1	Manufacture	r Disclosure Statement for Medic	al Device Security M	DS2
2	FUJIFILM SonoSite, Inc		D19108	October, 2019
3	FOJIFILIVI SONOSILE, INI		D13100	October, 2013
4	Question ID	Question		See note
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	- <del></del>
9				-
9	DOC-5	Manufacturer Contact Information	FUJIFILM SonoSite Technical Sup	—
		Intended use of device in network-connected		
10	DOC-6	environment:	DICOM based communications in	
11	DOC-7	Document Release Date	October, 2019	
		Coordinated Vulnerability Disclosure: Does the		
		manufacturer have a vulnerability disclosure program		
12	DOC-8	for this device?	Yes, https://www.sonosite.com/su	
12	DOC-8	Tor this device:	res, https://www.soriosite.com/su	—
		ISAO: Is the manufacturer part of an Information		
13	DOC-9	Sharing and Analysis Organization?	Yes	
		Diagram: Is a network or data flow diagram available		
		that indicates connections to other system		
1.1	DOC 10	•	Vac	
14	DOC-10	components or expected external resources?	Yes	-
		SaMD: Is the device Software as a Medical Device		
15	DOC-11	(i.e. software-only, no hardware)?	No	
16	DOC-11.1	Does the SaMD contain an operating system?	NA	_
		Does the SaMD rely on an owner/operator provided		
4-7	000443	operating system?	NIA.	
17	DOC-11.2		NA	
		Is the SaMD hosted by the manufacturer?		
18	DOC-11.3		NA	
19	DOC-11.4	Is the SaMD hosted by the customer?	NA	
20	DOC-11.4	is the Salvid Hosted by the customer:	IVA	
20				
			Yes, No,	
			N/A, or	
21			See Note	Note #
		MANAGEMENT OF PERSONALLY IDENTIFIABLE		
22		INFORMATION		
				Along with ultrasound images and clips, the device
		Can this device display, transmit, store, or modify		has the ability to store and transmit the following
		personally identifiable information (e.g. electronic	Yes	ePHI items: Full Patient Name, DOB, Gender, Pat
23	MPII-1	, , ,	163	
23	IVIPII-1	Protected Health Information (ePHI))?		ID, Accession Number and Indications.
		Does the device maintain personally identifiable		
24	MPII-2	information?	Yes	
		Does the device maintain personally identifiable		
		information temporarily in volatile memory (i.e., until		
25	MPII-2.1	cleared by power-off or reset)?	Yes	
دع	IVII II-Z.I		103	
		Does the device store personally identifiable		
26	MPII-2.2	information persistently on internal media?	Yes	_
		Is personally identifiable information preserved in the		
27	MPII-2.3	device's non-volatile memory until explicitly erased?	Yes	
		Does the device store personally identifiable		
20	MDII 2 4		Vos	
28	MPII-2.4	information in a database?	Yes	-
		Does the device allow configuration to automatically		
		delete local personally identifiable information after		
29	MPII-2.5	it is stored to a long term solution?	No	
		•		
		Does the device import/export personally identifiable		
		information with other systems (e.g., a wearable		
		monitoring device might export personally		
30	MPII-2.6	identifiable information to a server)?	Yes	
		Does the device maintain personally identifiable		
		information when powered off, or during power		
21	MDU 2.7		Vos	
31	MPII-2.7	service interruptions?	Yes	-
		Does the device allow the internal media to be		
		removed by a service technician (e.g., for separate		
		destruction or customer retention)?	Yes	

	Δ.	Ď.	C	
	А	В	C	D
2	FUJIFILM SonoSite, Inc	SII	D19108	October, 2019
3				
		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		
22	MPII-2.9		No	
33	IVIPII-2.9	storage location)?	No	
		Does the device have mechanisms used for the		
		transmitting, importing/exporting of personally		
34	MPII-3	identifiable information?	Yes	_
		Does the device display personally identifiable		
35	MPII-3.1	information (e.g., video display, etc.)?	Yes	
		Does the device generate hardcopy reports or images		
36	MPII-3.2	containing personally identifiable information?	Yes	_
		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,		
37	MPII-3.3	CF/SD card, memory stick, etc.)?	Yes	
- 51	3.3	Does the device transmit/receive or import/export		_
		personally identifiable information via dedicated		
		cable connection (e.g., RS-232, RS-423, USB, FireWire,		
38	MPII-3.4	etc.)?	No	_
		Does the device transmit/receive personally		
		identifiable information via a wired network		
39	MPII-3.5	connection (e.g., RJ45, fiber optic, etc.)?	Yes	_
		Does the device transmit/receive personally		
		identifiable information via a wireless network		
		connection (e.g., WiFi, Bluetooth, NFC, infrared,		
40	MPII-3.6	cellular, etc.)?	Yes	
		Does the device transmit/receive personally		
		identifiable information over an external network		
41	MPII-3.7	(e.g., Internet)?	No	
41	IVIF II-3.7		NO	-
42	MADU 2.0	Does the device import personally identifiable	V	
42	MPII-3.8	information via scanning a document?	Yes	
		Does the device transmit/receive personally		
43	MPII-3.9	identifiable information via a proprietary protocol?	No	
		Does the device use any other mechanism to		
		transmit, import or export personally identifiable		
44	MPII-3.10	information?	No	_
45	Management of Privat	e Data notes:		
46				
47				
48		AUTOMATIC LOGOFF (ALOF)		
		The device's ability to prevent access and misuse by		
40		unauthorized users if device is left idle for a period of		
49		time.		
