	A	B	C	D
1	**Manufacturer Disclosure Statement for Medical Device Security -- MDS2**			
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
4	**QUESTION ID**	**QUESTIONS**		**NOTES**
5	DOC-1	Manufacturer Name	FUJIFILM SonoSite, Inc.	__
6	DOC-2	Device Description	Ultrasound	__
7	DOC-3	Device Model	SII	__
8	DOC-4	Document ID	D19108	__
9	DOC-5	Manufacturer Contact Information	FUJIFILM SonoSite Technical Support Phone: 877-657-8118 Email: ffss-service@fujifilm.com	__
10	DOC-6	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	__
11	DOC-7	Document Release Date	December, 2019	__
12	DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	https://www.sonosite.com/support/security
13	DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	Yes	__
14	DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	__
15	DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	__
16	DOC-11.1	Does the SaMD contain an operating system?	NA	__
17	DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	NA	__
18	DOC-11.3	Is the SaMD hosted by the manufacturer?	NA	
19	DOC-11.4	Is the SaMD hosted by the customer?	NA	__
20				
21				
22		**MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION**		**NOTES**
23	MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	Along with ultrasound images and clips, the device has the ability to store and transmit the following ePHI items: Full Patient Name, DOB, Gender, Patient ID, Accession Number and Indications.
24	MPII-2	Does the device maintain personally identifiable information?	Yes	
25	MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	__
26	MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	__
27	MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	__
28	MPII-2.4	Does the device store personally identifiable information in a database?	Yes	__
29	MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	No	__
30	MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	The device must be licensed and configured for data communications

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
31	MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	—
32	MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	—
33	MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	
34	MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	—
35	MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	—
36	MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	Yes	—
37	MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	Yes	—
38	MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	—
39	MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	—
40	MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	Yes	—
41	MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	—
42	MPII-3.8	Does the device import personally identifiable information via scanning a document?	Yes	
43	MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
44		Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	—
45	Management of Private Data notes:			
46				
47				
48		**AUTOMATIC LOGOFF (ALOF)**		**NOTES**
49		*The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.*		
50	ALOF-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	Inactivity timer to enter sleep mode configurable to off, 5 minutes or 10 minutes. 2) Inactivity timer to power down configurable to off, 15 minutes or 30 minutes.
51	ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	Inactivity timer to enter sleep mode configurable to off, 5 minutes or 10 minutes. 2) Inactivity timer to power down configurable to off, 15 minutes or 30 minutes.
52				
53				
54		**AUDIT CONTROLS (AUDT)**		**NOTES**
55		*The ability to reliably audit activity on the device.*		

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
56	AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	__
57	AUDT-1.1	Does the audit log record a USER ID?	Yes	__
58	AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No	
59	AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	__
60	AUDT-2.1	Successful login/logout attempts?	Yes	__
61	AUDT-2.2	Unsuccessful login/logout attempts?	Yes	__
62	AUDT-2.3	Modification of user privileges?	Yes	__
63	AUDT-2.4	Creation/modification/deletion of users?	Yes	__
64	AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	No	__
65	AUDT-2.6	Creation/modification/deletion of data?	No	__
66	AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	No	__
67	AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	No	__
68	AUDT-2.8.1	Remote or on-site support?	NA	__
69	AUDT-2.8.2	Application Programming Interface (API) and similar activity?	NA	__
70	AUDT-2.9	Emergency access?	NA	__
71	AUDT-2.10	Other events (e.g., software updates)?	No	__
72	AUDT-2.11	Is the audit capability documented in more detail?	Yes	__
73	AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	
74	AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	__
75	AUDT-4.1	Does the audit log record date/time?	Yes	__
76	AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	__
77	AUDT-5	Can audit log content be exported?	Yes	__
78	AUDT-5.1	Via physical media?	Yes	__
79	AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	__
80	AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No	__
81	AUDT-5.4	Are audit logs encrypted in transit or on storage media?	Yes	Audit logs are encrypted on the device storage
82	AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	__
83	AUDT-7	Are audit logs protected from modification?	Yes	__
84	AUDT-7.1	Are audit logs protected from access?	Yes	
85	AUDT-8	Can audit logs be analyzed by the device?	Yes	__
86				
87				
88		**AUTHORIZATION (AUTH)**		**NOTES**
89		*The ability of the device to determine the authorization of users.*		
90	AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	__
91	AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	No	__
92	AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	__
93	AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	__
94	AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	Individual user accounts are required when the device is configured for Administrative mode. Accounts can be created for device administrators and general users.

