IMPAX

Version 6.5.2
March 1, 2012

Issued by:
Agfa HealthCare
Septestraat 27
B-2640 Mortsel
Belgium

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of the members of the National Electrical Manufacturers Association (NEMA) who were engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEITHER HEALTH INFORMATION MANAGEMENT SYSTEMS SOCIETY (HIMSS) NOR NEMA HAVE POWER, NOR DO THEY UNDERTAKE TO POLICE OR ENFORCE COMPLIANCE WITH THE CONTENTS OF THIS DOCUMENT. NEITHER HIMSS NOR NEMA CERTIFY, TEST, OR INSPECT PRODUCTS, DESIGNS, OR INSTALLATIONS FOR SAFETY OR HEALTH PURPOSES. ANY CERTIFICATION OR OTHER STATEMENT OF COMPLIANCE WITH ANY HEALTH OR SAFETY–RELATED INFORMATION IN THIS DOCUMENT SHALL NOT BE ATTRIBUTABLE TO HIMSS OR NEMA AND IS SOLELY THE RESPONSIBILITY OF THE CERTIFIER OR MAKER OF THE STATEMENT.

Manufacturer Disclosure Statement for Device Security

FOREWORD

This document consists of the Manufacturer Disclosure Statement for Device Security (MDS^2 form). The intent of the MDS^2 form is to supply healthcare providers with important information to assist them in assessing the VULNERABILITY and risks associated with protecting ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) transmitted or maintained by devices. Because security risk assessment spans an entire organization, this document focuses on only those elements of the security risk assessment process associated with devices and systems that maintain or transmit ePHI.

The MDS^2 form should:

(1) Be useful to healthcare provider organizations worldwide. While the form does supply information important to providers who must comply with HIPAA privacy and security rules, the information presented may be useful for any healthcare provider who aspires to have an effective information security RISK MANAGEMENT program. Outside the US, providers would therefore find the MDS^2 form an effective tool to address regional regulations such as EU 95/46 (Europe), Act on the Protection of Personal Information (Act No. 57 of 2003, Japan), and PIPEDA (Canada).

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

(3) Provide a simple, flexible way of collecting the technical, device-specific elements of the common/typical information needed by provider organizations (device users/operators) to begin device information security (i.e., confidentiality, integrity, availability) risk assessments.

(4) HIMSS and NEMA grant permission to make copies and use this form.

Using the information in the MDS^2 form together with information collected about the care delivery environment (e.g., through tools like ACCE / ECRI's Guide for Information Security for Biomedical Technology), the provider's multidisciplinary risk assessment team can review assembled information and make informed decisions on implementing a local security management plan.

Section 1
INSTRUCTIONS FOR OBTAINING AND USING THE MDS^2 FORM

1.1 USING THE MDS^2 FORM (HEALTHCARE PROVIDERS)

1.1.1 Section 1 – Questions 1-19

Section 1 of the MDS^2 form contains information on the type of data maintained / transmitted by the device, how the data is maintained / transmitted, and other security-related features incorporated in the device, as appropriate. The field "Other Security Considerations" allows the manufacturer to add some general security considerations.

PLEASE BE ADVISED—An indication of a device's ability to perform any listed function (i.e., a "Yes" answer) is not an implicit or explicit endorsement or authorization by the manufacturer to configure the device or cause the device to perform those listed functions.

It is important to distinguish between capability and permission. The questions contained on the MDS^2 form refer to device capability. Permission is a contractual matter separate from the MDS^2 form and is not covered by the MDS^2 form. Making changes to a device without explicit manufacturer authorization may have significant contractual, regulatory and liability issues.

1.1.2 Section 2 – Explanatory notes

The optional section 2 of the MDS^2 form contains space for explanatory notes if the manufacturer needs more space to explain specific details to the answers on questions 1-19.

NOTE—Agfa HealthCare may elect to attach supplementary material if additional space for recommended practices or explanatory notes is necessary.