		Can the device be configured to force reauthorization		Inactivity timer to enter sleep mode configurable to
		of logged-in user(s) after a predetermined length of		off, 5 minutes or 10 minutes. 2) Inactivity timer to
		inactivity (e.g., auto-logoff, session lock, password		power down configurable to off, 15 minutes or 30
50	ALOF-1	protected screen saver)?	Yes	minutes.
				Inactivity timer to enter sleep mode configurable to
		Is the length of inactivity time before auto-		off, 5 minutes or 10 minutes. 2) Inactivity timer to
		logoff/screen lock user or administrator		power down configurable to off, 15 minutes or 30
51	ALOF-2	configurable?	Yes	minutes.
52		·		
53				
		ALIDIT CONTROLS (ALIDT)		
54		AUDIT CONTROLS (AUDT)		
55		The ability to reliably audit activity on the device.		
		Can the medical device create additional audit logs or		
56	AUDT-1	reports beyond standard operating system logs?	Yes	_
57	AUDT-1.1	Does the audit log record a USER ID?	Yes	
		Does other personally identifiable information exist in		
58	AUDT-1.2	the audit trail?	No	
		* * * * *		

	А	В	С	D
2			D19108	October, 2019
3	FUJIFILM SonoSite, Inc	JII	D19108	October, 2019
- 3		Are events recorded in an audit log? If yes, indicate		
		which of the following events are recorded in the		
59	AUDT-2	audit log:	Yes	
	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	_
6.4	ALIDT 2.5	D		
	AUDT-2.5 AUDT-2.6	Presentation of clinical or PII data (e.g. display, print)? Creation/modification/deletion of data?	No	_
- 63	AUD1-2.0	Import/export of data from removable media (e.g.	INO .	_
66	AUDT-2.7	USB drive, external hard drive, DVD)?	No	
		Receipt/transmission of data or commands over a		<del></del>
67	AUDT-2.8	network or point-to-point connection?	No	
68	AUDT-2.8.1	Remote or on-site support?	NA	_
		Application Programming Interface (API) and similar		
	AUDT-2.8.2	activity?	NA	_
-	AUDT-2.9	Emergency access?	NA No.	_
71	AUDT-2.10	Other events (e.g., software updates)?	No	_
72	AUDT-2.11	Is the audit capability documented in more detail?	Yes	
		Can the owner/operator define or select which	· <del></del>	_
73	AUDT-3	events are recorded in the audit log?	No	
		Is a list of data attributes that are captured in the		
	AUDT-4	audit log for an event available?	Yes	_
75	AUDT-4.1	Does the audit log record date/time?	Yes	_
7.0	AUDT 4.4.4	Can date and time be synchronized by Network Time		
	AUDT-4.1.1 AUDT-5	Protocol (NTP) or equivalent time source?  Can audit log content be exported?	Yes Yes	_
	AUDT-5.1	Via physical media?	Yes	_
-70	A0D1 3.1	Via IHE Audit Trail and Node Authentication (ATNA)	103	<del>-</del>
79	AUDT-5.2	profile to SIEM?	No	
		Via Other communications (e.g., external service		
80	AUDT-5.3	device, mobile applications)?	No	_
		Are audit logs encrypted in transit or on storage		
81	AUDT-5.4	media?	Yes	Audit logs are encrypted on the device storage
00	ALIDT C	Can audit logs be monitored/reviewed by		
-	AUDT-6 AUDT-7	owner/operator? Are audit logs protected from modification?	Yes Yes	_
	AUDT-7.1	Are audit logs protected from access?	Yes	<del></del>
	AUDT-8	Can audit logs be analyzed by the device?	Yes	
86		, ,		
87				
88		AUTHORIZATION (AUTH)		
		The ability of the device to determine the		
89		authorization of users.		
		Does the device prevent access to unauthorized users		
20	A. (T. ). 4	through user login requirements or other		
90	AUTH-1	mechanism?	Yes	_
		Can the device be configured to use federated credentials management of users for authorization		
91	AUTH-1.1	(e.g., LDAP, OAuth)?	No	
		Can the customer push group policies to the device	<del></del>	
92	AUTH-1.2	(e.g., Active Directory)?	No	
		Are any special groups, organizational units, or group		
93	AUTH-1.3	policies required?	No	_
		Can users be assigned different privilege levels based		
	ALITH 2	on 'role' (e.g., user, administrator, and/or service,	V	
94	AUTH-2	etc.)?	Yes	_
		Can the device owner/operator grant themselves		
		unrestricted administrative privileges (e.g., access		
		operating system or application via local root or		
95	AUTH-3	administrator account)?	No	
		Does the device authorize or control all API access		
96	AUTH-4	requests?	NA	_
		Does the device run in a restricted access mode, or		
97	AUTH-5	'kiosk mode', by default?	Yes	_
98				

	А	В	С	D
$\overline{}$	FUJIFILM SonoSite, Inc	JII .	D19108	October, 2019
3				
99				
100		CYBER SECURITY PRODUCT UPGRADES (CSUP)		
100		The ability of on-site service staff, remote service		
		staff, or authorized customer staff to install/upgrade		
101		device's security patches.		