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
95	AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	No	__
96	AUTH-4	Does the device authorize or control all API access requests?	NA	__
97	AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	Yes	__
98				
99				
100		**CYBER SECURITY PRODUCT UPGRADES (CSUP)**		**NOTES**
101		*The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.*		
102	CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	FUJIFILM SonoSite systems run on a closed proprietary operating system which includes components from WindRiver VxWorks (5.4.2) and Windows Embedded Compact 7 (WEC7).
103	CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	FUJIFILM SonoSite systems run on a closed proprietary operating system which includes components from WindRiver VxWorks and Windows Embedded Compact 7 (WEC7).
104	CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__
105	CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__
106	CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	No	There is no remote access to the device
107	CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	__
108	CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	__
109	CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__
110	CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__
111	CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	__
112	CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	__
113	CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	No	__
114	CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	NA	__
115	CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	NA	__
116	CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	NA	__
117	CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	NA	__

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
118	CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	No	__
119	CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	NA	__
120	CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	NA	__
121	CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	NA	__
122	CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	NA	__
123	CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	No	__
124	CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	NA	__
125	CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	NA	__
126	CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	NA	__
127	CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	NA	__
128	CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	__
129	CSUP-8	Does the device perform automatic installation of software updates?	No	__
130	CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	NA	__
131	CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	Yes	__
132	CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	__
133	CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	__
134	CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	Yes	__
135	CSUP-11.2	Is there an update review cycle for the device?	Yes	__
136				
137				
138		**HEALTH DATA DE-IDENTIFICATION (DIDT)**		**NOTES**
139		*The ability of the device to directly remove information that allows identification of a person.*		
140	DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	Yes	The device can be configured to mask PHI on the display screen. The device has a feature to anonymize patient data prior to USB export.
141	DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes	The device can be configured to mask PHI on the display screen. The device has a feature to anonymize patient data prior to USB export.
142				
143				
144		**DATA BACKUP AND DISASTER RECOVERY (DTBK)**		**NOTES**

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
145		*The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.*		
146	DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	No	—
147	DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	Yes	—
148	DTBK-3	Does the device have an integral data backup capability to removable media?	No	—
149	DTBK-4	Does the device have an integral data backup capability to remote storage?	NA	
150	DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	No	
151	DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	NA	—
152				
153				
154		**EMERGENCY ACCESS (EMRG)**		**NOTES**
155		*The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.*		
156	EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	No	—
157				
158				
159		**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)**		**NOTES**
160		*How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.*		
161	IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No	—
162	IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	—
163				
164				
165		**MALWARE DETECTION/PROTECTION (MLDP)**		**NOTES**
166		*The ability of the device to effectively prevent, detect and remove malicious software (malware).*		
167	MLDP-1	Is the device capable of hosting executable software?	No	—
168	MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	No	FUJIFILM SonoSite ultrasound systems feature whitelist software, which prevents third-party software from being installed and/or executed on the product. No third party software can be installed and/or executed on FUJIFILM SonoSite ultrasound systems.
169	MLDP-2.1	Does the device include anti-malware software by default?	No	—
170	MLDP-2.2	Does the device have anti-malware software available as an option?	NA	—
171	MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	NA	—
172	MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	NA	—
173	MLDP-2.5	Does notification of malware detection occur in the device user interface?	NA	

