

**Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>**

**DEVICE DESCRIPTION**

|  |   |   |  |
|--|---|---|--|
| Device Category<br><a href="#">Ultrasound</a>      | Manufacturer<br><a href="#">FUJIFILM SonoSite, Inc.</a>                             | Document ID<br><a href="#">D13906 Rev. B</a>  | Document Release Date<br><a href="#">October, 2017</a> |
| Device Model<br><a href="#">M-Turbo</a>            | Software Revision<br><a href="#">1.9.2</a>  | Software Release Date<br><a href="#">March, 2017</a>                                    |  |
| Manufacturer or Representative Contact Information | Company Name<br><a href="#">FUJIFILM SonoSite, Inc.</a>                             | Manufacturer Contact Information<br><a href="#">FUJIFILM SonoSite Technical Support</a> |  |
|  | Representative Name/Position<br><a href="#">FUJIFILM SonoSite Technical Support</a> | <a href="#">Phone: 877-657-8118</a>   |  |
|  |   | <a href="#">Email: ffss-service@fujifilm.com</a>  |  |

**Intended use of device** in network-connected environment:  
[DICOM based communications including but not limited to: Ultrasound Image Storage, Modality Worklist, Print, Storage Commitment, Modality Performed Procedure Step](#)

**MANAGEMENT OF PRIVATE DATA**

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. |   | Yes, No, N/A, or See Note | Note # |
|--|---|---------------------------|--------|
| A  | Can this <b>device</b> display, transmit, or maintain <b>private data</b> (including <b>electronic Protected Health Information [ePHI]</b> )?   | Yes                       | 1      |
| B  | Types of <b>private data</b> elements that can be maintained by the <b>device</b> :   |                           |        |
|  | B.1 Demographic (e.g., name, address, location, unique identification number)?  | Yes                       | —      |
|  | B.2 Medical record (e.g., medical record #, account #, test or treatment date, <b>device</b> identification number)?  | Yes                       | —      |
|  | B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?  | Yes                       | —      |
|  | B.4 Open, unstructured text entered by <b>device user/operator</b> ?  | Yes                       | —      |
|  | B.5 <b>Biometric data</b> ?   | N/A                       | —      |
|  | B.6 Personal financial information?   | No                        | —      |
| C  | Maintaining <b>private data</b> - Can the <b>device</b> :   |                           |        |
|  | C.1 Maintain <b>private data</b> temporarily in volatile memory (i.e., until cleared by power-off or reset)?  | Yes                       | —      |
|  | C.2 Store <b>private data</b> persistently on local media?  | Yes                       | —      |
|  | C.3 Import/export <b>private data</b> with other systems?   | Yes                       | 2      |
|  | C.4 Maintain <b>private data</b> during power service interruptions?  | Yes                       | —      |
| D  | Mechanisms used for the transmitting, importing/exporting of <b>private data</b> – Can the <b>device</b> :  |                           |        |
|  | D.1 Display private data (e.g., video display, etc.)?   | Yes                       | —      |
|  | D.2 Generate hardcopy reports or images containing <b>private data</b> ?  | Yes                       | —      |
|  | D.3 Retrieve <b>private data</b> from or record <b>private data</b> to <b>removable media</b> (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?  | Yes                       | —      |
|  | D.4 Transmit/receive or import/export <b>private data</b> via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?   | No                        | —      |
|  | D.5 Transmit/receive <b>private data</b> via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?  | Yes                       | —      |
|  | D.6 Transmit/receive <b>private data</b> via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?   | Yes                       | —      |
|  | D.7 Import <b>private data</b> via scanning?  | Yes                       | —      |
|  | D.8 Other?  | —                         | —      |
| Management of Private Data notes:  | <p>1) Along with ultrasound images and clips, the device has the ability to store and transmit the following ePHI items: <a href="#">full patient name, DOB, gender, patient ID, accession number and indications.</a></p> <p>2) <a href="#">The device must be licensed and configured for data communications</a></p> |                           |        |

|                               |   |                                      |  |
|-------------------------------|---|--------------------------------------|--|
| Device Category<br>Ultrasound | Manufacturer<br>FUJIFILM SonoSite, Inc. | Document ID<br>D13906 Rev. B         | Document Release Date<br>October, 2017 |
| Device Model<br>M-Turbo       | Software Revision<br>1.9.2              | Software Release Date<br>March, 2017 |  |

