

Manufacturer Disclosure Statement for Medical Device Security – MDS²

Device Category : 16512	Manufacturer: Eastman Kodak	Document ID: 5H7393	Document Release Date: 11/14/05
Device Model: ACR-2000/2000i Kodak Radiation Oncology Beam Dosimetry SW	Software Revision: 1.0	Software Release Date: 10/14/05	
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)*? No _____
2. Types of ePHI data elements that can be maintained by the device:
 - a. Demographic (e.g., name, address, location, unique identification number)? No _____
 - b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? No _____
 - c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? . Yes 1 _____
 - d. Open, unstructured text entered by device user/operator? No _____
3. Maintaining ePHI: *Can the device*
 - a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)? No _____
 - b. Store ePHI persistently on local media? No _____
 - c. Import/export ePHI with other systems? No _____
4. Mechanisms used for the transmitting, importing/exporting of ePHI: *Can the device*
 - a. Display ePHI (e.g., video display)? No _____
 - b. Generate hardcopy reports or images containing ePHI? No _____
 - c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)? . No 2 _____
 - 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)? No _____
 - 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 _____
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 _____
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? No _____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? No _____

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)? . No _____
 - a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)? No _____
 - b. Can the device log provide an audit trail of remote-service activity? No _____
 - c. Can security patches or other software be installed remotely?..... No _____
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? Yes _____
 - c. Update virus definitions on manufacturer-installed antivirus software? Yes _____
 - 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? No _____
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)? 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? No _____
 - b. Viewing of ePHI? No _____
 - c. Creation, modification or deletion of ePHI? No _____
 - d. Import/export or transmittal/receipt of ePHI? No _____
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? N/A _____
18. Controls when exchanging ePHI with other devices:
 - a. Transmitted only via a physically secure connection (e.g., dedicated cable)? N/A _____
 - b. Encrypted prior to transmission via a network or removable media? N/A _____
 - c. Restricted to a fixed list of network addresses (i.e., host-based access control list)? N/A _____
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? N/A _____

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

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. The DICOM image header of a patient image will contain ePHI (e.g. Patient ID, Patient Last Name, and Field ID), the ePHI cannot be viewed within the software.
2. Only the DICOM image can be imported/exported.