSICAL SAFEGUARDS</u> 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)? ____ ____

<u>TECHNICAL SAFEGUARDS</u> Yes No N/A Note #

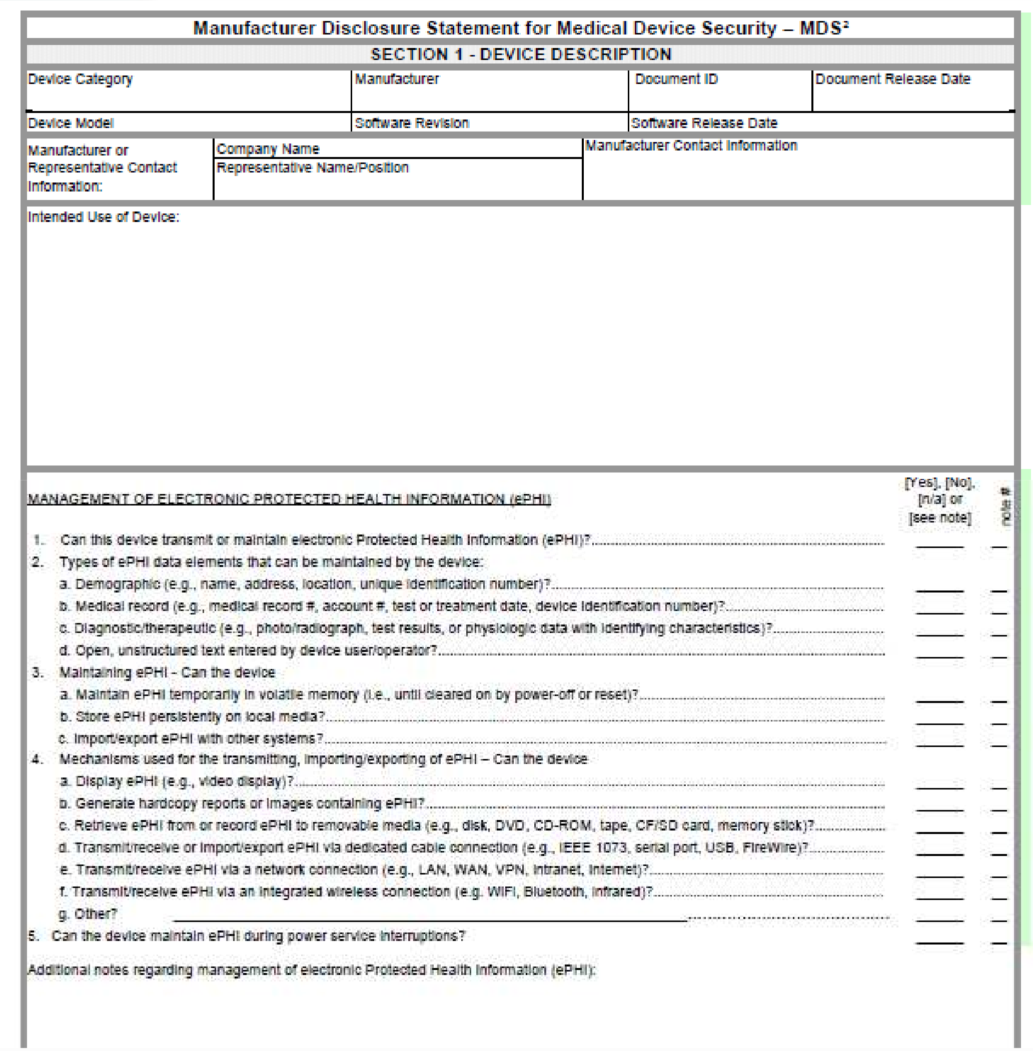
10. Can software or hardware not authorized by the device manufacturer be installed on the device? .... ____ ____
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?. ____ ____
    a. Can the device restrict remote access 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^2 v 1.0 *(2004-11-01)* Side 1

Proposed Updated MDS2 Form



Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1 - DEVICE DESCRIPTION

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

Intended Use of Device:

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) — [Yes], [No], [n/a] or [see note] — 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?
5. Can the device maintain ePHI during power service interruptions?

Additional notes regarding management of electronic Protected Health Information (ePHI):

Draft Revision addresses IEC 800001 and HITECH

Mitigation and Addressing Risks

- Adapt future development to include new FDA guidance
- Build security into the applications and devices
- Network Isolation Architecture
- Other Risk Mitigation

HIMSS MDSTF Future Projects

- Review and Release of new MDS2
- Development of Crosswalk between IEC 80001, NIST SP 800 series, and DIACAP

Review

- – Security requirements must be considered during development.
- – Regulations specific to medical device security should be more easily evaluated.
- – Medical devices can increase risks to your networks, risk assessment must be part of the process for procurement
- – Assign responsibility for risk mitigation to appropriate individuals.

Contact Information:

Dennis M. Seymour, CISSP, PMP

dseymour@ellumen.com

(419) 205-1619