Manufacturer Disclosure Statement for Medical Device Security – MDS^2

Device Category : 17237	Manufacturer: Eastman Kodak	Document ID:	Document Release Date: **8/1/05**
Device Model: 8800	Software Revision: 5.2	Software Release Date: 09/99	

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? .... No ___ _______
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?.......... No ___ _______
   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)? .... 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 ___ _______
   d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire*)*? ... Yes __ _______
   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 ____ ? .... No ___ _______

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? Proprietary O/S: VRTX 1.1B ______ _______

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? .... No ___ _______
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)? .... N/A __ _______
    b. Can the device log provide an audit trail of remote-service activity? .... No ___ _______
    c. Can security patches or other software be installed remotely?.......... 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? .... N/A __ _______
    b. Install or update antivirus software? .... N/A __ _______
    c. Update virus definitions on manufacturer-installed antivirus software? .... N/A __ _______
    d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? .. No ___ _______
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)? .... No ___ _______
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? .... No ___ _______
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)? .... No ___ _______

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? .... No ___ ______

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

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.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.