### TECHNICAL SAFEGUARDS

10. Can software or hardware not authorized by the device manufacturer be installed on the device? YES NO N/A
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?
   a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)? YES NO N/A
   b. Can the device log provide an audit trail of remote-service activity? YES NO N/A
   c. Can security patches or other software be installed remotely? YES NO 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? YES NO N/A
   b. Update virus definitions on manufacturer-installed antivirus software? YES NO N/A
   c. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? YES NO N/A
13. Does the device support user/operator specific ID and password? YES NO N/A
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)? YES NO 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 NO N/A
   b. Viewing of ePHI? YES NO N/A
   c. Creation, modification or deletion of ePHI? YES NO N/A
   d. Import/export or transmittal/receipt of ePHI? YES NO N/A
16. Does the device incorporate an emergency access (“break-glass”) feature that logs each instance of use? YES NO N/A
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? YES NO N/A
18. Controls when exchanging ePHI with other devices:
   a. Transmitted only via a physically secure connection (e.g., dedicated cable)? YES NO N/A
   b. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)? YES NO N/A
   c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)? YES NO N/A
   d. Import/export ePHI with other systems? YES NO N/A
   e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)? YES NO N/A
   f. Transmit/receive ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)? YES NO N/A
   g. Other? YES NO N/A

### PHYSICAL SAFEGUARDS

7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)? YES NO N/A
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? YES NO
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? YES NO

### ADMINISTRATIVE SAFEGUARDS

5. Does manufacturer offer operator and technical support training or document on device security features? YES NO N/A
6. What underlying operating system(s) (including version number) are used by the device? Proprietary OS YES NO N/A

---

Kodak Health Group MDS<sup>2</sup> v 1.0 – DryView 8300/8610 © 2004, HIMSS MDS<sup>2</sup> Format.
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.
2.
3. Local Media not supported on 8600 and 8610
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.