**SECURITY CAPABILITIES**

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. |   | Yes, No,<br>N/A, or<br>See Note | Note # |
|--|---|---------------------------------|--------|
| <b>1</b>   | <b>AUTOMATIC LOGOFF (ALOF)</b><br>The <b>device's</b> ability to prevent access and misuse by unauthorized <b>users</b> if <b>device</b> is left idle for a period of time.                                       |                                 |        |
| 1-1  | Can the <b>device</b> be configured to force reauthorization of logged-in <b>user(s)</b> after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?           | Yes                             | —      |
| 1-1.1  | Is the length of inactivity time before auto-logoff/screen lock <b>user</b> or administrator configurable? (Indicate time [fixed or configurable range] in notes.)  | Yes                             | 1,2    |
| 1-1.2  | Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the <b>user</b> ?   | No                              | —      |
| ALOF notes:  | 1) Inactivity timer to enter sleep mode configurable to off, 5 minutes or 10 minutes.<br>2) Inactivity timer to power down configurable to off, 15 minutes or 30 minutes.   |                                 |        |
| <b>2</b>   | <b>AUDIT CONTROLS (AUDT)</b><br>The ability to reliably audit activity on the <b>device</b> .   |                                 |        |
| 2-1  | Can the <b>medical device</b> create an <b>audit trail</b> ?  | Yes                             | 1      |
| 2-2  | Indicate which of the following events are recorded in the audit log:   |                                 |        |
| 2-2.1  | Login/logout  | Yes                             | —      |
| 2-2.2  | Display/presentation of data  | No                              | —      |
| 2-2.3  | Creation/modification/deletion of data  | No                              | —      |
| 2-2.4  | Import/export of data from <b>removable media</b>   | No                              | —      |
| 2-2.5  | Receipt/transmission of data from/to external (e.g., network) connection  | No                              | —      |
| 2-2.5.1  | <b>Remote service</b> activity  | N/A                             | 1      |
| 2-2.6  | Other events? (describe in the notes section)   | See Note                        | 2      |
| 2-3  | Indicate what information is used to identify individual events recorded in the audit log:  |                                 |        |
| 2-3.1  | <b>User ID</b>  | Yes                             | —      |
| 2-3.2  | Date/time   | Yes                             | —      |
| AUDT notes:  | 1) There is no remote access to the device.<br>2) Audit functions only provided when system is configured for Administrative mode. Individual user accounts are required when configured for Administrative mode. |                                 |        |
| <b>3</b>   | <b>AUTHORIZATION (AUTH)</b><br>The ability of the device to determine the authorization of users.   |                                 |        |
| 3-1  | Can the <b>device</b> prevent access to unauthorized <b>users</b> through <b>user</b> login requirements or other mechanism?  | Yes                             | —      |
| 3-2  | Can <b>users</b> be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular <b>users</b> , power <b>users</b> , administrators, etc.)?                                  | Yes                             | 1      |
| 3-3  | Can the <b>device</b> owner/ <b>operator</b> obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?  | No                              | —      |
| AUTH notes:  | 1) Individual user accounts are required when the device is configured for Administrative mode. Accounts can be created for device administrators and general users.  |                                 |        |

