Manufacturer Disclosure Statement for Medical Device Security – MDS²

Device Category : **7-175**	Manufacturer: **Eastman Kodak**	Document ID: **5H7385**	Document Release Date: **10/13/2005**
Device Model: **RIS2010**	Software Revision: **8.0**	Software Release Date: **05/2005**	

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)?........................... Yes __ _____
   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? Windows 2003, XP.............. _____ _____

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)? No __ _____
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? .... Yes __ _____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? Yes __ _____

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? .... 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)? .... 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? .... 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? .... No ____ _____

© **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's Health Group provides operator and system administration training for the KODAK RIS 2010 product. This training, along with associated User Guides, covers security features.
2. A speech mic that is used for integrated digital dictation is connected to the local workstation via local USB port.
3. RIS2010 applications are installed on existing hardware (customer purchased).
4. The RIS2010 features a robust Audit Trail that will log all PHI-related activities.
5.

Glossary

Term	Definition
Access	Read, write, modify, or transmit/receive data or otherwise make use of any system resource *[45 CFR Part 164]*
Administrative Safeguards	Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic Protected Health Information and to manage the conduct of the covered entity's workforce in relation to the protection of that information *[45 CFR Part 164]*
Anti-Virus Software	See *Virus Checking*
Archive	Store (data) for extended period of time (e.g., years)
Audit Trail	Data collected and potentially used to facilitate a security audit *[45 CFR Part 142]*
Availability	The property that data or information is accessible and usable on demand by an authorized person *[45 CFR Part 164]*
Biometric ID	A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, handwritten signature) *[45 CFR Part 142]*
Compact Disk (CD)	Optical storage media
Compact Flash (CF) Card™	Any of a family of solid-state memory cards
Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes *[45 CFR Part 164]*
Digital Versatile Disk (DVD)	Optical storage media

Term	Definition
Electronic Media	(1) Electronic storage media, including memory devices in computers (hard drives) and any removable/transportable digital memory media, such as magnetic tapes or disks, optical disks, or digital memory cards (2) Transmission media used to exchange information already in electronic storage media, including, for example, the Internet (wide open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, and private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile and of voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission *[45 CFR Part 160]*
EPHI	*Individually Identifiable Health Information* that is (1) transmitted or (2) maintained by *electronic media* *[45 CFR Part 160]*
Individually Identifiable Health Information (IIHI)	Any information, including demographic data collected from an *individual*, that (1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and 　　a. identifies the individual, or 　　b. with respect to which there is a reasonable basis to believe that the information can be used to identify the individual *[45 CFR Part 160]*
Integrity	The property that data or information has not been altered or destroyed in an unauthorized manner *[45 CFR Part 164]*
Local Area Network (LAN)	See *Networks*
Memory Stick™	One of a family of solid-state memory cards
Networks	A communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system; examples of networks include local area or wide area networks, including public networks such as the Internet *[NIST SP 800-26]*
Operating System	A collection of computer programs that manages the hardware for other computer applications; examples include Microsoft Windows, Novell Netware, Unix, Linux, Mac OS
Password	Confidential authentication information composed of a string of characters *[45 CFR Part 164]*
PC Card	A standard laptop personal computer device that plugs into a personal computer slot approximately the size of a credit card (formerly known as PCMCIA^{tm} card)
Personal Identification Number (PIN)	A number or code assigned to an individual and used to provide verification of identity *[45 CFR Part 142]*
Physical Safeguards	The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion *[45 CFR Part 164]*
Remote Service	Provide support service (e.g., testing, diagnostics, software upgrades) while not physically or directly connected to the device (e.g., remote access via modem, network, Internet)
Removable Media	See *Electronic Media*
Risk Analysis	Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the integrity, availability, and confidentiality of electronic Protected Health Information *[45 CFR Part 164]*
Risk Management	The ongoing process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk *[NIST SP 800-26]* Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level *[45 CFR Part 164]*
Secure Digital (SD) Card™	One of a family of solid-state memory cards

Term	Definition
Technical Safeguards	The technology, policies, and procedures to protect electronic Protected Health Information and control access to it *[45 CFR Part 164]*
Token	A physical authentication device that the user carries (e.g., smartcard, SecureID™, etc.). Often combined with a PIN to provide a two-factor authentication method that is generally thought of as superior to simple password authentication
Virtual Private Network (VPN)	See *Networks*
Virus	A computer program that is either: (1) A type of programmed threat—a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized *users* (2) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs; in addition to propagation, the virus usually performs some unwanted function *[45 CFR Part 142]*
Virus Checking	A computer program ("anti-virus software") that identifies and disables another "virus" computer program, typically hidden, that attempts to attach itself to other programs and has the ability to replicate (unchecked virus programs result in undesired side effects generally unanticipated by the user) *[45 CFR Part 142]*
Vulnerability	A flaw or weakness in system *procedures*, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's *security policy* *[NIST SP 800-30]*
Wide Area Network (WAN)	See *Networks*