Security of Medical Device Applications



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 DISITAL SOCIETY, its augmentant to recognize the increasing relicions and families of data objects. While this way were like contains when to information security preferencesh, according to a recent servery weeks that for Courtee (and for Courtee) and perturbly operation of the COURT, there is reason for concern.

"Organizations are they condend and the dangers," sees Boda Existic revents directive at CEC." However, where you look at the data, it suggests that we have services instant as an industry expectably considering how many peoply do not believe other earn pelation. There are hollow everywhere that are right or other attacks, and there is a send for expectations to take this rever serviced."

Information security professionals—such as security architects, developers and YI feabers—so both private and public sections across the globe participated in the Your of Security Application Lifection Management servey. The survey's goal was no establish a benchmark for security integration throughout the software development Maryotic.

"Serious the malastry can take a serious step forward, it's crucial to understand the capacity of organizations to achieve sources," Rottle sees. "The results devoid madde as so a community to assess the capacital

12 PRODUCTION PROFESSIONAL WAS ALREADY



- 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
	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
GUIDANCE	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
		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	Post Council Charter to FDA Website	March 31, 2011
	Establish a Center Science Council	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 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
INTERNAL and ADMINISTRATIVE MATTERS	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



			MILESTONE	DATE OF COMPLETION
	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 *
PROGRAMMATIC	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
and REGULATORY	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	To better characterize the root causes of existing challenges and trends in IDE decision making.	Complete program	June 30, 2011
	Process	Assess, characterize and mitigate challenges in reviewing IDE's.	assessment	
	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
	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
PROGRAMMATIC and REGULATORY (cont.)	Draft 510(k) Transfer of Ownership Regulation	To better document 510(k) transfers of ownership.	Issue proposed regulation	December 31, 2011
	Improve Medical	To develop an on-line labeling repository.	Public Meeting *	April 7 - 8, 2011 *
_	Device Labeling	To clarify the statutory listing requirements for the submission of labeling.	Issue proposed regulation	December 31, 2011



DESCRIPTION	ACTION	PURPOSE	MILESTONE	DATE OF COMPLETION
	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.		
	Postmarket Surveillance Authorities	To seek greater authorities to require postmarket surveillance studies as a condition of clearance for certain devices.		
ISSUES TO BE REFFERRED TO THE IOM	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.	IOM REPORT ble 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". 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



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.

		ideline for IEC 80001-1 Guidance for Security draft Securit C 80001-1 Needs, Risks, & Controls 2	ty T 2010
1 2 3		IEC 80001-1: Guidance for the communication of medical device sec needs, risks and controls	curi
4	Со	ontents	
5	1.	Introduction	
6	2.		
7	3.	Use of Security Capabilities	
	٥.	· ·	
8		3.1 Structure of a Security Capability entry	
9		3.2 Guidance for use of Security Capabilities in the Risk management Process	
10	4.	Security Capabilities	٠ '
11 12		4.1 ALOG: Automatic logoff	
13		4.3 CNFG: Security feature configuration	
14		4.4 DTBK: Data backup and disaster recovery	
15		4.5 EDID: HEALTH DATA de-identification	
16		4.6 ESTO: HEALTH DATA confidentiality for storage	
17		4.7 EMRG: Emergency access	
18		4.8 GUID: Security guides	
19 20		4.9 INTG: HEALTH DATA integrity and authenticity	
20		4.11 PEAU: Person and node authentication	
22		4.12 PLOK: Physical locks on device	
23		4.13 PRUP: Cybersecurity Product upgrades	10
24		4.14 RDMP: 3rd party components in product lifecycle roadmaps	
25		4.15 SAHD: System and application hardening	
26		4.16 SERV: Service access security	
27 28		4.17 TXCR: Transmission confidentiality	
29		4.19 UUID: Unique user ID.	5
30	5.	Example of detailed specification under Security Capability UUID	
31	6.	Examples of Regional specification on a few Security Capabilities	2
32	7.		
33	8.	Other Resources	
34		8.1 General	
35 36		8.2 Manufacture Disclosure Statement for Medical Device Security (MDS2)	
37		8.4 The Certification Commission for Healthcare Information Technology (CCHIT)	
38		8.5 HL7 Functional Electronic Health Record (EHR)	2
39		8.6 Common Criteria – ISO/IEC 15408	2
40	9.	Other readings	
41	10.	. Bibliography	2
42	App	pendix A. Sample Scenario Showing the Exchange of Security Information	3
43		A.1. Introduction to the Security Characteristics Scenario	3
44		A.2. Manufacturer (MDM) Security Characteristics Report – "The Offering"	3
45	Acc	A.3. Hospital's Reply to the MDM Security Characteristics Report - "The Response".	
46 47	App	pendix B. Security Capability Mapping to C-I-A-A	5
7/			

