

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Type 2 Medical	Hologic	MAN-00689 REV.002	Apr-09
Device Model	Software Revision	Software Release Date	
Selenia/Selenia S	3.x	N/A	
Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information	
	Hologic	Wayne.Tang@Hologic.com	
	Representative Name/Position		
	Wayne Tang, Security Systems Specialist		

<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:	Yes			_____
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	Yes			_____
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	Yes			_____
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)?.....	No			_____
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? Solaris 8/10.....				_____

<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)?.....	No			_____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No			_____

<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?.....	No			_____
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			1
b. Can the device provide an audit trail of remote-service activity?.....	Yes			_____
c. Can security patches or other software be installed remotely?.....	No			2
12. Level of owner/operator service access to device operating system: Can the device owner/operator	Yes			_____
a. Apply device manufacturer-validated security patches?.....	Yes			_____
b. Install or update antivirus software?.....	No			3
c. Update virus definitions on manufacturer-installed antivirus software?.....	No			3
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?.....	No			_____
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			_____

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Type 2 Medical	Hologic	MAN-00689 REV.002	Apr-09
Device Model	Software Revision	Software Release Date	
Selenia/Selenia S	3.x	N/A	
Manufacturer or Representative Contact Information:	Company Name Representative Name/Position Wayne Tang, Security Systems Specialist	Manufacturer Contact Information Wayne.Tang@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?..... Yes _____
 - 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 4
 - c. Restricted to a fixed list of network destinations..... No 1
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 – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Type 2 Medical	Hologic	MAN-00689 REV.002	Apr-09
Device Model	Software Revision	Software Release Date	
Selenia/Selenia S			
Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information	
	Representative Name/Position	Wayne.Tang@Hologic.com	
	Wayne Tang, Security Systems Specialist		

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. This restrictive control mechanism will have to be extrinsic from the medical device via a firewall, VLAN, or some other network control mechanism. This is a feature implement by the customer information security department.
2. For security, performance, and reliability reason any software installation or update has to be installed by Hologic Field Engineer locally onsite.
3. Selenia is based on Solaris OS and we have hardened it to greatly minimize against malware attacks. Malware attacks exploiting vulnerabilities within Microsoft platform is impervious against Solaris. Antivirus software is not supported as it is not necessary on Selenia system.
4. All ePHI data exchange between devices is done in DICOM standard which by default isn't encrypted.