1.2 THE ROLE OF HEALTHCARE PROVIDERS IN THE SECURITY MANAGEMENT PROCESS

It is the obligation of the users of the MDS^2 form (e.g., the healthcare provider) to employ all necessary and appropriate safeguards to meet their regulatory and organizational requirements. The MDS^2 document is intended to assist healthcare providers in meeting their regulatory obligations regarding device security. The healthcare provider organization (e.g., a hospital) has the ultimate responsibility for providing effective security management. Agfa HealthCare can assist providers in their security management programs by offering information describing:

- the type of data maintained / transmitted by the manufacturer's product;
- how data is maintained / transmitted by the manufacturer's product;
- any security–related features incorporated in the manufacturer's product.

In order to effectively manage medical information security and comply with relevant regulations, healthcare providers must employ ADMINISTRATIVE, PHYSICAL and TECHNICAL SAFEGUARDS—most of which are extrinsic to the actual device

1.3 DEFINITIONS

Administrative Safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic Protected Health Information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. [45 CFR Part 164]

Anti-Virus Software: See VIRUS SCANNER

Audit trail: Data collected and potentially used to facilitate a security audit [45 CFR Part 142]

Biometric ID: A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, handwritten signature). [45 CFR Part 142]

Electronic Media: (1) Electronic storage media, including memory devices in computers (hard drives) and any removable/transportable digital memory media, such as magnetic tapes or disks, optical disks, or digital memory cards. (2) Transmission media used to exchange information already in electronic storage media, including, for example, the Internet (wide open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, and private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile and of voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission. [45 CFR Part 160.103]

Electronic Protected Health Information (ePHI): individually identifiable health information (IIHI) that is (1) transmitted by or (2) maintained in electronic media. [45 CFR Part 160.103]

Individually Identifiable Health Information (IIHI): Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. [45 CFR Part 160.103].

Personal Identification Number (PIN): A number or code assigned to an individual and used to provide verification of identity. [45 CFR Part 142]

Physical Safeguards: The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. [45 CFR Part 164]

Remote Service: A support service (e.g., testing, diagnostics, software upgrades) while not physically or directly connected to the device (e.g., remote access via modem, network, Internet).

Removable Media: See ELECTRONIC MEDIA

Security Risk Analysis: Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the integrity, availability, and confidentiality of electronic protected health information. [45 CFR Part 164]

Security Risk Management: (1) The ongoing process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. [NIST SP 800-26] (2) Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. [45 CFR Part 164]

Technical Safeguards: The technology, policies, and procedures to protect electronic Protected Health Information and control access to it. [45 CFR Part 164]

Token: A physical authentication device that the user carries (e.g., smartcard, SecureID^{tm}, etc.). Often combined with a PIN to provide a two-factor authentication method that is generally thought of as superior to simple password authentication.

Virus: In general, computer code that is either:

(1) A type of programmed threat—a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

(2) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs; in addition to propagation, the virus usually performs some unwanted function. [45 CFR Part 164]

Virus scanner: A computer program ("ANTI-VIRUS SOFTWARE") that detects a VIRUS computer program, or other kind of malware (e.g., worms and Trojans), warns of its presence, and attempts to prevent it from affecting the protected computer. Malware often results in undesired side effects generally unanticipated by the user.)

Vulnerability: A flaw or weakness in system procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [NIST SP 800-30]

ARCRONYMS

CD: Compact Disk

CF:	Compact Flash
DVD:	Digital Versatile Disk
IP:	Internet Protocol
LAN:	Local Area Network
ROM:	Read Only Memory
SD:	Secure Digital
USB:	Universal Serial Bus
VPN:	Virtual Private Network
WAN:	Wide Area Network
WiFi:	Wireless Fidelity

Manufacturer Disclosure Statement for Device Security

Section 2
MDS^2 FORM

IMPAX
Version 6.5.2

Manufacturer Disclosure Statement for Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS[2]

Device Category † Medical device software	Manufacturer † Agfa HealthCare	Document ID Livelink ID: 35920926	Document Release Date February 8, 2012
Device Model IMPAX	Software Revision 6.5	Software Release Date 6.5.2 November 16, 2011	

Manufacturer or Representative Contact Information:	Name Chris Townend	Title Snr. Solution Manager	Waterloo Research and Development
	Company Name Agfa HealthCare	Telephone # 519 746 6210 x3225	e-mail christopher.townend@agfa.com

