Manufacturer Disclosure Statement for Medical Device Security – MDS[2]

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Ultrasound	FUJIFILM SonoSite, Inc.		Feb 07th, 2017

Device Model	Software Revision	Software Release Date
iViz ®	1.1.2	Feb 20th, 2017

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	Fujifilm SonoSite	1 877 657 8118 ffss-service@fujifilm.com
	Representative Name/Position	
	Rick Hippe, Sr Director, Medical Informatics	

Intended use of **device** in network-connected environment:

DICOM based communications including but not limited to: Image Archive, Modality Worklist.

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 **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	Yes	
B	Types of **private data** elements that can be maintained by the **device**:		
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, **device** 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 **device user/operator**?	Yes	__
B.5	**Biometric data**?	N/A	__
B.6	Personal financial information?	No	__
C	Maintaining **private data** - Can the **device**:		
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	__
C.2	Store **private data** persistently on local media?	Yes	__
C.3	Import/export **private data** with other systems?	Yes	
C.4	Maintain **private data** during power service interruptions?	Yes	__
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
D.1	Display private data (e.g., video display, etc.)?	Yes	__
D.2	Generate hardcopy reports or images containing **private data**?	Yes	__
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	__
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	No	
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	
D.7	Import **private data** via scanning?	Yes	__
D.8	Other?	_____	__

Management of Private Data notes:

Device Category	Manufacturer	Document ID	Document Release Date
Ultrasound	FUJIFILM SonoSite, Inc.		Feb 07th, 2017
Device Model	**Software Revision**		**Software Release Date**
iViz ®	1.1.2		Feb 20th, 2017

SECURITY CAPABILITIES

	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 #
1	**AUTOMATIC LOGOFF (ALOF)**		
	The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) 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 **user** 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 **user**?	Yes	__
ALOF notes:	1) Inactivity timer to enter sleep mode configurable to off, range from 15 seconds to 30 minutes. 2) Inactivity timer to power down configurable off, range from 15 seconds to 30 minutes. 3) iViz has Power button to lock screen 4) Auto Freeze feature makes iViz to go sleep mode and eventually to shutdown		
2	**AUDIT CONTROLS (AUDT)**		
	The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	No	__
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	N/A	__
2-2.2	Display/presentation of data	N/A	__
2-2.3	Creation/modification/deletion of data	N/A	__
2-2.4	Import/export of data from **removable media**	N/A	__
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	N/A	__
2-2.5.1	**Remote service** activity	N/A	__
2-2.6	Other events? (describe in the notes section)	_____	__
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1	**User** ID	N/A	__
2-3.2	Date/time	N/A	__
AUDT notes:			
3	**AUTHORIZATION (AUTH)**		
	The ability of the device to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	See Note	1
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	No	__
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	__
AUTH notes:	1) iViz provides access control through PIN / Pattern / Password selected by user. This is not enforced; the user can opt to not have any access control.		

the Healthcare Information and Management Systems Society.

Device Category	Manufacturer	Document ID	Document Release Date
Ultrasound	FUJIFILM SonoSite, Inc.		Feb 07th, 2017
Device Model	**Software Revision**		**Software Release Date**
iViz ®	1.1.2		Feb 20th, 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 #
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)**		
	The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/operator reconfigure product **security capabilities**?	See Note	_1_
CNFS notes:	1) Device owner may reconfigure security capabilities such as to use passwords or not.		
5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)**		
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	Yes	1
5-1.1	Can security patches or other software be installed remotely?	Yes	2
CSUP notes:	1) FFSS can send software versions over the air to the device (except in Japanese markets). 2) The product owner needs to explicitly allow and accept the available software version upgrade to be applied the device.		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)**		
	The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	Yes	1
DIDT notes:	1) Annonymization of private data happens at time of export		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)**		
	The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	No	1
DTBK notes:	1) The user can enable patient and study data backup to the cloud based archive for patient data only. 2) User can reset device to Factory default setting		
8	**EMERGENCY ACCESS (EMRG)**		
	The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	No	__
EMRG notes:			
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)**		
	How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	__
IGAU notes:	1. If Pin/Password is set, access to device is secured hence data alteration is not possible 2. Once study is archieved, study can not be altered		