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



	ice Calegory †		Manufacturer †		Document ID	Document Re	lease Date	
	ice Model		Software Revision		Software Release De	ale		
	ufacturer or	Name	.00	Title	- 3	Department		
	resentative tact Information:	Company Name		Telephone #		етаї		•••••
100	NO SOURCE TO PRODUCE OF		ECTED HEALTH INFORMAT		• 28) ************************************		e115-62-000 co	
3.	Types of ePHI a. Demogri b. Medical c. Diagnosi d. Open, ui maintaining ei a. Maintain b. Store ef c. Import/ Mechanisms u a. Display b. Generat c. Retrieve d. Transmit e. Transmit e. Transmit	data elements that applic (e.g., name, a a record (e.g., med, a a record (e.g., med, a ic/therapeutic (e.g., structured text ent) PHI: Can the device ePHI temporarily in it persistently on it export ePHI with oth sed for the transmil ePHI (e.g., video dis a hardcopy reports or ePHI from or record (receive ePHI via a receive or import/ preceive ePHI via a	ain electronic Protected III can be maintained by the didress, location, unique is in record #, account #, ites photo/radiograph, test rend by device user/operal velatile memory (i.e., unical media? er systems? Litting, importing/exporting pigh?) r images containing ePHI time is ePHI to removable media export ePHI via dedicated export ePHI via dedicated metwork connection (e.g., enetwork enetwork connection (e.g., enetwork enetwork connection (e.g., enetwork	device: to treatment date, d suits, or physiologic d tor? til cleared on by powe of ePHI: Can the devi y (e.g., disk, DVD, CD-6 cable connection (e.g., LAN, WAN, PWN, intre	evice identification lets with identifying r-off or reset)?	number)? characteristics)? d, memory stick)? , USB, FireWire)?		
5. 6.	What underly	turer offer operator ng operating system	and technical support train(s) (including version nur			features?		
5. 6. PHY 7. 8.	What underly SICAL SAFEGI Are all device Does the devi	turer offer operator ing operating system JARDS components maintage ce have an integral		mber) are used by the vable media) physically , backup onto removable	secure (i.e., cannot r	features?	es No N/A	Note
5. 6. PHY 7. 8. 9.	What underly SICAL SAFEGI Are all device Does the devi	cturer offer operator ing operating system JARDS components mainta ce have an integral e boot from uncontr	n(s) (including version nur sining ePHI (other than remo data backup capability (i.e.	mber) are used by the vable media) physically , backup onto removable	secure (i.e., cannot r	remove without tools) lisk)?	es No N/A	Note
5. 6. PH) 7. 8. 9.	Does manufactive What underly CSICAL SAFEGI Are all device Does the devican the devic CHNICAL SAFEC Can software	turer offer operator ing operating system JARDS components mainta ce have an integral e boot from uncontr SUARDS or hardware not aut	n(s) (including version nur bining ePHI (other than remo data backup capability (i.e. oilled or removable media thorized by the device mar	mber) are used by the vable media) physically ., backup onto removable (i.e., a source other than nufacturer be installed	secure (i.e., cannot r media such as tape, c an internal drive or m on the device?	reatures?	es No N/A	Note
5. 6. PH) 7. 8. 9.	Does manufact What underly SICAL SAFEG Are all device Does the device Can the device Can software Can the device Can control of the device Can the device Ca	turer offer operator ng operating system JARDS components mainta ce have an integral e boot from uncontr SJARDS or hardware not aute be serviced remot device restrict remo	n(s) (including version nur sining ePHI (other than remo data backup capability (i.e. olled or removable media chorized by the device mar- ely (i.e., maintenance activities the access to specific device	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than nufacturer be installed as performed by service p es or network location	Secure (Le., cannot r media such as tape, c an internal drive or m on the device? erson via network or r s (e.g., specific IP a	features?	es No N/A ?	Note
5. 6. PH) 7. 8. 9.	Does manufar What underly! SICAL SAFEG! Are all device Does the device Can the device CHNICAL SAFE! Can software Can the device a. Can the b. Can the	cturer offer operator ing operating system IARDS components maintage e boot from uncontract SUARDS or hardware not aut e be serviced remot device restrict remot provide as	n(s) (including version nur sining ePHI (other than remo data backup capability (i.e. olled or removable media thorized by the device mar lely (i.e., maintenance activitie te access to specific device in audit trail of remote-ser-	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than urfacturer be installed as performed by service p es or network location vice activity?	Secure (i.e., cannot r media such as tape, c an internal drive or m on the device? erson via network or r s (e.g., specific IP a	reatures?	es No N/A	Note