| Device Category  | Manufacturer  | Document ID   | Document Release Date     |        |
|--|---|---|---------------------------|--------|
| Ultrasound   | FUJIFILM SonoSite, Inc.   | D13906 Rev. B   | October, 2017             |        |
| Device Model   | Software Revision   | Software Release Date   |                           |        |
| M-Turbo  | 1.9.2   | March, 2017   |                           |        |
| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. |   |   | Yes, No, N/A, or See Note | Note # |
| <b>4</b>   | <b>CONFIGURATION OF SECURITY FEATURES (CNFS)</b>  |   |                           |        |
|  | The ability to configure/re-configure <b>device security capabilities</b> to meet <b>users'</b> needs.  |   |                           |        |
| 4-1  | Can the <b>device</b> owner/operator reconfigure product <b>security capabilities</b> ?   |   | Yes                       | 1      |
| CNFS notes:  | 1) With the appropriate administrative privileges, the device owner may reconfigure the security capabilities.  |   |                           |        |
| <b>5</b>   | <b>CYBER SECURITY PRODUCT UPGRADES (CSUP)</b>   |   |                           |        |
|  | The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade <b>device's</b> security patches.                     |   |                           |        |
| 5-1  | Can relevant OS and <b>device</b> security patches be applied to the <b>device</b> as they become available?  |   | No                        | 1      |
|  | 5-1.1   | Can security patches or other software be installed remotely? | N/A                       | 2      |
| CSUP notes:  | 1) FUJIFILM SonoSite will provide system updates to deploy any applicable security patches.<br>2) There is no remote access to the device.                        |   |                           |        |
| <b>6</b>   | <b>HEALTH DATA DE-IDENTIFICATION (DIDT)</b>   |   |                           |        |
|  | The ability of the <b>device</b> to directly remove information that allows identification of a person.   |   |                           |        |
| 6-1  | Does the <b>device</b> provide an integral capability to de-identify <b>private data</b> ?  |   | Yes                       | 1,2    |
| DIDT notes:  | 1) The device can be configured to mask PHI on the display screen.<br>2) The device can has a feature to anonymize patient data prior to USB export.              |   |                           |        |
| <b>7</b>   | <b>DATA BACKUP AND DISASTER RECOVERY (DTBK)</b>   |   |                           |        |
|  | The ability to recover after damage or destruction of <b>device</b> data, hardware, or software.  |   |                           |        |
| 7-1  | Does the <b>device</b> have an integral data backup capability (i.e., backup to remote storage or <b>removable media</b> such as tape, disk)?                     |   | No                        | —      |
| DTBK notes:  |   |   |                           |        |
| <b>8</b>   | <b>EMERGENCY ACCESS (EMRG)</b>  |   |                           |        |
|  | The ability of <b>device users</b> to access <b>private data</b> in case of an emergency situation that requires immediate access to stored <b>private data</b> . |   |                           |        |
| 8-1  | Does the <b>device</b> incorporate an <b>emergency access</b> ("break-glass") feature?  |   | No                        | —      |
| EMRG notes:  |   |   |                           |        |
| <b>9</b>   | <b>HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)</b>  |   |                           |        |
|  | How the <b>device</b> ensures that data processed by the <b>device</b> has not been altered or destroyed in an unauthorized manner and is from the originator.    |   |                           |        |
| 9-1  | Does the <b>device</b> ensure the integrity of stored data with implicit or explicit error detection/correction technology?                                       |   | No                        | —      |
| IGAU notes:  |   |   |                           |        |