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
174	MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	NA	
175	MLDP-2.7	Are malware notifications written to a log?	NA	
176	MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	NA	
177	MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	Yes	__
178	MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	Yes	__
179	MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	No	__
180	MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	NA	__
181	MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	NA	__
182				
183				
184		**NODE AUTHENTICATION (NAUT)**		**NOTES**
185		*The ability of the device to authenticate communication partners/nodes.*		
186	NAUT-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 (e.g. Web APIs, SMTP, SNMP)?	Yes	When optionally configured for DICOM based communications, the modality (sender) and the recipient must be identified
187	NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	Yes	Connections limited to pre defined DICOM server.
188	NAUT-2.1	Is the firewall ruleset documented and available for review?	NA	__
189	NAUT-3	Does the device use certificate-based network connection authentication?	No	__
190				
191				
192		**CONNECTIVITY CAPABILITIES (CONN)**		**NOTES**
193		*All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.*		
194	CONN-1	Does the device have hardware connectivity capabilities?	Yes	__
195	CONN-1.1	Does the device support wireless connections?	Yes	__
196	CONN-1.1.1	Does the device support Wi-Fi?	Yes	__
197	CONN-1.1.2	Does the device support Bluetooth?	No	__
198	CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	__
199	CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	No	__
200	CONN-1.2	Does the device support physical connections?	Yes	__
201	CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	__
202	CONN-1.2.2	Does the device have available USB ports?	Yes	__
203	CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	__
204	CONN-1.2.4	Does the device support other physical connectivity?	No	__

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
205	CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	__
206	CONN-3	Can the device communicate with other systems within the customer environment?	Yes	__
207	CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	__
208	CONN-5	Does the device make or receive API calls?	Yes	__
209	CONN-6	Does the device require an internet connection for its intended use?	No	__
210	CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	__
211	CONN-7.1	Is TLS configurable?	No	
212	CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	__
213				
214				
215		**PERSON AUTHENTICATION (PAUT)**		**NOTES**
216		*The ability to configure the device to authenticate users.*		
217	PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	There are no default service accounts on the device.
218	PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes	__
219	PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	__
220	PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	__
221	PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	__
222	PAUT-5	Can all passwords be changed?	Yes	__
223	PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	No	__
224	PAUT-7	Does the device support account passwords that expire periodically?	No	__
225	PAUT-8	Does the device support multi-factor authentication?	No	__
226	PAUT-9	Does the device support single sign-on (SSO)?	No	__
227	PAUT-10	Can user accounts be disabled/locked on the device?	Yes	__
228	PAUT-11	Does the device support biometric controls?	No	__
229	PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	__
230	PAUT-13	Does the device support group authentication (e.g. hospital teams)?	Yes	__
231	PAUT-14	Does the application or device store or manage authentication credentials?	Yes	__
232	PAUT-14.1	Are credentials stored using a secure method?	Yes	__
233				
234				
235		**PHYSICAL LOCKS (PLOK)**		**NOTES**
236		*Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media*		
237	PLOK-1	Is the device software only? If yes, answer “N/A” to remaining questions in this section.	No	__

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
238	PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes	__
239	PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	Yes	__
240	PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	NA	Media is None removable
241				
242				
243		**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**		**NOTES**
244		*Manufacturer's plans for security support of third-party components within the device's life cycle.*		
245	RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	__
246	RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	__
247	RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	__
248	RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	https://www.sonosite.com/support/sonosite-product-retirement-schedule
249				
250		**SOFTWARE BILL OF MATERIALS (SBoM)**		**NOTES**
251		*A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.*		
252	SBOM-1	Is the SBoM for this product available?	Yes	__
253	SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	__
254	SBOM-2.1	Are the software components identified?	Yes	__
255	SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	__
256	SBOM-2.3	Are the major version numbers of the software components identified?	Yes	__
257	SBOM-2.4	Are any additional descriptive elements identified?	Yes	__
258	SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	Yes	__
259	SBOM-4	Is there an update process for the SBoM?	Yes	__
260				
261		**SYSTEM AND APPLICATION HARDENING (SAHD)**		**NOTES**
262		*The device's inherent resistance to cyber attacks and malware.*		
263	SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	All ports and services not needed for the device to operate as intended have been disabled or removed
264	SAHD-2	Has the device received any cybersecurity certifications?	Yes	This device has been tested by 3rd Party Cyber Security tested organization
265	SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	System and Integerity checking is performed during boot up
266	SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	Yes	System and Integerity checking is performed during boot up