5. 6. 7. 8. 9. TEC 10.	Does manufact What underly YSICAL SAFEGI Are all device Does the devic Can the devic ChINICAL SAFEC Can software Can the devic a. Can the b. Can the c. Can sect Level of owne	turer offer operator no operating system JARDS: components mainta- ce have an integral e boot from uncontr SJARDS: or hardware not aut e be serviced remot device not provide a intly patches or othe ripperator service a	n(s) (including version nur sining ePHI (other than remo data backup capability (i.e. olled or removable media thorized by the device mar ely (i.e., maintenance activitie te access to specific device in audit trail of remote-ser is software be installed ner cocess to device operating in	mber) are used by the vable media) physically , backup onto removable (i.e., a source other than nufacturer be installed as performed by service p as or network location vice activity? motely? system: Can the device	secure (i.e., cannot r media such as tape, c an internal drive or m on the device? erson via network or r s (e.g., specific IP a	Yy emove without tools) lisk)? emory component)? Yy emote connection)?. ddresses)?	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10.	Does manufar What underly YSICAL SAFEGI Are all device Does the devi Can the devic Can software Can the devic a. Can the b. Can the c. Can sec Level of owne a. Apply de b. Install o	aturer offer operator no operating system JARDS components maintace have an integral e boot from uncontrol JARDS or hardware not aut e be serviced remote device restrict remo device to provide a unity patches or othe properator service a vice manufacturer update antivirus y update antivirus y update y update	n(s) (including version nur tining ePHI (other than remo data backup capability melia olided or removable melia olided or removable melia objective that the contract of the objective that the contract of the objective that the contract of the second of the contract of the contract of the second of the contract of the contract of the second of the contract of the contract of the version of the contract of the contract of the contract of the version of the contract of the contract of the contract of the version of the contract	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than nufacturer be installed as performed by service ses or network location vice activity? motely? system: Can the device?	device? Secure (i.a., cannot r media such as tape, c an internal drive or m on the device? erson via network or n s (e.g., specific IP a	features?	es No N/A	Note
5. 6. 7. 8. 9. TEC 10.	Does manufar What underly PSICAL SAFEG Does the devic Can the	turer offer operation no operating system JARDS components maintage e boot from uncontrol SUARDS or hardware not aut be serviced remot device to provide device restrict ritry patches or vice manufacturer- update antivirus drives demanufacturer- update antivirus drives demanufacturer- update antivirus drives demanufacturer- update antivirus drives demanufacturer- update antivirus drives demanufacturer- update antivirus drives drives demanufacturer- update antivirus drives drives demanufacturer- update antivirus drives drives demanufacturer- update antivirus drives drives demanufacturer- update antivirus drives	n(s) (including version nur sining ePHI (other than remo data backup capability (a. solided or removable media chorized by the device mar- ley (1.e., maintenance activities the access to specific device an audit trail of remote-se- re software be installed rer coses to device operating of the period of the cost of the cost product of the cost pro	mber) are used by the vable media) physically , backup onto removable (i.e., a source other than nufacturer be installed as performed by service p so or network location vice activity? modely? system: Can the devic? 	device? secure (i.e., cannot r media such as tape, an internal drive or m on the device? erron via network or r s (e.g., specific IP a	features?	es No N/A	Note
5. 6. 7. 8. 9. TEC 10. 11.	Does manufar What underly YSICAL SAFEG Are all device Does the devic Can the devic Can the devic Can the devic a. Can the b. Can the c. Can sec Level of owne a. Apply de b. Install o c. Update v d. Obtain a d. Obtain a	turer offer operation may operating system IARDS components maintace have an integral to boot from uncontract IARDS or hardware not auto device restrict remove device restrict remove envice manufacturer- vice manufacturer- vice manufacturer- in update antivirent in update in	n(s) (including version nur tining ePHI (other than remo data backup capability (i.e., oiled or removable media bioled or removable media bioled or removable media biolegical periodical periodical biolegical periodical periodical periodical periodical periodical p	when are used by the vable media) physically , backup onto removable (i.e., a source other than ufacturer be installed as performed by service jee or network location vice activity motely? system: Can the device vicinity of the control of the con	secure (i.a., cannot r media such as tape, e an internal drive or m on the device? erson via network or r s (e.g., specific IP a ce owner/operator m via local root or a	features?	es No N/A	Note
5. 6. 7. 8. 9. TEC 10. 11.	Does manufar What underly! **SICAL SAFEG Can the devic a. Can the b. Can the c. Can sec Level of owne a. Apply de b. Install o c. Update v d. Obtain a Does the devic	turer offer operation on operating system IARDS components maintace components maintace as boot from uncontrol in the component of hardware not suit as be serviced remote device to provide until patches or unity patches or unity patches or unity estimate unity estimate unity service unity s	n(s) (including version nur sining ePHI (other than remo data backup capability (a. solided or removable media chorized by the device mar- ley (1.e., maintenance activities the access to specific device an audit trail of remote-se- re software be installed rer coses to device operating of the period of the cost of the cost product of the cost pro	mber) are used by the vable media) physically , backup onto removable (i.e., a source other than nufacturer be installed so performed by service p so or network location vice activity? modely? system: Can the devic yiems: Can the application word?	secure (i.e., cannot remedia such as tape, de an internal drive or m on the device? earon via network or re (i.e.g., specific IP a secure over over over over over over over ov	features? Yi emove without tools] lisks? emory component)? Yi emovic connection)? ddresses)? ddresses)? ddmin account)?	