|  |  |  |  |        |
|--|--|--|--|--------|
| Device Category<br><a href="#">Ultrasound</a>  | Manufacturer<br><a href="#">FUJIFILM SonoSite, Inc.</a>  | Document ID<br><a href="#">D13906 Rev. B</a>         | Document Release Date<br><a href="#">October, 2017</a> |        |
| Device Model<br><a href="#">M-Turbo</a>  | Software Revision<br><a href="#">1.9.2</a>   | Software Release Date<br><a href="#">March, 2017</a> |  |        |
| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.   |  |  | Yes, No,<br>N/A, or<br>See Note                        | Note # |
| <b>10 MALWARE DETECTION/PROTECTION (MLDP)</b>  |  |  |  |        |
| The ability of the <b>device</b> to effectively prevent, detect and remove malicious software ( <b>malware</b> ).  |  |  |  |        |
| 10-1   | Does the <b>device</b> support the use of <b>anti-malware</b> software (or other <b>anti-malware</b> mechanism)?   |  | No   | 1      |
| 10-1.1   | Can the <b>user</b> independently re-configure <b>anti-malware</b> settings?   |  | N/A  | —      |
| 10-1.2   | Does notification of <b>malware</b> detection occur in the <b>device user</b> interface?   |  | N/A  | —      |
| 10-1.3   | Can only manufacturer-authorized persons repair systems when <b>malware</b> has been detected?   |  | N/A  | —      |
| 10-2   | Can the device owner install or update <b>anti-virus software</b> ?  |  | No   | 1      |
| 10-3   | Can the device owner/ <b>operator</b> (technically/physically) update virus definitions on manufacturer-installed <b>anti-virus software</b> ?   |  | N/A  | —      |
| MLDP notes:  | <a href="#">1) No third party software can be installed on the device, including anti-virus and malware detection software. All applicable security patches and vulnerabilities are addressed by FUJIFILM SonoSite through system updates.</a> |  |  |        |
| <b>11 NODE AUTHENTICATION (NAUT)</b>   |  |  |  |        |
| The ability of the <b>device</b> to authenticate communication partners/nodes.   |  |  |  |        |
| 11-1   | Does the <b>device</b> provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?                                  |  | Yes  | 1      |
| NAUT notes:  | <a href="#">1) When optionally configured for DICOM based communications, the modality (sender) and the recipient must be identified.</a>  |  |  |        |
| <b>12 PERSON AUTHENTICATION (PAUT)</b>   |  |  |  |        |
| Ability of the <b>device</b> to authenticate <b>users</b>  |  |  |  |        |
| 12-1   | Does the <b>device</b> support <b>user/operator</b> -specific username(s) and password(s) for at least one <b>user</b> ?   |  | Yes  | —      |
| 12-1.1   | Does the device support unique <b>user/operator</b> -specific IDs and passwords for multiple users?  |  | Yes  | —      |
| 12-2   | Can the <b>device</b> be configured to authenticate <b>users</b> through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?  |  | No   | —      |
| 12-3   | Can the <b>device</b> be configured to lock out a <b>user</b> after a certain number of unsuccessful logon attempts?   |  | No   | —      |
| 12-4   | Can default passwords be changed at/prior to installation?   |  | N/A  | —      |
| 12-5   | Are any shared <b>user</b> IDs used in this system?  |  | Yes  | 1      |
| 12-6   | Can the <b>device</b> be configured to enforce creation of <b>user</b> account passwords that meet established complexity rules?   |  | No   | —      |
| 12-7   | Can the <b>device</b> be configured so that account passwords expire periodically?   |  | No   | —      |
| PAUT notes:  | <a href="#">1) User authentication is required when the system is configured in the optional Administrative mode. Up to 20 user accounts can be created, and may be shared.</a>  |  |  |        |
| <b>13 PHYSICAL LOCKS (PLOK)</b>  |  |  |  |        |
| Physical locks can prevent unauthorized <b>users</b> with physical access to the <b>device</b> from compromising the integrity and confidentiality of <b>private data</b> stored on the <b>device</b> or on <b>removable media</b> . |  |  |  |        |
| 13-1   | Are all <b>device</b> components maintaining <b>private data</b> (other than <b>removable media</b> ) physically secure (i.e., cannot remove without tools)?   |  | Yes  | —      |
| PLOK notes:  |  |  |  |        |

| Device Category | Manufacturer            | Document ID           | Document Release Date |
|-----------------|-------------------------|-----------------------|-----------------------|
| Ultrasound      | FUJIFILM SonoSite, Inc. | D13906 Rev. B         | October, 2017         |
| Device Model    | Software Revision       | Software Release Date |                       |
| M-Turbo         | 1.9.2                   | March, 2017           |                       |

  

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. |  |   | Yes, No, N/A, or See Note | Note # |
|--|--|---|---------------------------|--------|
| <b>14</b>  | <b>ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)</b>  | Manufacturer's plans for security support of 3rd party components within <b>device</b> life cycle.                            |                           |        |
| 14-1   | In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).   | Yes   | 1                         |        |
| 14-2   | Is a list of other third party applications provided by the manufacturer available?  | Yes   | —                         |        |
| RDMP notes:  | 1) Device uses VxWorks embedded OS and a sub-set of Windows CE for underlying communications tasks. No Windows interfaces provided. VxWorks 5.4.2/ WinCE 6.0 R2  |   |                           |        |
| <b>15</b>  | <b>SYSTEM AND APPLICATION HARDENING (SAHD)</b>   | The <b>device's</b> resistance to cyber attacks and <b>malware</b> .  |                           |        |
| 15-1   | Does the <b>device</b> employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.  | Yes   | 1                         |        |
| 15-2   | Does the <b>device</b> employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?   | No  | —                         |        |
| 15-3   | Does the <b>device</b> have external communication capability (e.g., network, modem, etc.)?  | Yes   | 2                         |        |
| 15-4   | Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?  | No  | —                         |        |
| 15-5   | Are all accounts which are not required for the <b>intended use</b> of the <b>device</b> disabled or deleted, for both <b>users</b> and applications?  | Yes   | 3                         |        |
| 15-6   | Are all shared resources (e.g., file shares) which are not required for the <b>intended use</b> of the <b>device</b> , disabled?   | Yes   | —                         |        |
| 15-7   | Are all communication ports which are not required for the <b>intended use</b> of the <b>device</b> closed/disabled?   | Yes   | 1                         |        |
| 15-8   | Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the <b>intended use</b> of the <b>device</b> deleted/disabled?  | Yes   | —                         |        |
| 15-9   | Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the <b>intended use</b> of the <b>device</b> deleted/disabled?   | Yes   | —                         |        |
| 15-10  | Can the <b>device</b> boot from uncontrolled or <b>removable media</b> (i.e., a source other than an internal drive or memory component)?  | No  | —                         |        |
| 15-11  | Can software or hardware not authorized by the <b>device</b> manufacturer be installed on the device without the use of tools?   | No  | —                         |        |
| SAHD notes:  | 1) All ports and services not needed for the device to operate as intended have been disabled or removed.<br>2) The device can to connect to a wired or wireless network. The DICOM ports are configurable in Settings.<br>3) There are no default service accounts on the device. |   |                           |        |
| <b>16</b>  | <b>SECURITY GUIDANCE (SGUD)</b>  | The availability of security guidance for <b>operator</b> and administrator of the system and manufacturer sales and service. |                           |        |
| 16-1   | Are security-related features documented for the <b>device user</b> ?  | Yes   | —                         |        |
| 16-2   | Are instructions available for <b>device</b> /media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?   | Yes   | —                         |        |
| SGUD notes:  |  |   |                           |        |

