Artwork and Signature File for:

MAN-03239, "MDS^2 Sheet for Aegis"

Artwork consists of:

- Three (3) 8 ½ inch x 11 inch pages.

REV AUTHORED BY	DATE
S.RAO	9/24/2012
REV DRAFTED BY	DATE
S.RAO	9/24/2012

HOLOGIC™ TORONTO, ON

SIGNATURES ON FILE

TITLE	DOCUMENT NUMBER	REV
MDS^2 Sheet for Aegis	AW-08834	001
ARTWORK	SIZE A	SHEET 1 OF 1

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	Hologic Inc.	MAN-03239 Rev 001	

Device Model	Aegis	Software Revision	3.2	Software Release Date	Jun-12

Manufacturer or Representative Contact Information:	Company Name	Hologic Inc.	Manufacturer Contact Information
	Representative Name/Position	Sachin Rao	sachin.rao@hologic.com

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	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)?	No	1
g. Other? _____	N/A	

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	Yes	2
6. What underlying operating system(s) (including version number) are used by the device? Win Serv.2008 R2 64b / Win 7 64b....		

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 like tape, disk)?	No	3
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 without the use of tools?	yes	
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 provide an audit trail of remote-service activity?	Yes	
c. Can security patches or other software be installed remotely?	Yes	
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	4
c. Update virus definitions on manufacturer-installed antivirus software?	Yes	5
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 username and password?	Yes	
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?	No	6

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	Hologic Inc.	MAN-03239 Rev 001	

Device Model	Aegis	Software Revision	3.2	Software Release Date	Jun-12

Manufacturer or Representative Contact Information:	Company Name	Hologic Inc.	Manufacturer Contact Information
	Representative Name/Position	Sachin Rao	sachin.rao@hologic.com

15. Events recorded in device audit trail (e.g., user, date/time, action taken): Can the audit trail record.....		
a. Login and logout by users/operators?.....	Yes	_____
b. Viewing of ePHI?.....	Yes	_____
c. Creation, modification or deletion of ePHI?.....	No	_____
d. Import/export or transmittal/receipt of ePHI?.....	No	_____
16. Does the device incorporate an emergency access (“break-glass”) feature that is logged?.....	Yes	_____
17. Can the device maintain ePHI during power service interruptions?.....	Yes	7
18. Controls when exchanging ePHI with other devices:.....		
a. Transmitted only via a point-to-point dedicated cable?.....	Yes	8
b. Encrypted prior to transmission via a network or removable media?.....	No	_____
c. Restricted to a fixed list of network destinations.....	Yes	_____
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?.....	Yes	_____

Other Security Considerations

Please review Hologic Enterprise Cybersecurity best practices guide for more inforamtion on some good strategies on how to protect your medical systems at:
http://www.hologic.com/data/ProductSupport/DigitalMammo/Selenia/CyberSecurity/AW-00966_005_01%5B1%5D.pdf

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	Hologic Inc.	MAN-03239 Rev 001	

Device Model	Aegis	Software Revision	3.2	Software Release Date	Jun-12

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information:	Hologic Inc.	
	Representative Name/Position: Sachin Rao	sachin.rao@hologic.com

SECTION 2

EXPLANATORY NOTES (from questions 1 - 19)

IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form

1. Aegis can be setup to transmit ePHI data to the web client over a wireless connection. However, this is not standard configuration.

2. Hologic provides operator and technical training for Aegis on customer request.
   Training for configuration/operational guidelines includes creation of user/admin accounts.

3. Data is stored on the server configured with RAID disks. The system is not to be used as a persistent data store.

4. Only Hologic validated Antivirus software may be used on this medical device.

5. It is the customer's responsibility to obtain the Antivirus software and license. It is not included with the device system configuration.

6. Planned for future release, reference Trac #8745.

7. ePHI is stored locally on the server and is maintained during power and service interruptions.

8. ePHI transmitted using dicom standard only to devices that are configured on the host server.