Device Category	Manufacturer	Document ID	Document Release Date
Ultrasound	FUJIFILM SonoSite, Inc.		Feb 07th, 2017
Device Model	**Software Revision**		**Software Release Date**
iViz ®	1.1.2		Feb 20th, 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 #
10	**MALWARE DETECTION/PROTECTION (MLDP)**		
	The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	No	_1_
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	N/A	__
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	N/A	__
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	__
10-2	Can the device owner install or update **anti-virus software**?	No	
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	N/A	__
MLDP notes:	1) Installed applications are locked to read only area at time of shipment. User can not install any application		
11	**NODE AUTHENTICATION (NAUT)**		
	The ability of the **device** to authenticate communication partners/nodes.		
11-1	Does the **device** 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:	1) When using DICOM based communications, the modality (sender) and the recipient must be identified. 2) Device also support Wifi certificate based authentication (EAP/TLS)		
12	**PERSON AUTHENTICATION (PAUT)**		
	Ability of the **device** to authenticate **users**		
12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	No	__
12-1.1	Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	N/A	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	No	__
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	Yes	__
12-4	Can default passwords be changed at/prior to installation?	Yes	1
12-5	Are any shared **user** IDs used in this system?	No	
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	No	__
12-7	Can the **device** be configured so that account passwords expire periodically?	No	__
PAUT notes:	1) No default password set at time of shipping. User must set password and change frequently		
13	**PHYSICAL LOCKS (PLOK)**		
	Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.		
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	Yes	__
PLOK notes:			

Device Category	Manufacturer	Document ID	Document Release Date
Ultrasound	FUJIFILM SonoSite, Inc.		Feb 07th, 2017
Device Model	**Software Revision**		**Software Release Date**
iViz ®	1.1.2		Feb 20th, 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 #
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**		
	Manufacturer's plans for security support of 3rd party components within **device** 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	2
RDMP notes:	1) Android OS 4.4.2 2) Adobe reader, Printhand application		
15	**SYSTEM AND APPLICATION HARDENING (SAHD)**		
	The **device**'s resistance to cyber attacks and **malware**.		
15-1	Does the **device** 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 **device** 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?	Yes	2
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes	
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 **intended use** of the **device** disabled or deleted, for both **users** and applications?	Yes	
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	Yes	
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** 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 **intended use** of the **device** deleted/disabled?	Yes	
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	No	
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No	
SAHD notes:	1) Device locks down all the open ports 2) Every software upgrade has unique checksum 3)		
16	**SECURITY GUIDANCE (SGUD)**		
	The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the **device user**?	Yes	
16-2	Are instructions available for **device**/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.		Feb 07th, 2017
Device Model	**Software Revision**		**Software Release Date**
iViz ®	1.1.2		Feb 20th, 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 #
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)**		
	The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.		
17-1	Can the **device** encrypt data at rest?	No	—
STCF notes:			
18	**TRANSMISSION CONFIDENTIALITY (TXCF)**		
	The ability of the **device** to ensure the confidentiality of transmitted **private data**.		
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	No	—
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	Yes	1
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	—
TXCF notes:	1) For network transmission, Any communication to the public secure cloud is encrypted using 128b TLS. For removable media it is not encrypted		
19	**TRANSMISSION INTEGRITY (TXIG)**		
	The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	See Note	1
TXIG notes:	1) Use of TLS with the proper CA certs ensures that the data has not been tampered by an intermediary ("man in the middle") during transmission to the cloud.		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)**		
	Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	No	—
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	N/A	—
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	N/A	—
OTHR notes:			