Manufacturer Disclosure Statement for Medical Device Security – MDS^2

Device Category:* 15949 Device Model: DRYVIEW 5950 Laser Imaging System	Manufacturer:* Carestream Health, Inc. Software Revision: 1.x	Document ID: 9J5578 Software Release Date: December 2012	Document Release Date: 01/26/2018
Manufacturer or Representative Contact Information:	Name: Technical Support Company Name: Carestream Health, Inc.	Title: N/A U.S.A. Telephone #: 1-800-328-2910	Department: US&C Service

	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?	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	8
	b. Store ePHI persistently on local media?	Yes	8
	c. Import/export ePHI with other systems?	Yes	1
4	Mechanisms used for the transmitting, importing/exporting of ePHI: *Can the device*		
	a. Display ePHI (e.g., video display)?	No	
	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)?	No	
	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?	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	
6	What underlying operating system(s) (including version number) are used by the device?	Microsoft Windows XP Embedded SP3 / Windows Embedded Standard 2009 7	

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

	TECHNICAL SAFEGUARDS	Yes No N/A	Note #
10	Can software or hardware not authorized by the device manufacturer be installed on the device?	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	
	b. Can the device log provide an audit trail of remote-service activity?	Yes	2
	c. Can security patches or other software be installed remotely?	Yes	3
12	Level of owner/operator service access to device operating system: *Can the device owner/operator*		
	a. Apply device manufacturer-validated security patches?	Yes	6
	b. Install or update antivirus software?	No	4
	c. Update virus definitions on manufacturer-installed antivirus software?	No	4
	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 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?	No	
	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 logs each instance of use?	No	
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?	No	5
	c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?	No	
19	Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?	No	

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

RECOMMENDED SECURITY PRACTICES

Below Recommendations are included in the product User Manual:

Network Requirements
The purpose of connection to an external network is for reception of DICOM image/data.
The intended information flow is the DICOM image from modality to printer, and the intended routing is based on local area network that supports DICOM protocol.
The external network shall be 10/100Base-T or 1000Base-T Ethernet network, providing DICOM print service based on DICOM protocol as a DICOM printer.

To ensure network security, a network firewall shall be utilized and kept up to date, and the network integrator shall ensure that only the necessary network ports are opened for remote access.

Caution
Connection of the equipment to an external network that includes other equipment could result in previously unidentified risks to patients, operators, or third parties.
The person responsible for the maintenance of this equipment shall identify, analyze, evaluate and control these risks according to IEC 80001-1:2010.
After the initial installation, subsequent changes to the network to which this equipment is connected could introduce new risks and require additional analysis. Typical changes may include but are not limited to:
- Changes in the network configuration
- Connection of additional items to the network
- Disconnection of items from the network
- Update or upgrade of equipment connected to the network

EXPLANATORY NOTES *(from questions 1 – 19):*
IMPORTANT: Refer to Instructions for the Manufacturers Disclosure Statement for Medical Device Security for the proper interpretation of information provided in this form.

1. When Remote Service Management (RMS) is activated the hard drive of the device (where ePHI is stored) can be accessed remotely. Only qualified service personnel from Carestream Health Inc. have this kind of access.

2. The log will be lost if the machine is re-ghosted.

3. Certain software patches can be downloaded through RMS and installed. This can only be done by qualified Carestream Health Inc. service personnel.

4. The system is protected from malicious attack by utilizing the Microsoft firewall to block/disable all ports not needed for DICOM printing or secure remote access. Applicable MICROSOFT Windows Embedded Security Patches are incorporated into the software to provide additional protection.

5. All RMS related network communication is encrypted and goes through the Status Link Enterprise Server owned and operated by Carestream Health Inc. in Rochester NY, USA.

6. Carestream Health Inc. authorized service providers must make software updates available on the device before customers can install software updates containing validated security updates.

7. Microsoft Windows XP Embedded SP3 installed in manufacturing on units prior to Serial Number 59539745. Microsoft Windows Embedded Standard 2009 (WES2009) installed on units starting with Serial Number 59539745. Note that imagers with Serial Numbers prior to 59539745 may also have WES2009 if service modification was completed.

8. ePHI stored data files that are obtained from the connected modality are deleted from memory upon the user's print job being completed.

9.

10.

11.

12.

13.

14.

15.

16.

17.

18.

19.

20.

Adapted from Information Security for Biomedical Technology: A HIPAA Compliance Guide, ACCE/ECRI, 2004.
ACCE – the American College of Clinical Engineering: ECRI – formerly the Emergency Care Research Institute.