

Manufacturer Disclosure Statement for Medical Device Security – MDS ²			
SECTION 1			
Device Category	Manufacturer	Document ID	Document Release Date
	Carestream Health, Inc.		7/15/2009
Device Model	Carestream PACS	Software Revision	11.0
		Software Release Date	05/2009
Manufacturer or Representative Contact Information:	Company Name Carestream Health, Inc. Representative Name/Position Technical Support	Manufacturer Contact Information Privacy & Product Security 1-585-627-8880 health.imaging.tsc@carestreamhealth.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)?			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?			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?			Win 2000/2003/XP, Solaris9/10
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)?			N/A
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
TECHNICAL SAFEGUARDS			Yes No N/A Note #
10. Can software/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)?			Yes
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?			N/A
c. Update virus definitions on manufacturer-installed antivirus software?			N/A
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	Document ID	Document Release Date
	Carestream Health, Inc.		7/15/2009
Device Model	Software Revision	Software Release Date	
Carestream PACS	11.0	05/2009	

Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information
	Representative Name/Position	
	Carestream Health, Inc.	Privacy & Product Security 1-585-627-8880 health.imaging.tsc@carestreamhealth.com
	Technical Support	

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?..... Yes
 - b. Encrypted prior to transmission via a network or removable media?..... Yes
 - 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

Other Security Considerations

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.

Manufacturer Disclosure Statement for Medical Device Security – MDS²			
SECTION 1			
Device Category	Manufacturer	Document ID	Document Release Date
	Carestream Health, Inc.		7/15/2009
Device Model	Software Revision	Software Release Date	
Carestream PACS	11.0	05/2009	
Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information	
	Carestream Health, Inc.		
	Representative Name/Position		
	Technical Support	Privacy & Product Security 1-585-627-8880 health.imaging.tsc@carestreamhealth.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			
The customer must configure the system to a secure mode operation to fulfill the above			