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
267	SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	System and Integerity checking is performed during boot up
268	SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	
269	SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	__
270	SAHD-5.1	Does the device provide role-based access controls?	Yes	__
271	SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes	__
272	SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	__
273	SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	Individual user accounts are required when the device is configured for Administrative mode. Accounts can be created for device administrators and general users.
274	SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	__
275	SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	__
276	SAHD-9	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	__
277	SAHD-10	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	__
278	SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes	__
279	SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	__
280	SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	__
281	SAHD-14	Can the device be hardened beyond the default provided state?	No	__
282	SAHD-14.1	Are instructions available from vendor for increased hardening?	NA	
283	SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes	
284	SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	Yes	__
285				
286				
287		**SECURITY GUIDANCE (SGUD)**		**NOTES**
288		*Availability of security guidance for operator and administrator of the device and manufacturer sales and service.*		
289	SGUD-1	Does the device include security documentation for the owner/operator?	Yes	__
290	SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes	__
291	SGUD-3	Are all access accounts documented?	Yes	__
292	SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	__

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
293	SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	—
294				
295				
296		**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)**		**NOTES**
297		*The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.*		
298	STCF-1	Can the device encrypt data at rest?	Yes	The device uses AES-256 bit encryption to protect data at rest.
299	STCF-1.1	Is all data encrypted or otherwise protected?	Yes	
300	STCF-1.2	Is the data encryption capability configured by default?	Yes	The device uses 256 bit encryption to protect data at rest
301	STCF-1.3	Are instructions available to the customer to configure encryption?	NA	Device is already configured
302	STCF-2	Can the encryption keys be changed or configured?	No	—
303	STCF-3	Is the data stored in a database located on the device?	Yes	—
304	STCF-4	Is the data stored in a database external to the device?	Yes	The device can to connect to a wired or wireless network. The DICOM ports are configurable in Settings
305				
306				
307		**TRANSMISSION CONFIDENTIALITY (TXCF)**		**NOTES**
308		*The ability of the device to ensure the confidentiality of transmitted personally identifiable information.*		
309	TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	—
310	TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	—
311	TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	—
312	TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	—
313	TXCF-4	Are connections limited to authenticated systems?	Yes	—
314	TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	—
315				
316				
317		**TRANSMISSION INTEGRITY (TXIG)**		**NOTES**
318		*The ability of the device to ensure the integrity of transmitted data.*		
319	TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes	Customers can order an optional FIPS 140-2 validated WiFi module to ensure data confidentiality between the system and their access point.
320	TXIG-2	Does the device include multiple sub-components connected by external cables?	No	—
321				
322				
323		**REMOTE SERVICE (RMOT)**		**NOTES**
324		*Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.*		
325	RMOT-1	Does the device permit remote service connections for device analysis or repair?	No	The device does not have any remote service capability. All servicing requires physical access to the device

	A	B	C	D
2	**FUJIFILM SonoSite, Inc.**	**SII**	**D19108**	**December, 2019**
3				
326	RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	NA	__
327	RMOT-1.2	Is there an indicator for an enabled and active remote session?	NA	__
328	RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	NA	__
329	RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	NA	__
330	RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	No	__
331				
332				
333		**OTHER SECURITY CONSIDERATIONS (OTHR)**		
334		*NONE*		
335		**Notes:**		
336				
337				
338				
339				