		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		
100	CCUP 4	software/firmware? If no, answer "N/A" to questions	L.	
102	CSUP-1	in this section.	Yes	_
103	CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	
103	C30F-2	Does the device documentation provide instructions	163	<del>-</del>
		for owner/operator installation of patches or		
104	CSUP-2.1	software updates?	Yes	
		·		
		Does the device require vendor or vendor-authorized		
105	CSUP-2.2	service to install patches or software updates?	No	
		Does the device have the capability to receive remote		
106	CSUP-2.3	installation of patches or software updates?	No	—
		Does the medical device manufacturer allow security		
		updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the		
107	CSUP-2.4	manufacturer?	No	
107	C301 2.4	Does the device contain Drivers and Firmware? If yes,	110	_
108	CSUP-3	complete 3.1-3.4.	Yes	
		Does the device documentation provide instructions		
		for owner/operator installation of patches or		
109	CSUP-3.1	software updates?	Yes	
	CCLID 2 C	Does the device require vendor or vendor-authorized		
110	CSUP-3.2	service to install patches or software updates?	No	_
		Does the device have the capability to receive remote		
111	CSUP-3.3	installation of patches or software updates?	No	
		Does the medical device manufacturer allow security	-	
		updates from any third-party manufacturers (e.g.,		
		Microsoft) to be installed without approval from the		
112	CSUP-3.4	manufacturer?	No	_
		Does the device contain Anti-Malware Software? If		
113	CSUP-4	yes, complete 4.1-4.4.	No	_
		Does the device documentation provide instructions		
114	CCLID 4.1	for owner/operator installation of patches or	NIA.	
114	CSUP-4.1	software updates?	NA	_
		Does the device require vendor or vendor-authorized		
115	CSUP-4.2	service to install patches or software updates?	NA	
		and the second s		
		Does the device have the capability to receive remote		
116	CSUP-4.3	installation of patches or software updates?	NA	_
		Does the medical device manufacturer allow security		
		updates from any third-party manufacturers (e.g.,		
	CCLID 4 :	Microsoft) to be installed without approval from the		
117	CSUP-4.4	manufacturer?	NA	—
		Does the device contain Non-Operating System		
118	CSUP-5	commercial off-the-shelf components? If yes, complete 5.1-5.4.	No	
110	3301 3	Does the device documentation provide instructions		-
		for owner/operator installation of patches or		
119	CSUP-5.1	software updates?	NA	
		Does the device require vendor or vendor-authorized		
120	CSUP-5.2	service to install patches or software updates?	NA	_
1	CCLID F C	Does the device have the capability to receive remote		
121	CSUP-5.3	installation of patches or software updates?	NA	_

	А	В	C	D
			-	
2	FUJIFILM SonoSite, Inc	SII	D19108	October, 2019
3				
		Does the medical device manufacturer allow security		
		updates from any third-party manufacturers (e.g.,		
		Microsoft) to be installed without approval from the		
122	CSUP-5.4	manufacturer?	NA	
		Does the device contain other software components		
		(e.g., asset management software, license		
400		management)? If yes, please provide details or		
123	CSUP-6	reference in notes and complete 6.1-6.4.	No	—
		Does the device documentation provide instructions		
124	CSUP-6.1	for owner/operator installation of patches or software updates?	NA	
124	C30F-0.1	software updates:	NA .	_
		Does the device require vendor or vendor-authorized		
125	CSUP-6.2	service to install patches or software updates?	NA	
5	000. 0.2	service to instan pateries or sortificine apartes.		_
		Does the device have the capability to receive remote		
126	CSUP-6.3	installation of patches or software updates?	NA	
		Does the medical device manufacturer allow security		
		updates from any third-party manufacturers (e.g.,		
		Microsoft) to be installed without approval from the		
127	CSUP-6.4	manufacturer?	NA	_
		Does the manufacturer notify the customer when		
128	CSUP-7	updates are approved for installation?	Yes	_
		Does the device perform automatic installation of		
129	CSUP-8	software updates?	No	_
		Does the manufacturer have an approved list of third-		
130	CSUP-9	party software that can be installed on the device?	NA	_
		Can the owner/operator install manufacturer-		
131	CSUP-10	approved third-party software on the device themselves?	Yes	
131	C30P-10	Does the system have mechanism in place to prevent	res	_
132	CSUP-10.1	installation of unapproved software?	Yes	
132	C501 10.1	Does the manufacturer have a process in place to	103	<del>-</del>
133	CSUP-11	assess device vulnerabilities and updates?	Yes	
		Does the manufacturer provide customers with		
134	CSUP-11.1	review and approval status of updates?	Yes	
135	CSUP-11.2	Is there an update review cycle for the device?	Yes	_
136				
137				
138				
139		HEALTH DATA DE-IDENTIFICATION (DIDT)		
		The ability of the device to directly remove		
140		information that allows identification of a person.		The device can be configured to seed BULL at the
				The device can be configured to mask PHI on the
		Does the device provide an integral capability to de-		display screen.  The device has a feature to anonymize nations data
141	DIDT-1	identify personally identifiable information?	Yes	The device has a feature to anonymize patient data prior to USB export.
	0.011	Does the device support de-identification profiles	165	prior to our export.
		that comply with the DICOM standard for de-		
142	DIDT-1.1	identification?	Yes	
143				
144				
145		DATA BACKUP AND DISASTER RECOVERY (DTBK)		
		The ability to recover after damage or destruction of		
		device data, hardware, software, or site		
146		configuration information.		
		Does the device maintain long term primary storage		
		of personally identifiable information / patient		
147	DTBK-1	information (e.g. PACS)?	No	_
		Does the device have a "factory reset" function to		
		restore the original device settings as provided by the		
148	DTBK-2	manufacturer?	Yes	_
140	מ אמדת	Does the device have an integral data backup	No	
149	DTBK-3	capability to removable media?	No	_

Does the device have an integral data backup  130 OTBS-C4 capability to remote stronger  151 OTBS-C5 capability to remote stronger  152 OTBS-C6 capability to remote stronger  153 OTBS-C6 capability to remote stronger  154 OTBS-C6 capability to remote stronger  155 OTBS-C6 capability to remote stronger  156 capability to remote stronger  157 OTBS-C6 capability to remote stronger  158 OTBS-C6 capability to remote stronger  159 OTBS-C6 capability to remote stronger  150 OTBS-C6 capability to remote stronger  150 OTBS-C6 capability to remote stronger  151 OTBS-C6 capability or remote stronger  152 OTBS-C6 capability or remote stronger  153 OTBS-C6 capability or remote stronger  154 capability of the device user to access personally interceptions on capability of remote capability to check the integrity and authenticity of a backup?  156 OTBS-C6 capability of remote capability to check the integrity and authenticity of a backup?  157 OTBS-C7 Capability of remote capability to check the integrity capability of remote capability		A	В	С	D
Does the device have an integral data backup Does the device have a minetizal data backup Does the device have a backup capability for systems configuration information, patch restoration, and software restoration?  Does the device provide the capability to check the integral was a substitution of a backup?  Does the device provide the capability to check the integral was a substitution of a backup?  The ability of the device user to occess personally disemplose information is case of a medical energetic shability of the device user to access personally disemplose information is case of an ended energetic shability of the device user to access personally disemplose information in case of an ended energetic shability of the device user to access personally disemplose information in case of an ended energetic shability of the device user to access personally disemplose information in case of an ended energetic shability of the device user to access personally disemplose information in case of an ended energetic shability of the device user to access personally disemplose information in the requires immediate access in the advice of the device and an energetic shability of the access to a provide an energetic shability of the access of the energy of	2				
