### MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) As defined by HIPAA Security Rule, 45 CFR Part 164

1. Can this device transmit or maintain electronic Protected Health Information (ePHI)? Yes No N/A Note # 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

5. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? Yes

6. Do access sessions automatically terminate after a predetermined length of inactivity (e.g., auto logoff)? Yes

7. Is the device configured to use an audit log to record access attempts? Yes

8. Can the device admit access only from a fixed list of network addresses (i.e., host-based access control list)? Yes

9. Does the device incorporate an emergency access (“break-glass”) feature that logs each instance of use? Yes

10. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? Yes

11. Does the device maintain ePHI (e.g., by internal battery) during power service interruptions? Yes

12. Does the device incorporate a feature to log each instance of use to an audit log? Yes

13. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? Yes

14. Can the device boot from uncontrolled or removable media (i.e., backup onto removable media such as tape, disk)? Yes

15. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)? Yes

16. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? Yes

17. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? Yes

---

1 Recommendation of ECRi's Universal Medical Device Nomenclature System (UMDNS).


ACCE – the American College of Clinical Engineering; ECRI – formerly the Emergency Care Research Institute.
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. Carestream Health provides operator and technical training for the DirectView DR systems at our Carestream Health facility. Service/technical documentation includes configuration guidelines for a certified service provider to configure the CR system activation of the software firewall services.
2. Valid Digital Certificate is required for service access (e.g. system modification, loading additional software, use of the CD/DVD or USB drives, etc.)
3. The clinical user does not have access to the system desktop, limiting access to the Windows Operating System.
4. DR systems have the capability to complete a backup of configuration data via removable media.
5. DR systems have boot capability via the CD/DVD drive.
6. The product does not include Anti-Virus software. Cisco Security Agent is included in the product.
7. The auto logout feature is provided but can be disabled by the local security administrator.
8. The customer has the option of creating an emergency access user account. This is accomplished by creating a user account and safeguarding the password such that it can be used for emergency situations.
9. The system limits transfer of ePHI through defined DICOM associations, which requires defined IP addresses and AE titles.