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11.	Does manufar What underly! What underly! SIGLAL SAFEG Are all device Does the devic Can the devic Can the device Can the control Can the	turer offer operation may operating system IARDS components maintage components maintage to boot from uncontrol IARDS or hardware not auto device restrict remove device restrict remove device restrict remove device log provide entitle provide entitle provide entitle provide entitle provide entitle injustice injust	n(s) (including version nur tining ePHI (other than remo data backup capability (i.e., colled or removable media bioled or removable media bioled or removable media biolegical periodical periodical biolegical periodical biolegical periodical validated security patches cross to device operating validated security patches travere? nanufacturer-installed and proposed periodical proposed periodical validated	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than unfacturer be installed as performed by service es or network location vicio activity? motely? system: Can the device livinus software? g system or application word? to finactivity (e.g., as sction taken): Can the section taken): Can the	secure (i.e., cannot remedia such as tape, on internal drive or modia such as tape, an internal drive or mon the device? estoo via nativois or is (e.g., specific IP a commercial or internal drive or mon via local root or a subto logoff)? uto logoff)?	Yis emove without tools; list()? Yis emove without tools; list()? Yis emory component()? Yis emory component()? Yis emote connection()?	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11.	Does manufar What underly! STICAL SAFEGE AFE GE AFE AFE AFE AFE AFE AFE AFE AFE AFE AF	turer offer operator no operating system IARDS components maintace control of the control of the control of the the control of the the the the the the the the	n(s) (including version nur sining ePHI (other than remo data backup capability (i.e. colled or removable media chorized by the device mar- ley (i.e., maintenance activities the access to specific device in sudit trail of remote-ser- software be installed rer coess to device operating; influence of the control of the con- pression of the con- trained o	mber) are used by the vable media) physically , backup onto removable (i.e., a source other than nufacturer be installed as performed by service p so or network location vice activity? modely? system: Can the devic yellow vice activity? modely? system or application word? to finactivity (e.g., a sction taken): Can the	device? secure (Le., cannot remedia such as tape, de an internal drive or mon the device? on the device? erson via network or re (e.g., specific IP a commen/operator n via local root or a suto logoff)? a sudit log record	reatures? senove without tools) likely? semory component)? Yu semory components? Yu semory components? direction)? directions directions	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11.	Does manufar What underly Wiscla LaReiga Are all device Does the devi Can the device Can the device a. Can the b. Can the c. Can sect Level of owne a. Apply de b. Install of C. Update v d. Obtain a Does the devi Are access se Events record a. Login an b. Update v d. Obtain a Does the devi Are access and a Login and b. Update v d. Update v d. Obtain a Does the devi Are access and b. Update v d. Update v d. Obtain a Does the devi Are access and b. Update v d. C. Update v d. Obtain a Does the devi Are access and b. Update v d. C. Update v d. Obtain a Does the devi Are access access and b. Update v d. C. Update v d. C. Update v d. Obtain a Does the devi Are access and b. Update v d. C. Update v d. C. Update v d. Obtain a Does the devi Are access access and b. Update v d. Login and c. Login and b. Update v d. C. C. Evention of the devi	turer offer operation may operating system IARDS components maintage components maintage both the maintage components	n(s) (including version nur tining ePHI (other than remo data backup capability (i.e., colled or removable media bioled or removable media bioled or removable media biolegical periodical periodical biolegical periodical biolegical periodical validated security patches cross to device operating validated security patches travere? nanufacturer-installed and proposed periodical proposed periodical validated	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than unfacturer be installed as performed by service set or network location vice activity? system: Can the device system: Can the device ivirus software? g system or system: Can the to the control of the word? the finactivity (e.g., a sction taken): Can the	secure (i.e., cannot remedia such as tape, an internal drive or mon the device? on the device? sector via natwork or a (e.g., specific IP a commercial properties of via the commercial properties of via local root or a subto logoff)? a sudit log record	features?	es No N/A	Note