| Device Category   | Manufacturer   | Document ID           | Document Release Date |                                 |        |
|---|--|-----------------------|-----------------------|---------------------------------|--------|
| Ultrasound  | FUJIFILM SonoSite, Inc.  | D13906 Rev. B         | October, 2017         |                                 |        |
| Device Model  | Software Revision  | Software Release Date |                       |                                 |        |
| M-Turbo   | 1.9.2  | March, 2017           |                       |                                 |        |
| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.  |  |                       |                       | Yes, No,<br>N/A, or<br>See Note | Note # |
| <b>17 HEALTH DATA STORAGE CONFIDENTIALITY (STCF)</b>  |  |                       |                       |                                 |        |
| The ability of the <b>device</b> to ensure unauthorized access does not compromise the integrity and confidentiality of <b>private data</b> stored on <b>device</b> or <b>removable media</b> . |  |                       |                       |                                 |        |
| 17-1  | Can the <b>device</b> encrypt data at rest?  |                       | Yes                   |                                 | 1      |
| STCF notes:   | 1) The device uses 256 bit encryption to protect data at rest.   |                       |                       |                                 |        |
| <b>18 TRANSMISSION CONFIDENTIALITY (TXCF)</b>   |  |                       |                       |                                 |        |
| The ability of the <b>device</b> to ensure the confidentiality of transmitted <b>private data</b> .   |  |                       |                       |                                 |        |
| 18-1  | Can <b>private data</b> be transmitted only via a point-to-point dedicated cable?  |                       | No                    |                                 | —      |
| 18-2  | Is <b>private data</b> encrypted prior to transmission via a network or <b>removable media</b> ? (If yes, indicate in the notes which encryption standard is implemented.) |                       | No                    |                                 | —      |
| 18-3  | Is <b>private data</b> transmission restricted to a fixed list of network destinations?  |                       | Yes                   |                                 | —      |
| TXCF notes:   |  |                       |                       |                                 |        |
| <b>19 TRANSMISSION INTEGRITY (TXIG)</b>   |  |                       |                       |                                 |        |
| The ability of the <b>device</b> to ensure the integrity of transmitted <b>private data</b> .   |  |                       |                       |                                 |        |
| 19-1  | Does the <b>device</b> support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)    |                       | No                    |                                 | —      |
| TXIG notes:   |  |                       |                       |                                 |        |
| <b>20 OTHER SECURITY CONSIDERATIONS (OTHR)</b>  |  |                       |                       |                                 |        |
| Additional security considerations/notes regarding <b>medical device</b> security.  |  |                       |                       |                                 |        |
| 20-1  | Can the <b>device</b> be serviced remotely?  |                       | No                    |                                 | —      |
| 20-2  | Can the <b>device</b> restrict remote access to/from specified devices or <b>users</b> or network locations (e.g., specific IP addresses)?                                 |                       | N/A                   |                                 | —      |
| 20-2.1  | Can the <b>device</b> be configured to require the local <b>user</b> to accept or initiate remote access?  |                       | N/A                   |                                 | —      |
| OTHR notes:   |  |                       |                       |                                 |        |