**Manufacturer Disclosure Statement for Medical Device Security – MDS²**

**Device Category**: 16512  
**Manufacturer**: Carestream Health, Inc.  
**Device Model**: DirectView DR 3000, DR 3500  
**Software Revision**: 3.0.x, 3.5.x  
**Document ID**: 7H4555  
**Document Release Date**: 2007.10.03

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

---

### MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)

1. **Can this device transmit or maintain electronic Protected Health Information (ePHI)?**
   - Yes **______**  
   - No **______**  
   - N/A

2. **Types of ePHI data elements that can be maintained by the device:**
   - a. Demographic (e.g., name, address, location, unique identification number)? **______**
   - b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? **______**
   - c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? **______**
   - d. Open, unstructured text entered by device user/operator? **______**

3. **Maintaining ePHI:**
   - a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)? **______**
   - b. Store ePHI persistently on local media? **______**
   - c. Import/export ePHI with other systems? **______**

4. **Mechanisms used for the transmitting, importing/exporting of ePHI:**
   - a. Display ePHI (e.g., video display)? **______**
   - b. Generate hardcopy reports or images containing ePHI? **______**
   - c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)? **______**
   - d. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)? **______**
   - e. Transmit/receive ePHI via a dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)? **______**
   - f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)? **______**
   - g. Other? **______**

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

---

### PHYSICAL SAFEGUARDS

5. **Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?**
   - Yes **______**
   - No **______**  
   - N/A

6. **Can the device owner/operator change passwords?**
   - Yes **______**
   - No **______**  
   - N/A

**PHYSICAL SAFEGUARDS**

---

### TECHNICAL SAFEGUARDS

7. **Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?**
   - Yes **______**
   - No **______**  
   - N/A

8. **Can the device perform encrypted prior to transmission via a network or removable media?**
   - Yes **______**
   - No **______**  
   - N/A

9. **Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?**
   - Yes **______**
   - No **______**  
   - N/A

---

### ADMINISTRATIVE SAFEGUARDS

10. **Can software or hardware not authorized by the device manufacturer be installed on the device?**
    - Yes **______**
    - No **______**  
    - N/A

11. **Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?**
    - Yes **______**
    - No **______**  
    - N/A

---

**Technical Support**

---

**Manufacturer Disclosure Statement for Medical Device Security – MDS²**

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

© 2004, HIMSS. All rights reserved.
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. Carestream Health, Inc. provides operator and technical training for the DirectView DR systems at our Dallas, TX facility. Service/technical documentation includes configuration guidelines for a certified service provider to configure the DR system activation of the software firewall services.

2. Valid Digital Certificate is required for service access (e.g. system modification, loading additional software, use of the CD or USB drives, etc.)

3. Access to the CD drive or USB ports would require the individual to open the access door and slide out the CPU. Normal operation of the DR system does not require the use of a keyboard.

4. The clinical user does not have access to the system desktop, limiting access to the Windows Operating System.

5. DR Systems have the capability to complete a backup of configuration data via the floppy drive.

6. DR Systems have boot capability via the CD drive.

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.

MDS$^2$ v 1.0 (2004-11-01) Side 2 © 2004, HIMSS. All rights reserved.