### MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Note #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2. Types of ePHI data elements that can be maintained by the device:</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>a. Demographic (e.g., name, address, location, unique identification number)</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>d. Open, unstructured text entered by device user/operator?</td>
<td></td>
<td>No</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### PHYSICAL SAFEGUARDS

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

### TECHNICAL SAFEGUARDS

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Can software or hardware not authorized by the device manufacturer be installed on the device?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>b. Can the device log provide an audit trail of remote-service activity?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>c. Can security patches or other software be installed remotely?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

**Manufacturer Disclosure Statement for Medical Device Security – MDS²**

**Device Category:** 15949  
**Manufacturer:** Eastman Kodak  
**Document ID:** 7F9048  
**Document Release Date:** 8/1/2005

**Device Model:** DryView 8100/8200  
**Software Revision:** 8100 - 2.4.3  
**Software Release Date:** 8100 - 04/04

**Device Category:** 8200 - 3.6  
**Software Revision:** 8200 - 06/04

**Manufacturer or Representative Contact Information:**  
**Name:** Technical Support  
**Title:** N/A  
**Company Name:** Eastman Kodak  
**Telephone #:** 1-800-328-2910  
**Department:** US&C Service  
**e-mail:** health.imaging.tsc@kodak.com

---

The table above includes the following questions and responses related to the security features of the DryView 8100/8200 device:

1. Does the device incorporate an emergency access (“break-glass”) feature that logs each instance of use?  
   - No

2. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?  
   - No

3. Does the device support user/operator specific ID?  
   - N/A

4. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?  
   - No

5. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?  
   - No

6. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?  
   - No

7. Does the device have an audit log that records events related to ePHI?  
   - Yes

8. Does the device incorporate an emergency access (“break-glass”) feature that logs each instance of use?  
   - No

9. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?  
   - No

---

**Kodak Health Group MDS² v 1.0 – DryView 8100/8200**  
© 2004, HIMSS MDS² Format

---

**Administrative Safeguards**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Does manufacturer offer operator and technical support training or documentation on device security features?</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>6. What underlying operating system(s) (including version number) are used by the device? pSOS 2.1.3</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

**Physical Safeguards**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)?</td>
<td></td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?</td>
<td></td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>
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 ___ ______

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).
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.