Does the device have an integral data backup  capability for remote storage  Does the device have a backup capability for system confliguration information, packin responsion, and confliguration information, packin  Does the device power of the capability to chack the integrity and subhembothy of a backup?  NA  NA  STEP 1915.  Does the device power of cocces personally interripable information in case of a medical energency substantion float require immediate access to stored personally interripable information.  Does the device interripable immediate access to stored personally interripable information.  In the ability of the device power on emergency access to stored personally interripable information.  In the ability of the device interripable information.  In the ability of the device information.  No  HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)  Above the device ensures that the stored data on the device has not been offerted or destroyed in a non- ountainment ensurance and pack may be enginerary.  In machinistics of stores health data (e.g.,  No  Does the device power mechanisms for stored health data (e.g.,  No  ALIDE-1 is the device exapted of hosting executable software?  MLDP-2 and the device support the sace of and immiliated and of the enginerary.  No  ALIDE-1 is the device support the sace of and immiliated and the enginerary.  No  ALIDE-2 is device provide details or reference in notes.  No  ALIDE-3 is the device support the sace of and immiliated and the enginerary of the packing of the device and packing of the device of the packing of the packing of the device of the pac		FUJIFILIVI SONOSITE, INC	J-11	D13100	October, 2013
1550   DT64-6   Capability for remote storage?			Does the device have an integral data backup		
configuration information, gatch restoration, and Solventian Configuration information, and Solventian Configuration information, and Solventian Configuration information in Integrity and authenticity of a backup?    152	150	DTBK-4		NA	
Does the device provide the capability to check the integrity and authenticity of a backup?   NA					
Does the device provide the capability to check the integrity and authenticity of a backup?    Signature					
1526 OTRA-6 integrity and authenticity of a backup?  153	151	DTBK-5	software restoration?	No	
1526 OTRA-6 integrity and authenticity of a backup?  153			Does the device provide the capability to check the		
154	152	DTBK-6		NA	_
EMERGENCY ACCESS (EMRG)   The ability of the device user to access personally identifibility by dentifibility by dentifibil	153		· ·		
The ability of the device user to access personally identifiable information in case of a medical emergency shutoth that requires immediate occess to stored personally identifiable information.  157 Device device incorporate an emergency access 158	154				
Identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.	155		EMERGENCY ACCESS (EMRG)		
Identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.			The ability of the device year to access norsenally		
Bear					
156					
1575   158   158   159   158   159	156				
158   159   HEALTH DATA INTEGRITY AND AUTHENTICITY   160			Does the device incorporate an emergency access		
HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)    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.   Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?   No	-	EMRG-1	(i.e. "break-glass") feature?	No	_
HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)  How the device ensures that the stored data on the device has not been oltered or destroyed in a non- unthrined momen and is from the originator.  Does the device provide at a integrity checking mechanisms of stored health data (e.g., hash or digital signature)  IGAU-1					
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 enjainator.	159		HEALTH DATA INTEGRITY AND AUTHENTICITY		
How the device ensures that the stored data on the device has not been altered or destroyed in a non- uuthorized manner and is from the originator.  Does the device provide data integrity rebecting mechanisms of stored health data (e.g., hash or oligital signature)?  Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., hash or oligital signature)?  In IGAU-2 RAID-5)?  No  MALWARE DETECTION/PROTECTION (MLDP)  The ability of the device to effectively prevent, detect and remove molicious software (malware).  In IGAU-1 Is the device capable of hosting executable software?  No  FUIFILM SonoSite ultrasound systems feath whitelist software, which prevents third par software from being installed and/or executed on the product. No party software on being installed and/or executed on the product. No party software on being installed and/or executed on the product. No Does the device include anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device chause anti-malware software by default?  No Does the device documentation allow the owner/operator independently (re- locnfigure anti-malware settings?  No Does ontification of malware detection occur in the device owner/operator independently (re- locnfigure anti-malware settings?  No Does notification of malware detection occur in the device owner/operator independently (re- locnfigure anti-malware settings?  No Does notification of malware detection occur in the device owner/operator independently (re- locnfigure anti-malware settings?  No Does the d	160				
devike his not been altered or destroyed in a non- authorized manner and is from the originator.  Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)  163 IGAU-1 (digital signature)  Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., hash or device device provide error/failure protection and recovery mechanisms for stored health data (e.g., hash or device device provide error/failure protection and recovery mechanisms for stored health data (e.g., hash or device device provide error/failure protection and recovery mechanisms for stored health data (e.g., hash or device devi			•		
161   authorized manner and is from the originator. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., no			How the device ensures that the stored data on the		
Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?  Does the device provide error/fallure protection and recovery mechanisms for stored health data (e.g., hash or digital signature)?  IGAU-2 RAID-5)?  No  MALWARE DETECTION/PROTECTION (MLDP)  The ability of the device to effectively prevent, detect and remove malicious software (mahware).  Is the device capable of hosting executable software?  No  FIJIFILM SonoSite ultrasound systems feat whitelist software, which prevents third-par software (are the device support the use of anti-malware software parts of the device of the device of the device in the device support the use of anti-malware software (are the device support the use of anti-malware software (are the device support the use of anti-malware software (are the device support the use of anti-malware software (by the device of the device support the use of anti-malware software (by the device of the device support the use of anti-malware software (by the device under the device support the use of anti-malware software (by the device under the device support the use of anti-malware software (by the device under the device undevice under the device under the device undevice u					
mechanisms of stored health data (e.g., hash or digital signature)?  Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., no    IGAU-2 RAID-5)?  No	161				
162   IGAU-1   digital signature;   Does the device provide error/fallure protection and recovery mechanisms for stored health data (e.g., no.)					
Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., no    163	162	IGAU-1	· -	No	
163   IGAU-2   RAID-5)?   No					
164   165   166   MALWARE DETECTION/PROTECTION (MLDP)			1		
165   166   MALWARE DETECTION/PROTECTION (MLDP)   167   168   MLDP-1   168   MLDP-1   169   MLDP-2   169   MLDP-2.1   169   MLDP-2.2   170   MLDP-2.4   171   MLDP-2.5   MLDP-2.5   MLDP-2.6   MLDP-2.6   MLDP-2.8   MLDP-		IGAU-2	RAID-5)?	No	_
MALWARE DETECTION/PROTECTION (MLDP)  The ability of the device to effectively prevent, detect and remove molicious software (molware).  168 MLDP-1 Is the device capable of hosting executable software?  Does the device capable of hosting executable software?  Does the device support the use of anti-malware with the software (or other anti-malware mechanism)?  Provide details or reference in notes.  Does the device include anti-malware software by default?  Does the device have anti-malware software wavilable as an option?  Does the device documentation allow the owner/operator to install or update anti-malware software  MLDP-2.3 software?  MLDP-2.4 loconfigure anti-malware software  MLDP-2.5 Loconfigure anti-malware settings?  NA  Does not device owner/operator independently (re- loconfigure anti-malware settings?  NA  Does not device wore/operator independently (re- loconfigure anti-malware settings?  NA  Does not device wore/operator independently (re- loconfigure anti-malware settings?  NA  And  Can the device wore/operator independently (re- loconfigure anti-malware settings?  NA  And  And  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA					
The ability of the device to effectively prevent, detect and remove malicious software (malware).  168 MLDP-1 Is the device capable of hosting executable software? No  FUJIFILM SonoSite ultrasound systems featt whitelist software, which prevents third-par software from being installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party soft	103				
The ability of the device to effectively prevent, detect and remove malicious software (malware).  168 MLDP-1 Is the device capable of hosting executable software? No  FUJIFILM SonoSite ultrasound systems featt whitelist software, which prevents third-par software from being installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party soft	166		MALWARE DETECTION/PROTECTION (MLDP)		
168 MLDP-1 Is the device capable of hosting executable software? No  FUJIFILM SonoSite ultrasound systems feature whitelist software, which prevents third-parasoftware from being installed and/or executed on the product. No party software from being installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party sof					
MLDP-1 Is the device capable of hosting executable software? No  FUJIFILM SonoSite ultrasound systems feat whitelist software, which prevents third-par software from being installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed on the product. N party software can be installed and/or executed					
FUJIFILM SonoSite ultrasound systems feature whitelists oftware, which prevents third-part software from being installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No ultrasound systems.  Does the device details or reference in notes. No ultrasound systems.  Does the device include anti-malware software by default? No —  Does the device have anti-malware software available as an option? NA —  Does the device documentation allow the owner/operator to install or update anti-malware software? NA —  Can the device owner/operator independently (reposential to the device owner/operator independently (	167		and remove malicious software (malware).		
FUJIFILM SonoSite ultrasound systems feature whitelists oftware, which prevents third-part software from being installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed on the product. No ultrasound systems.  Does the device details or reference in notes. No ultrasound systems.  Does the device include anti-malware software by default? No —  Does the device have anti-malware software available as an option? NA —  Does the device documentation allow the owner/operator to install or update anti-malware software? NA —  Can the device owner/operator independently (reposential to the device owner/operator independently (	168	MLDP-1	Is the device capable of hosting executable software?	No	
Software from being installed and/or executed on the product. No party software can be installed and/or executed on the product. No party software can be installed and/or executed and the product. No party software can be installed and/or executed and the product. No party software can be installed and/or executed and the product of the provide details or reference in notes.    No			8		FUJIFILM SonoSite ultrasound systems feature
Does the device support the use of anti-malware software (or other anti-malware mechanism)?  169 MLDP-2 Provide details or reference in notes. No ultrasound systems.  Does the device include anti-malware software by default? No Does the device have anti-malware software available as an option? NA Does the device documentation allow the owner/operator to install or update anti-malware software? NA Does notification of malware settings? NA Does notification of malware detection occur in the device user interface? NA Does notifications written to a log? NA Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? NA					whitelist software, which prevents third-party
Does the device support the use of anti-malware software (or other anti-malware mechanism)?  Provide details or reference in notes.  Does the device include anti-malware software by default?  No  Does the device have anti-malware software available as an option?  No  Does the device documentation allow the owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re-lookingure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA  Does the device support the use of anti-malware software FUIIFILM SonoSite ultrasound systems.  NO  Ultrasound systems.  NO  NO  Looking details or reference in notes.  NO  NO  NO  NO  NO  NO  NO  NO  NO  N					5
software (or other anti-malware mechanism)? Provide details or reference in notes.  Does the device include anti-malware software by default?  No  Does the device have anti-malware software available as an option?  NA  Does the device documentation allow the owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re-)configure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA  FUJIFILM SonoSite ultrasounds with authors.  No  ultrasound systems.  No  Ultrasound systems.  No  NA			Does the device support the core of		installed and/or executed on the product. No third
169 MLDP-2 Provide details or reference in notes. No ultrasound systems.  Does the device include anti-malware software by default? No Does the device have anti-malware software available as an option? NA Does the device documentation allow the owner/operator to install or update anti-malware software? NA Can the device owner/operator independently (re-173 MLDP-2.4 )configure anti-malware settings? NA Does notification of malware detection occur in the device user interface? NA device user interface? NA Are malware has been detected? NA Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? NA					
Does the device include anti-malware software by default?  No  Does the device have anti-malware software available as an option?  No  Does the device documentation allow the owner/operator to install or update anti-malware software?  NA  The device documentation allow the owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Does the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Does the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Can the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Does the device occurrence with the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Can the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Can the device owner/operator independently (re-loonfigure anti-malware settings?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA  NA  NA  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	169	MLDP-2	,	No	
Does the device have anti-malware software available as an option?  Does the device documentation allow the owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re- ponfigure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  NA  MLDP-2.6 systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA					
171 MLDP-2.2 available as an option?  Does the device documentation allow the owner/operator to install or update anti-malware  172 MLDP-2.3 software?  Can the device owner/operator independently (re- )configure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  176 MLDP-2.6 systems when malware has been detected?  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	170	MLDP-2.1		No	_
Does the device documentation allow the owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re-)configure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  To MLDP-2.6 systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	474	MIDD 2.3		NA.	
