Manufacturer Disclosure Statement for Medical Device Security – MDS²

Device Category : **16512**	Manufacturer: **Eastman Kodak**	Document ID: 5H8308	Document Release Date: **12/31/2005**
Device Model: **DirectView CR 500/800/825/850/900/950/975 and ROP**	Software Revision: **4.31**	Software Release Date: **03/21/05**	

Manufacturer or Representative Contact Information:	Name: **Technical Support**	Title: **N/A**	Department: **US&C Service**
	Company Name: **Eastman Kodak**	Telephone #: **1-800-328-2910**	e-mail: **health.imaging.tsc@kodak.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? .... 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)? ... No ____   _____
    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)?............................ No ____   _____
    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 __   __1__
6. What underlying operating system(s) (including version number) are used by the device? <u>Microsoft Windows 2000 SP4</u>   _____   _____

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 _   _2, 3, 4_
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? .... Yes __   __6__
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? Yes __   _7__

TECHNICAL SAFEGUARDS   Yes No N/A   Note

10. Can software or hardware not authorized by the device manufacturer be installed on the device?.............................. 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 log 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? .... No ____   _____
    c. Update virus definitions on manufacturer-installed antivirus software? .... No ____   _____
    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)? .... Yes __   _____
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? .... 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 logs each instance of use? .... No ____   _____
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? .... Yes __   _____
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 __   _____

---

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

Kodak Health Group MDS² v 1.0 – DirectView 500/825/850/900/950/975 & ROP SW v4.31
© **2004, HIMSS MDS² Format**

Manufacturer Disclosure Statement for Medical Device Security – MDS²

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 CR systems at our Dallas, TX facility. Service/technical documentation includes configuration guidelines for a certified service provider to configure the CR 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 CR 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. The system limits transfer of ePHI through defined DICOM associations which requires defined IP addresses and AE Titles
6. CR Systems have the capability to complete a backup of configuration data via the floppy drive
7. CR Systems have boot capability via the CD drive
8.