Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer Carestream	Document ID	Document Release Date 02/2012
Device Model PACS	Software Revision 11.3.x	Software Release Date	06/2011

Manufacturer or Representative Contact Information:	Company Name Carestream Representative Name/Position Tom Rohr Director, WW Corporate Security	Manufacturer Contact Information WW Corporate Security 585 627 8880 hg- carestreamcorpsecurity@carestream.com technical health-imaging-tsc@carestream.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)?	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)?	Yes	_____
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? Windows & Solaris	N/A	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)?	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	2
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	Yes	3
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	N/A	
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	_____

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer Carestream	Document ID	Document Release Date 02/2012
Device Model PACS	Software Revision 11.3.x	Software Release Date 06/2011	

Manufacturer or Representative Contact Information:	Company Name Carestream	Manufacturer Contact Information
	Representative Name/Position Tom Rohr Director, WW Corporate Security	WW Corporate Security 585 627 8880 hg-carestreamcorpsecurity@carestream.com technical health-imaging-tsc@carestream.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?......	N/A	_____
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?......	Yes	4
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	5

Other Security Considerations

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category		Manufacturer Carestream		Document ID	Document Release Date 02/2012	
Device Model	PACS	Software Revision	11.3.x	Software Release Date		06/2011

Manufacturer or Representative Contact Information:	Company Name Carestream	Manufacturer Contact Information WW Corporate Security 585 627 8880 hg-carestreamcorpsecurity@carestream.com technical health-imaging-tsc@carestream.com
	Representative Name/Position Tom Rohr Director, WW Corporate Security	

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

Notes:

1. The PACS server can be installed on either Windows Server R2 2008, or Solaris 10. The clinical application (client) can be installed on Windows 7, Windows XP or Windows Vista.

The Carestream PACS enterprise viewer is hardware agnostic, and can operate on any HTML5 compliant browser. Please note that this software component is 100% web based and does not require a local installation, nor does it save any patient related data on the hosting device.

2. The product is installed on an "of the shelf" server, it is the responsibility of the local IT to prevent unotherized 3rd party softwre components from being installed on the system.

3. Yes, via Carestream's secure & encrypted service network.

4. This capability is configurable.

5. The PACS uses an elaborate patient matching mechanism to minimize patient metadata inconsitencies and errors.