owner/operator to install or update anti-malware software?  NA  Can the device owner/operator independently (re- )configure anti-malware settings? NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  The MLDP-2.6 systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	1/1	IVILUP-2.2	·	INA	_
172 MLDP-2.3 software?  Can the device owner/operator independently (re- 173 MLDP-2.4 )configure anti-malware settings?  NA  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  175 MLDP-2.6 systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA					
Can the device owner/operator independently (re- )configure anti-malware settings?  Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  175 MLDP-2.6 systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	172	MLDP-2.3		NA	
Does notification of malware detection occur in the device user interface?  NA  Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  175 MLDP-2.6 systems when malware has been detected?  NA  MLDP-2.7 Are malware notifications written to a log?  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA					
174 MLDP-2.5 device user interface? NA  Can only manufacturer-authorized persons repair systems when malware has been detected? NA  176 MLDP-2.7 Are malware notifications written to a log? NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? NA	173	MLDP-2.4		NA	_
Can only manufacturer-authorized persons repair systems when malware has been detected?  NA  MLDP-2.6 Systems when malware has been detected?  NA  Are malware notifications written to a log?  NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	174	MIDD 2 E		NA	
175 MLDP-2.6 systems when malware has been detected? NA  176 MLDP-2.7 Are malware notifications written to a log? NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? NA	1/4	IVILUP-2.5	uevice user interrace?	IVA	
175 MLDP-2.6 systems when malware has been detected? NA  176 MLDP-2.7 Are malware notifications written to a log? NA  Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? NA			Can only manufacturer-authorized persons repair		
Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  NA	175	MLDP-2.6		NA	
177 MLDP-2.8 purchase, installation, configuration, scheduling)? NA	176	MLDP-2.7	Are malware notifications written to a log?	NA	
177 MLDP-2.8 purchase, installation, configuration, scheduling)? NA					
	177	MI DP-2 9	· -	NΔ	
If the answer to MIDD 2 is NO and anti-malways	177	IVILUF-4.0	parenase, mstanation, configuration, scrieduling)?	IVA	
II tile diswei to ivitur-2 is NO, dilu dilu-fildiwale			If the answer to MLDP-2 is NO, and anti-malware		
cannot be installed on the device, are other					
178 MLDP-3 compensating controls in place or available? Yes	178	MLDP-3	compensating controls in place or available?	Yes	

	A	В	С	D
2	FUJIFILM SonoSite, Inc	SII	D19108	October, 2019
3				
		Does the device employ application whitelisting that		
		restricts the software and services that are permitted		
179	MLDP-4	to be run on the device?	Yes	-
400		Does the device employ a host-based intrusion		
180	MLDP-5	detection/prevention system?	No	-
		Can the host-based intrusion detection/prevention		
181	MLDP-5.1	system be configured by the customer?	NA	-
		Can a host-based intrusion detection/prevention		
	MLDP-5.2	system be installed by the customer?	NA	_
183				
184				
185		NODE AUTHENTICATION (NAUT)		
		The ability of the device to authenticate		
186		communication partners/nodes.		
		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		When optionally configured for DICOM based
		authorized to receive transferred information (e.g.		communications, the modality (sender) and the
187	NAUT-1	Web APIs, SMTP, SNMP)?	Yes	recipient must be identified
		Are network access control mechanisms supported		
		(E.g., does the device have an internal firewall, or use		
188	NAUT-2	a network connection white list)?	Yes	Connections limited to pre defined DICOM server.
		Is the firewall ruleset documented and available for		
189	NAUT-2.1	review?	NA	
		Does the device use certificate-based network		
	NAUT-3	connection authentication?	No	
191				
192				
193		CONNECTIVITY CAPABILITIES (CONN)		
		All network and removable media connections must		
		be considered in determining appropriate security		
		controls. This section lists connectivity capabilities		
194		that may be present on the device.		
		Does the device have hardware connectivity		
	CONN-1	capabilities?	Yes	
	CONN-1.1	Does the device support wireless connections?	Yes	
197	CONN-1.1.1	Does the device support Wi-Fi?	Yes	
198	CONN-1.1.2	Does the device support Bluetooth?	No	
		Does the device support other wireless network		
199	CONN-1.1.3	connectivity (e.g. LTE, Zigbee, proprietary)?	No	_
		Does the device support other wireless connections	L.	
	CONN-1.1.4	(e.g., custom RF controls, wireless detectors)?	No	_
201	CONN-1.2	Does the device support physical connections?	Yes	-
202	CONN 4 3 4	December design have the District of the Control of	V	
202	CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	_
203	CONN-1.2.2	Does the device have available USB ports?	Yes	_
20.	CONN 4 2 2	Does the device require, use, or support removable	V	
204	CONN-1.2.3	memory devices?	Yes	_
205	CONN 1 3 4	Doos the device support ather physical account 11.2	No	
205	CONN-1.2.4	., , ,	No	-
		Does the manufacturer provide a list of network ports		
206	CONN-3	and protocols that are used or may be used on the device?	Vos	
206	CONN-2		Yes	_
207	CONN-3	Can the device communicate with other systems within the customer environment?	Yes	
201	CONTR O	Can the device communicate with other systems	100	_
		external to the customer environment (e.g., a service		
208	CONN-4	host)?	No	
209	CONN-5	Does the device make or receive API calls?	Yes	—
203	CONTR. J	Does the device require an internet connection for its	100	-
210	CONN-6	intended use?	No	
2.10	3 0	Does the device support Transport Layer Security	<del>-</del>	
211	CONN-7	(TLS)?	Yes	
		(\$ - *F*		_

	А	В	С	D
2	FUJIFILM SonoSite, Inc		D19108	October, 2019
3	i can ilivi autioatte, IIIC	·	-=**	
212	CONN-7.1	Is TLS configurable?	No	
		Does the device provide operator control		
		functionality from a separate device (e.g.,		
213	CONN-8	telemedicine)?	No	_
214 215				
216		PERSON AUTHENTICATION (PAUT)		
210		The ability to configure the device to authenticate		
217		users.		
		Does the device support and enforce unique IDs and		
		passwords for all users and roles (including service		
218	PAUT-1	accounts)?	Yes	_
		Does the device enforce authentication of unique IDs and passwords for all users and roles (including		
219	PAUT-1.1	service accounts)?	Yes	
		·		_
		Is the device configurable to authenticate users		
222	DALIT 3	through an external authentication service (e.g., MS	N-	
220	PAUT-2	Active Directory, NDS, LDAP, OAuth, etc.)?	No	_
		Is the device configurable to lock out a user after a		
221	PAUT-3	certain number of unsuccessful logon attempts?	No	
		Are all default accounts (e.g., technician service		
		accounts, administrator accounts) listed in the		
	PAUT-4	documentation?	Yes	_
223	PAUT-5	Can all passwords be changed?	Yes	
		Is the device configurable to enforce creation of user		
		account passwords that meet established		
224	PAUT-6	(organization specific) complexity rules?	No	_
225	DALLE 7	Does the device support account passwords that		
225	PAUT-7	expire periodically?	No	_
226	PAUT-8	Does the device support multi-factor authentication?	No	
	PAUT-9	Does the device support single sign-on (SSO)?	No	
	PAUT-10	Can user accounts be disabled/locked on the device?	Yes	_
229	PAUT-11	Does the device support biometric controls?  Does the device support physical tokens (e.g. badge	No	-
230	PAUT-12	access)?	No	
		Does the device support group authentication (e.g.		
