

**Artwork and Signature File for:**

**MAN-01404, "MDS<sup>2</sup> Sheet for Cenova"**

Artwork consists of:

- Two (2) 8 ½ inch x 11 inch pages.

REV AUTHORED BY	DATE	<b>HOLOGIC™</b>	SANTA CLARA, CA	<del>SIGNATURES ON FILE</del>
W. TANG	4/30/2009			
REV DRAFTED BY	DATE	TITLE	DOCUMENT NUMBER	REV
W. TANG	4/30/2009			
PROPRIETARY INFORMATION: The content of this document is the exclusive property of Lorad and may not, without prior written permission of Lorad, be reproduced, copied or used for any purpose whatsoever.				
		ARTWORK	SIZE A	SHEET 1 OF 1

**Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>**

**SECTION 1**

Device Category	Manufacturer	Document ID	Document Release Date
	Hologic	MAN-01404 REV 001	
Device Model	Software Revision	Software Release Date	
	Cenova	1.0, 1.1, 1.2, 1.3	N/A
Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information	
	Hologic	Brian.Matuska@hologic.com	
	Representative Name/Position		
	Brian Matuska, Manager Santa Clara Software Eng.		

<u>MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)</u>	<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Note #</u>
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? .....				___

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

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

<u>TECHNICAL SAFEGUARDS</u>	<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Note #</u>
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 – MDS<sup>2</sup>**

**SECTION 1**

Device Category	Manufacturer Hologic	Document ID MAN-01404 REV 001	Document Release Date
Device Model Cenova	Software Revision 1.0, 1.1, 1.2, 1.3	Software Release Date	N/A
Manufacturer or Representative Contact Information:	Company Name Hologic Representative Name/Position Brian Matuska, Manager Santa Clara Software Eng.	Manufacturer Contact Information Brian.Matuska@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?..... 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/cc/productsecurity.htm>

**Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>**

**SECTION 1**

Device Category	Manufacturer Hologic	Document ID MAN-01404 REV 001	Document Release Date
Device Model Cenova	Software Revision 1.0, 1.1, 1.2, 1.3	Software Release Date	N/A
Manufacturer or Representative Contact Information:	Company Name Hologic	Manufacturer Contact Information	
	Representative Name/Position Brian Matuska, Manager Santa Clara Software Eng.	Brian.Matuska@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. The Cenova family of products is based upon Microsoft Platform Windows XP.
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.