Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category		Manufacturer		Document ID	Document Release Date
		Hologic		MAN-01404 REV 002	Mar-13
Device Model	Cenova	Software Revision	ALL	Software Release Date	N/A

Manufacturer or Representative Contact Information:	Company Name	Hologic	Manufacturer Contact Information
	Representative Name/Position		Joseph.Zatkovich@hologic.com
	Joseph Zatkovich, Security Systems Engineer		

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?.................................	NO	_____
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	_____
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? Microsoft OS..............	_____	1

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)?..........	YES	_____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	YES	2

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)?..........	NO	_____
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	_____
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 username and password?........................	YES	_____
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?..........	YES/NO	3

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category		Manufacturer		Document ID	Document Release Date
		Hologic		MAN-01404 REV 002	Mar-13
Device Model	Cenova	Software Revision	ALL	Software Release Date	N/A

Manufacturer or Representative Contact Information:	Company Name Hologic	Manufacturer Contact Information
	Representative Name/Position	Joseph.Zatkovich@hologic.com
	Joseph Zatkovich, Security Systems Engineer	

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?..	N/A	_____
d. Import/export or transmittal/receipt of ePHI?..	YES	_____
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	_____
18. Controls when exchanging ePHI with other devices:..		
a. Transmitted only via a point-to-point dedicated cable?..	NO	_____
b. Encrypted prior to transmission via a network or removable media?..	NO	_____
c. Restricted to a fixed list of network destinations...	NO	_____
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 information on some good strategies on how to protect your medical systems at:

http://www.hologic.com/en/product-support/cad-film-digitizers/digital-cad/

Manufacturer Disclosure Statement for Medical Device Security – MDS²				
SECTION 1				

Device Category		Manufacturer	Document ID	Document Release Date
		Hologic	MAN-01404 REV 002	Mar-13
Device Model	Cenova	Software Revision ALL	Software Release Date	N/A

Manufacturer or Representative Contact Information:	Company Name Hologic	Manufacturer Contact Information
	Representative Name/Position	Joseph.Zatkovich@hologic.com
	Joseph Zatkovich, Security Systems Engineer	

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. The Cenova family of products is based upon Microsoft Platforms such as Windows XP and Windows 7.
2. Cenova, by default, boots from the internal harddisk. However, you can change the BIOS boot order and boot from a CD.
3. Cenova, by default, does have session locking but does not have auto logoff.