231	PAUT-13	hospital teams)?	Yes	_
222	DALLE 44	Does the application or device store or manage		
232	PAUT-14 PAUT-14.1	authentication credentials?  Are credentials stored using a secure method?	Yes Yes	_
234	1 701-14.1	And dicaetitials stored using a secure method?	163	
235				
236		PHYSICAL LOCKS (PLOK)		
		Physical locks can prevent unauthorized users with		
		physical access to the device from compromising the		
		integrity and confidentiality of personally identifiable		
237		information stored on the device or on removable media		
		Is the device software only? If yes, answer "N/A" to		
238	PLOK-1	remaining questions in this section.	No	
		Are all device components maintaining personally		
		identifiable information (other than removable		
239	PLOK-2	media) physically secure (i.e., cannot remove without tools)?	Yes	
233	I LUN-Z	Are all device components maintaining personally	163	_
		identifiable information (other than removable		
		media) physically secured behind an individually		
240	PLOK-3	keyed locking device?	Yes	_
		Does the device have an option for the customer to		
241	PLOK-4	attach a physical lock to restrict access to removable media?	NA	Media is None removable
241	I LUN-4	incuia:	IVA	Michig is Notic (CITIOVADIC
243				

2.4 FUBFILM Sorresties, Inc. 98 October, 2019  2.4 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)  Manufacturer's plans for security support of third-party components within the device's 8/ge optic.  2.5 Was a secure software development procloses, such as 150/RC 2794 or IEC \$2304, followed during product vest of the security of the components within the device's 8/ge optic.  2.40 RDMP-1 development?  Does the manufacturer relation as web page or other source of information as software progress, such as 150/RC 2794 or IEC \$2304, followed during product vest the device's for secure development practicacy?  2.40 RDMP-2 Does the manufacturer relation as web page or other source of information as software unapproached to the device's for secure development practicacy?  2.40 RDMP-3 updates?  2.40 RDMP-3 updates?  2.40 RDMP-0 third-party component end-of-life?  2.40 RDMP-0 third-party component end-of-life?  2.41 RDMP-1 third-party component end-of-life?  2.42 SOFTWARE BILL OF MATERIALS (SDMM)  2.43 Aspirace and jud selected Stockhilds as of the software components that are incorporated into the device being developed from the party origination. This section supports controls in the device being developed from the product available?  2.55 SBMM-2 is the SBMM follow a standard or common method or developed production of the software components identified?  2.55 SBMM-2 is the SBMM follow a standard or common method or developed production of the software components identified?  2.56 SBMM-2 is the section. This section supports controls in the software components identified?  2.57 SBMM-2 is the section numbers of the software components identified?  2.58 SBMM-2 is the section of the software components identified?  2.59 SBMM-2 is the section of the software components identified?  2.50 SBMM-2 is the section of the software components identified?  2.50 SBMM-2 is the section of the software components identified?  2.50 SBMM-2 is the section of the software components?  2.50 SBMM-2 is the section of the soft		A	В	С	D
ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE USE CYCLE (ROMP)  Manufacturer's plans for security support of third party components within the device's tile que's.  Was a secure software development process, such as ISO/IEC 27933 or IEC 25304, followed during product development?  Des the manufacturer evaluate bittid-service or product development?  Does the manufacturer relates bittid-service or product of the device for secure development pracess, such as ISO/IEC 27933 or IEC 25304, followed during product or better source of information an software support dates and updates?  248 80MP-2	2				
ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CVCILE (ROMP)  Attanufacturer's plans for security support of third-party components within the device's life cycle.  Was a socrue software development prostices?  246 ROMP-1 development?  Does the manufacturer evaluate third-party applications and software components included in the device for secure development prostices?  247 ROMP-2 the development prostices?  248 ROMP-3 updates?  Does the manufacturer maintain a web page or other source of information on software support dates and vest of the software support software installed on the device support of the software support software installed on the device support of the software support software installed on		FOJIFILIVI SONOSITĖ, INC	J.1.	010100	0000001, 2010
DEVICE LIFE CYCLE (ROMP)  Manufacturer's plans for executive support of third- party components within the device's life cycle.  Was a secrue software development process, such as ISONICE 2708 or IEC 62304, followed during product  Does the manufacturer evaluate third-party applications and software components included in the device for secure development practice?  Does the manufacturer evaluate third-party applications and software components included in the device for secure development practice?  Does the manufacturer maintain a web page or other source of information on software support distes and Yes  ADMP-2  Does the manufacturer development practice?  Does the manufacturer hands a web page or other source of information on software support distes and Yes  ADMP-3  Does the manufacturer hands a web page or other source of information on software support distes and Yes  Does the manufacturer hands a web page or other source of information on software support distes and Yes  Does the manufacturer maintain a web page or other source of information on software support distes and Yes  SOMM-2 third party componence that on the plan for managing Yes  Does the familiar third party componence that on the software development of the software deve	3				
Monufacturer's plans for security support of third- party components which the device's life cycle.  Was a secure software development process, such as isOnEC 27934 or ICC 62304, followed during product development?  Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?  AB RDMP-2 the device of secure development practices?  Does the manufacturer within a web page or other source of information on software support disters and updates?  Does the manufacturer bear a plan for managing third party component on development practices?  Post of information on software support disters and updates?  Software BitL OF MATERIALS (SBM) A Software BitL OF MATERIALS (SBM) A Software BitL OF MATERIALS (SBM) A Software components that are incorporated into the device being described for the upprace of operational security planning by the healthcare delivery organization. This section supports controls in the device being described for the upprace of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.  Section SBMO-1. Is the SBM follow a standard or common method in describing offorware components identified? Yes SBMO-2. Are the device includes a command or process method avelopenelymmulaturers of the software components identified? Are the ordiverse process for the SBM?  Are the software components identified? Are the device process for the SBM?  SBMO-2. Are the device includes a command or process method available to generate a list of software components identified? Are the device employ any mechanism for yes SBMO-2. SBMO-3. SBMO-4. Is the device employ any mechanism for yes SBMO-3. SBMO-4. Is the device employ any mechanism for yes SBMO-3. SBMO-3. Individual published to generate a list of software components installed on the device. SBMO-3. SBMO-3. Individual published process for the SBMO-7. Yes SBMO-3. SBMO-3. Individual published process for the SBMO-7. Yes SBMO-7. SBMO			ROADMAP FOR THIRD PARTY COMPONENTS IN		