5. 6. PHY 7. 8. 9. TEC 10. 11. 12. 13. 14. 15.	Does manufar What underly VSICAL SAFE(SAFE) Are all device Does the device Can the device Can the device Can the device a. Can the device a. Can the the Can the device a. Can the the Can the device a. Can the Can t	turer offer operation may operating system JARDS components maintage components maintage to boot from uncontrol SIARDS or hardware not auto device restrict remo- device restrict remo- device restrict remo- device restrict remo- device restrict remo- vice manufacturer- vice manufacturer- vice manufacturer- vice manufacturer- vice manufacturer- sirius definitions on a control to ministrative privile ce support user/ope de di ne device audit ic di opout by users/or of ePHI? modification or de export or transmittal modification or de export or transmittal en incorporate en er en en er en incorporate en er en er en en er en er e	n(s) (including version nur tining ePHI (other than remo data backup capability (i.e., oilled or removable media bioled or removable media bioled or removable media biolegical periodical periodical biolegical periodical biolegical periodical	wher) are used by the vable media) physically ,, backup onto removable (i.e., a source other than unfacturer be installed as performed by service ge es or network location vice activity vice activity motely? system: Can the devic livirus software? g system or a system or a g system	secure (i.e., cannot r media such as tape, a an internal drive or m on the device? estoo via network or estoo via network or es (e.g., specific IP a cower/operator m via local root or a sub logoff)? audit log record	features? Yx emove without tools j lisk!? yx emory component)? yx emote connection)? ddriesses)? dmin account)? dmin account)? use?	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11. 12. 13. 14. 15.	Does manufar What underly "SICAL SAFEGI Are all device Does the devi Con the device." Can the device according to the control of the control	turer offer operation may operating system IARDS. Components maintace have an integral of the boot from uncontrol of the boot fr	n(s) (including version nur ining ePHI (other than reme data backup capability (i.e. collide or removable media thorized by the device mar left (i.e., maintenance activitie to a collide or removable es access to specific device in sudit trail of remote-set or software be installed ret coses to device operation prediction of the collider of the collider of the collider prediction of the collider prediction of ePHI? (receipt of ePHI	wher) are used by the vable media) physically ,, backup onto removable (i.e., a source other than unfacturer be installed as performed by service ge es or network location vice activity vice activity motely? system: Can the devic livirus software? g system or a system or a g system	secure (i.e., cannot r media such as tape, a an internal drive or m on the device? estoo via network or estoo via network or es (e.g., specific IP a cower/operator m via local root or a sub logoff)? audit log record	features? Yx emove without tools j lisk!? yx emory component)? yx emote connection)? ddriesses)? dmin account)? dmin account)? use?	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11. 12. 13. 14. 15. 16. 17.	Does manufar What underly VISICAL SAFEG Are all device Does the devi Can the devic Can software Can the devic Can software Can the devic Can software Can the	turer offer operator no operator no operator system JARDS components maintace con have an integral as boot from uncontrol of the control of	n(s) (including version nur ining ePHI (other than remo data backup capability (i.e. collide or removable media thorized by the device mar left (i.e., maintenance activitie es access to specific device in sudit trail of remote-set es access to specific device in sudit trail of remote-set ansulated searchy patches: fribure? "Interest of the properties of persions of the properties of persions of (i.e., user, date/time, a perstors? "etcon of ePHI?" "receipt of ePHI?" "receipt of ePHI?" "receipt of ePHI?" "receipt of ePHI?" "receipt of ePHI?" "receipt of ePHI?" "well the persions of perstors? "" "" "" "" "" "" "" "" "" "	mber) are used by the vable media) physically , backup onto removable (i.e., a source other than hufacturer be installed as performed by service a sor network location vice activity? modelly? vivirus software? vivi	secure (Le., cannot media such as tape, c an internal drive or m on the device?	reatures? senove without tools) listel? senove component?? Yu senove component?? direction)? directions directions	es No N/A	Note
5. 6. PHO 7. 8. 9. TEC 10. 11. 12. 13. 14. 15.	Does manufar What underly Can the devic Children Can the devic Controls when Can the devic	turer offer operation may operating system IARDS components maintage components maintage be boot from uncontrol SIARDS or hardware not automated device restrict remote device restrict remote device restrict remote from the control from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from the from from the from from the from from the from from the fr	n(s) (including version nur tining ePHI (other than remo data backup capability (i.e., oiled or removable media bhorized by the device man by (i.e., maintenne exhibits the access to specific device by (i.e., maintenne exhibits the access to device operating validated security patches inthered in the properties of the pro- vious of the pro- perations of the pro- perations of the pro- perations of the pro- perations of the pro- tion of ePHI? (inception of ePHI? (inception of ePHI? (inception of ePHI? (inception of ePHI? (inception of ePHI) (inception of ePHI) (inception of ePHI) (inception of ePHI) (i	mber) are used by the vable media) physically ,, backup onto removable (i.e., a source other than surfacturer be installed as performed by service vice activity. modely? invited by system or graystem or graystem or graystem or population popula	secure (i.e., cannot redistrict such as tape, an internal drive or m on the device?	features?	es No N/A	Note

