### Technical Safeguards

1. **Can this device transmit or maintain electronic Protected Health Information (ePHI)?**
   - Yes ☒ No ☐ N/A ☐

2. **Types of ePHI data elements that can be maintained by the device:**
   - a. Demographic (e.g., name, address, location, unique identification number)?
     - No ☐
   - b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?
     - Yes ☒ No ☐ N/A ☐
   - c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?
     - Yes ☒ No ☐ N/A ☐
   - d. Open, unstructured text entered by device user/operator?
     - Yes ☒ No ☐ N/A ☐

3. **Maintaining ePHI: Can the device**
   - a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?
     - No ☐
   - b. Store ePHI persistently on local media?
     - Yes ☒ No ☐ N/A ☐
   - c. Import/export ePHI with other systems?
     - Yes ☒ No ☐ N/A ☐

4. **Mechanisms used for the transmitting, importing/exporting of ePHI: Can the device**
   - a. Display ePHI (e.g., video display)?
     - Yes ☒ No ☐ N/A ☐
   - b. Copy hardcopy reports or images containing ePHI?
     - 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. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1394, serial port, USB, FireWire)?
     - Yes ☒ No ☐ N/A ☐
   - e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, internet, Internet)?
     - Yes ☒ No ☐ N/A ☐
   - f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?
     - Yes ☒ No ☐ N/A ☐
   - g. Other?
     - Yes ☒ No ☐ N/A ☐

5. **Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?**
   - Yes ☒ No ☐ N/A ☐

6. **Can the device log provide an audit trail of remote-service activity?**
   - Yes ☒ No ☐ N/A ☐

7. **Can the device owner/operator obtain administrative privileges (e.g., access operating system or application via local root or admin account)?**
   - Yes ☒ No ☐ N/A ☐

8. **Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?**
   - Yes ☒ No ☐ N/A ☐

9. **Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?**
   - Yes ☒ No ☐ N/A ☐

10. **Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?**
    - Yes ☒ No ☐ N/A ☐

11. **Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?**
    - Yes ☒ No ☐ N/A ☐

12. **Controls when exchanging ePHI with other devices:**
    - a. Transmitted only via a physically secure connection (e.g., dedicated cable)?
      - Yes ☒ No ☐ N/A ☐
    - b. Encrypted prior to transmission via a network or removable media?
      - Yes ☒ No ☐ N/A ☐
    - c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?
      - Yes ☒ No ☐ N/A ☐

13. **Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?**
    - Yes ☒ No ☐ N/A ☐
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. The DICOM image header of a patient image will contain ePHI (e.g. Patient ID, Patient Last Name, and Field ID), the ePHI cannot be viewed within the software.
2. Only the DICOM image can be imported/exported.