Manufacturer Disclosure Statement for Medical Device Security – MDS2

Device Category: 19549  
Device Model: DryView 8900

Manufacturer: CareStream Health Inc.  
Software Revision 3.X

Document ID: 8F5741  
Document Release Date: 07/31/2009

Company Name: Carestream Health Inc.  
Telephone # 1-800-328-2910  
e-mail: health.imaging.tsc@carestreamhealth.com

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) (As defined by HIPAA Security Rule, 45 CFR Part 164)

1. Can this device transmit or maintain electronic Protected Health Information (ePHI)? Yes No N/A Note #
2. Types of ePHI data elements that can be maintained by the device:
   a. Demographic (e.g., name, address, location, unique identification number)? Yes No N/A Note #
   b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? Yes No N/A Note #
   c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? Yes No N/A Note #
   d. Open, unstructured text entered by device user/operator? Yes No N/A Note #

3. Maintaining ePHI: Can the device
   a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)? Yes No N/A Note #
   b. Store ePHI persistently on local media? Yes No N/A Note #
   c. Import/export ePHI with other systems? Yes No N/A Note #

4. Mechanisms used for the transmitting, importing/exporting of ePHI: Can the device
   a. Display ePHI (e.g., video display)? Yes No N/A Note #
   b. Generate hardcopy reports or images containing ePHI? Yes No N/A Note #
   c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)? Yes No N/A Note #
   d. Transmit/receive ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)? Yes No N/A Note #
   e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)? Yes No N/A Note #
   f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)? Yes No N/A Note #
   g. Other ____________

ADMINISTRATIVE SAFEGUARDS

5. Does manufacturer offer operator and technical support training or documentation on device security features? Yes No N/A Note #
6. What underlying operating system(s) (including version number) are used by the device? Microsoft Windows 2000 SP4

PHYSICAL SAFEGUARDS

7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)? Yes No N/A Note #
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? Yes No N/A Note #
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? Yes No N/A Note #

TECHNICAL SAFEGUARDS

10. Can software or hardware not authorized by the device manufacturer be installed on the device? Yes No N/A Note #
11. Can the device be securely operated (i.e., maintenance activities performed by service person via network or remote connection)? Yes No N/A Note #
   a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)? Yes No N/A Note #
   b. Can the device log provide an audit trail of remote-service activity? Yes No N/A Note #
   c. Can security patches or other software be installed remotely? Yes No N/A Note #

12. Level of owner/operator service access to device operating system: Can the device owner/operator
   a. Apply device manufacturer-validated security patches? Yes No N/A Note #
   b. Install or update antivirus software? Yes No N/A Note #
   c. Update virus definitions on manufacturer-installed antivirus software? Yes No N/A Note #
   d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? Yes No N/A Note #

13. Does the device support user/operator specific ID and password? Yes No N/A Note #
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)? Yes No N/A Note #
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 No N/A Note #
   b. Viewing of ePHI? Yes No N/A Note #
   c. Creation, modification or deletion of ePHI? Yes No N/A Note #
   d. Import/export or transmission/receipt of ePHI? Yes No N/A Note #

16. Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use? Yes No N/A Note #
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? Yes No N/A Note #
18. Controls when exchanging ePHI with other devices: Yes No N/A Note #
   a. Transmitted only via a physically secure connection (e.g., dedicated cable)? Yes No N/A Note #
   b. Encrypted prior to transmission via a network or removable media? Yes No N/A Note #
   c. Restricted to a fixed list of network addresses (i.e., host-based access control list)? Yes No N/A Note #
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? Yes No N/A Note #

ACCE – the American College of Clinical Engineering; ECRI – formerly the Emergency Care Research Institute.
Manufacturer Disclosure Statement for Medical Device Security – MDS²

RECOMMENDED SECURITY PRACTICES

EXPLANATORY NOTES (from questions 1 – 20):

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 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 when hard drive is re-ghosted.

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

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

5. The system is protected from malicious attack by disabling all ports not needed for printing or secure remote monitoring. MICROSOFT Security Patches have been incorporated into the software to provide additional protection.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

16.

17.

18.

19.

20.

ACCE – the American College of Clinical Engineering; ECRI – formerly the Emergency Care Research Institute.