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)?	Yes___	_____
2. Types of ePHI data elements that can be maintained by the device:		
a. Demographic (e.g., name, address, location, unique identification number)?	Yes___	_____
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	Yes___	_____
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes___	_____
d. Open, unstructured text entered by device user/operator?	Yes___	_____
3. Maintaining ePHI: *Can the device*		
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?	Yes___	_____
b. Store ePHI persistently on local media?	Yes___	_____
c. Import/export ePHI with other systems?	Yes___	_____
4. Mechanisms used for the transmitting, importing/exporting of ePHI: *Can the device*		
a. Display ePHI (e.g., video display)?	Yes___	_____
b. Generate hardcopy reports or images containing ePHI?	Yes___	_____
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?	Yes___	_____
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	Yes___	_____
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?	Yes___	_____
f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?	Yes___	1
g. Other _____ ?	_____	_____

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	Yes___	_____
6. What underlying operating system(s) (including version number) are used by the device? Windows/Solaris		

Client: Windows 7 SP1 64 bit Professional and Ultimate, Windows XP (x86) Professional SP3

Application Server: Windows Server 2008 SP2 Standard or Enterprise Edition, Windows Server 2003 R2 SP2, Standard or Enterprise Edition

IMPAX Server: Windows Server 2008 SP2 (x86, x64) Standard or Enterprise Edition, Windows Server 2003 (x86, x64) R2 SP2 Standard or Enterprise Edition, Solaris 10u9 or later

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)?	Yes _	_____
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?	Yes___	_____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No ___	_____

TECHNICAL SAFEGUARDS	Yes No N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device?	Yes___	2 _____
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	Yes___	_____
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	Yes___	_____
b. Can the device log provide an audit trail of remote-service activity?	Yes___	_____
c. Can security patches or other software be installed remotely?	Yes___	_____

Manufacturer Disclosure Statement for Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS[2]

12.	Level of owner/operator service access to device operating system: *Can the device owner/operator*		
	a. Apply device manufacturer-validated security patches?	Yes___	_____
	b. Install or update antivirus software?	Yes___	_____
	c. Update virus definitions on manufacturer-installed antivirus software?	Yes___	_____
	d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)?	Yes___	_____
13.	Does the device support user/operator specific ID *and* password?	Yes___	_____
14.	Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?	Yes___	_____
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?	Yes___	_____
	b. Viewing of ePHI?	Yes___	_____
	c. Creation, modification or deletion of ePHI?	Yes___	_____
	d. Import/export or transmittal/receipt of ePHI?	Yes___	_____
16.	Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use?	Yes___	_____
17.	Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?	Yes___	_____
18.	Controls when exchanging ePHI with other devices:		
	a. Transmitted only via a physically secure connection (e.g., dedicated cable)?	No ___	_____
	b. Encrypted prior to transmission via a network or removable media?	Yes___	_____
	c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?	Optional	_____
19.	Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?	Yes___	_____

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

AGFA HealthCare

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

2.1.1 RECOMMENDED SECURITY PRACTICES

Introduction

This is a cumulative effort based on past experience with earlier previous systems, Security Seminars and direct input from Military sites.

System Hardening

- Verify System Operation - Prior to Hardening
- Backup Procedure - Prior to Hardening
- Procedure – For Back out Purposes Only
- Database Hardening Procedures
- Manually complete remaining lockdown of script tasks
- Operating System Hardening Procedure
- Internet Information Server Hardening Procedure

PASSWORD MANAGEMENT

- Password protect the classes/admin directory
- Update Web services, system and user account passwords

ACCESS CONTROL

- Configure to auto logoff user
- Configure access to confidential information (VIP Studies via Confidentiality Code)
- Configure Web services for encryption

Manufacturer Disclosure Statement for Device Security

SECTION 2

EXPLANATORY NOTES (from questions 1 – 19)
IMPORTANT: Refer to Section 1.2.2 of the Instructions for this form for the proper interpretation of information requested in this form).

1. Communication between IMPAX Client and Server can be wireless. Receiving and transmitting data wirelessly is possible if enabled by the hardware… however, it is not a standard configuration.
2. Software can be installed on client workstations. No other software is allowed to be installed on servers.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.