

# Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

Device Category: <b>16512</b>	Manufacturer: <b>Eastman Kodak</b>	Document ID: <b>5H8309</b>	Document Release Date: <b>12/31/2005</b>
Device Model: <b>DirectView DR 5000/5100/7100/9000</b>	Software Revision: <b>2.0</b>	Software Release Date: <b>11/23/05</b>	
Manufacturer or Representative Contact Information:	Name: <b>Technical Support</b>	Title: <b>N/A</b>	Department: <b>US&amp;C Service</b>
	Company Name: <b>Eastman Kodak</b>	Telephone #: <b>1-800-328-2910</b>	e-mail: <b>health.imaging.tsc@kodak.com</b>

**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  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
  - b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? ..... Yes  No  N/A
  - c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? ..... Yes  No  N/A
  - d. Open, unstructured text entered by device user/operator? ..... Yes  No  N/A
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
  - b. Store ePHI persistently on local media? ..... Yes  No  N/A
  - c. Import/export ePHI with other systems? ..... Yes  No  N/A
4. Mechanisms used for the transmitting, importing/exporting of ePHI: *Can the device*
  - a. Display ePHI (e.g., video display)? ..... Yes  No  N/A
  - b. Generate hardcopy reports or images containing ePHI? ..... Yes  No  N/A
  - 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
  - d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)? ... No  Yes  N/A
  - e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)? ..... Yes  No  N/A
  - f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)? ..... No  Yes  N/A
  - 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  No  N/A  Note # 1
6. What underlying operating system(s) (including version number) are used by the device? Microsoft Windows 2000 SP4 \_\_\_\_\_

**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  No  N/A  Note # 2, 3, 4
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 # 5
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 # 6

**TECHNICAL SAFEGUARDS**      **Yes No N/A Note #**

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 serviced remotely (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
  - b. Can the device log provide an audit trail of remote-service activity? ..... Yes  No  N/A
  - c. Can security patches or other software be installed remotely?..... Yes  No  N/A
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
  - b. Install or update antivirus software? ..... No  Yes  N/A
  - c. Update virus definitions on manufacturer-installed antivirus software? ..... No  Yes  N/A
  - d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? .. Yes  No  N/A
13. Does the device support user/operator specific ID *and* password? ..... Yes  No  N/A
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)? ..... Yes  No  N/A
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
  - b. Viewing of ePHI? ..... Yes  No  N/A
  - c. Creation, modification or deletion of ePHI? ..... Yes  No  N/A
  - d. Import/export or transmittal/receipt of ePHI? ..... Yes  No  N/A
16. Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use? ..... No  Yes  N/A
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? ..... Yes  No  N/A
18. Controls when exchanging ePHI with other devices:
  - a. Transmitted only via a physically secure connection (e.g., dedicated cable)? ..... No  Yes  N/A
  - b. Encrypted prior to transmission via a network or removable media? ..... No  Yes  N/A
  - c. Restricted to a fixed list of network addresses (i.e., host-based access control list)? ..... No  Yes  N/A
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? .... Yes  No  N/A

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

## Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

### **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. Kodak Health Group 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; therefore no keyboard is attached to the system
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