

Manufacturer Disclosure Statement for Medical Device Security – MDS²

Device Category: 16512	Manufacturer: Eastman Kodak	Document ID: 5H7395	Document Release Date: 11/14/05
Device Model: ACR-2000/2000i Kodak Radiation Oncology Software	Software Revision: 6.0	Software Release Date: 08/18/05	
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 ___
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? Yes ___
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? 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? No ___ **1**
18. Controls when exchanging ePHI with other devices:
 - a. Transmitted only via a physically secure connection (e.g., dedicated cable)? Yes ___ **2**
 - b. Encrypted prior to transmission via a network or removable media? Yes ___
 - c. Restricted to a fixed list of network addresses (i.e., host-based access control list)? Yes ___
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).

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. It is recommended that the customers provide their own power backup system. There is no UPS backup system sold at time of sale.
2. When the device is installed on the customer network behind an external firewall, the network can be configured to allow communications only to customer defined DICOM destinations. The application uses TCP/IP for transmission, ability to encrypt the data can be configured by the customers network and is managed by the local switch port, router or firewall.