ACCE – the American Cone MDS² v 1.0 (2004-11-01)

Side 1

⁶ 2004, HIMSS. All rights reserved.

Proposed Updated MDS2 Form



N	Manufacturer Dis	sclosure Statement	for Medica	al Device Security – I	MDS ²	
		SECTION 1 - DEVI	CE DESCRI	PTION		
Device Category		Manufacturer		Document ID	Document Release Date	e
Device Model		Software Revision		Software Release Date		
/anufacturer or	Company Name		Manu	facturer Contact Information		
Representative Contact nformation:	Representative Nam	e/Position				
	nit or maintain electroni		56		[res], [No [n/s] or [see note	3
			er)?			
				fication number)?		
				entifying characteristics)?		- 0=
d. Open, unstructured	text entered by device	user/operator?				
3. Maintaining ePHI - Car						
a. Maintain ePHI temp	orarily in volatile memo	ry (i.e., until cleared on by p	ower-off or resi	et)?		- 8
 b. Store ePHI persister 	ntly on local media?					
						- 2
		ng/exporting of ePHI – Can				
						Re-
				e, CF/SD card, memory stick	20	
				3, serial port, USB, FireWire)	CONTRACTOR OF THE PROPERTY OF	-
				net)?	11,19,19,19,19,19,19	-
	HI via an integrated wir	eless connection (e.g. WIFI,	Bluetooth, infra	ared)?		- % <u>-</u>
g. Other?		ALLON AND AND AND AND AND AND ADDRESS OF THE PARTY OF THE				-
Can the device maintain	n ePHI during power se	rvice Interruptions?				128
Additional notes regarding r	management of electron	nic Protected Health Informa	ition (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 <u>dseymour@ellumen.com</u> (419) 205-1619