Manufacturer Disclosure Statement for Medical Device Security – MDS^2

Device Category: **16512**	Manufacturer: **Carestream Health, Inc.**	Document ID: **7H4185**	Document Release Date: **7/15/08**
Device Model: **PoC 360,260,140,120**	Software Revision **3.0**	Software Release Date: **7/24/08**	

Manufacturer or Representative Contact Information:	Name **Technical Support**	Title: **N/A**	Department: **US&C Service**
	Company Name: **Carestream Health, Inc.**	Telephone # **1-800-328-2910**	email **health.imaging.tsc@carestreamhealth.com**

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	
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)?†	Yes	
g. Other ________________________________ ?	None	

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?	WinXP SP3 ,Vista Business SP1	

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)?	No	1
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?	Yes	9
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?	Yes	8
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	Yes	2
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	Yes	3
b. Can the device log provide an audit trail of remote-service activity?	Yes	4
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	7
c. Update virus definitions on manufacturer-installed antivirus software?	Yes	7
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 ID *and* password?	Yes	
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?	No	
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?	Yes	
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?	Yes	
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?	No	
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	
c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?	Yes	5
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?	Yes	6

† Recommend use of ECRI's Universal Medical Device Nomenclature System (UMDNS).

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.

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

RECOMMENDED SECURITY PRACTICES

Users must take steps to secure their networks and protect their Medical Information Systems which includes a risk assessment strategy, network defense in depth strategy, business continuity planning, etc.

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. Site's responsibility is to protect the PC equipment. (By locking the PC to the table etc.)
2. Requires the site to be connected to the network and allow remote access.
3. Requires modifications to the Window's OS definitions.
4. System has an internal login user names from service.
5. PHI data is sent to a predefined DICOM targets only.
6. Based on TCP/IP.
7. It is strongly recommended not to install AntiVirus software on the same PC as it may interfere with nominal flow.
8. Only privileged users can reach the desktop and install additional software on the PC.
9. Data can be archived on a DVD/CD.

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.