Manufacturer's plans for security support of third- party components within the device's life cycle.  Was a secure software development process, such as isO/IEC 27034 or IEC 2304, followed during product development?  Does the manufacturer evaluate third-party applications and software components included in the device for secure development practicos?  Does the manufacturer maintain a web page or other source of information in a software support dates and updates?  Does the manufacturer maintain a web page or other source of information in a software support dates and updates?  Does the manufacturer have a plan for managing  Ves  Post the manufacturer have a plan for managing  Ves  SOFTWARE BILL OF MATERIALS (SBM)  A Software BILL OF MATERIALS (SBM)  A Software components that are incorporated into the software components that are incorporated into the device being described for the purpose of operancenal security planning by the healthcare delivery organization. This section supports controls in the BILL OF MATERIALS (SBM)  A Software BILL OF MATERIALS (SBM)  A Software components that are incorporated into the device being described for the purpose of operancenal security planning by the healthcare delivery organization. This section supports controls in the BILL OF MATERIALS (SBM)  2253 SBOM-1 is the SBM follow a standard or common method in describing offorware components? Ves  2254 SBOM-2 and the software components? Ves  SBOM-2 and the developer/manufacturers of the software  226 SBOM-2 and the software components identified? Ves  SBOM-2 and the software components identified? Ves  SBOM-2 and the software components identified? Ves  Does the device include a command or process method available to operance a list of software  Components identified?  Yes  SBOM-2 and the software components for software  Does the device include a command or process method available to operance a list of software  Components included on the device?  Yes  SBOM-2 and industry standards?  Yes  SBOM-2 before the device encloved	244				
Was accure software device size (species)					
A Springer Bird Market Bull of Mar			Manufacturer's plans for security support of third-		
Was a secure software development process, such as   SO/RE 2294 or IEEE 2330, followed during product   Yes   Does the manufacturer evaluate third-party   Yes   Does the manufacturer manuf	245				
Does the manufacturer evaluate bird-party ves paplications and software components included in the device for secure development practices?  Does the manufacturer maintaina web map or other source of information on software support dates and updates?  248 RDMP-3 updates?  Does the manufacturer have a plan for managing https://www.sonostle.com/support/sond-product-retirement-schedule  259 Does the manufacturer have a plan for managing https://www.sonostle.com/support/sond-product-retirement-schedule  250 SOFTWARE BILL OF MATERIALS (SBM)  A Software Bill of Material (SBM) lists oil 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 RDMM section.  253 SBOM-1 Is the SBM for this product available? Ves ——  254 SBOM-1 Is the SBM for this product available? Ves ——  255 SBOM-2 method in describing software components? Ves ——  256 SBOM-2.1 Are the software components identified? Ves ——  Are the device bedeepers/manufacturers of the software components identified? Ves ——  257 Are the software components identified? Ves ——  258 SBOM-2.3 components dentified? Ves ——  259 SBOM-2.4 Are any additional descriptive elements identified? Ves ——  260 SBOM-3 components sidentified? Ves ——  261 SBOM-4 is the remajor version numbers of the software components identified? Ves ——  262 SSOM-3 components identified? Ves ——  263 SSOM-4 is there are update process for the SBOM? Ves ——  264 The device include a command or process method available to generate a list of software components identified? Ves ——  265 SSOM-3 components installed on the device? Ves ——  266 SSOM-3 components installed on the device? Ves ——  267 SAHD-3 SYSTEM AND APPLICATION HARDENING (SAHD)  268 SAPD-1 industy standrais? Ves ——  269 SAHD-3 Software integrity checking, digital signature, etc.) to ensure the installed on standracturer- ves boot up one the device employ any mechanism for System and Integerity checkin					
Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices? Yes Does the manufacturer maintain a web page or other source of information on software support dates and yupitates?  AMBMP-3 Updates? Yes Does the manufacturer have a plan for managing with the party component end-of-life? Yes product-retirement-schedule					
### Applications and software components included in Service for secure development practices?  ### Applications and software womponents included in Service for secure development practices?  ### Applications and software womponents are plan for managing third-party component end-of-life?  ### Applications and software uponents are plan for managing third-party component end-of-life?  ### Applications and software aplan for managing third-party component and-of-life?  ### Applications and software aplan for managing third-party component software upone of percentions are plan for managing third-party components for the software components for the incorporated into the device being discribed for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the ROMP section.  #### Applications are software components. This section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components. The section supports controls in the ROMP section.  #### Applications are software components identified?  #### Applications are software components identified?  #### Applications are software components identified?  #### Does the device include a command or process method available to generate all sof software components identified?  #### Applications are software includes are software components identified?  #### Applications are software includes are	246	RDMP-1	development?	Yes	
applications and software components included in source of the device for secure development practices?  248 RDMP-3 Does the manufacturer maintain a web page or other source of information on software support dates and updates?  259 Does the manufacturer have a plan for managing third-party component end-of-life? Yes product-retirement-schedule  250 Yes  251 SOFTWARE BILL OF MATERIALS (SBOM)  252 SOFTWARE BILL OF MATERIALS (SBOM)  253 A Software Bill of Material (SBOM) Issue of the software components for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the software components for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the ROMP section.  254 SBOM-1 Is the SBoM for this product available? Yes  255 SBOM-2 Are the developers' manufacturers of the software components demified?  256 SBOM-2.1 Are the offware components identified? Yes  257 SBOM-2.2 Are the major resion numbers of the software components demified?  258 SBOM-2.3 Are the major resion numbers of the software components demified?  259 SBOM-2.4 Are any additional descriptive elements identified? Yes  260 SBOM-2.5 Are any additional descriptive elements identified?  260 SBOM-3 components identified?  260 SBOM-3 components identified?  261 SBOM-4 is the major resion numbers of the software components with any industry standards?  262 SBOM-3 components identified?  263 SBOM-3 components identified?  264 Yes  265 SBOM-4 is the even update process or the software components or the device and the device of the software components identified?  266 SBOM-3 components identified?  267 SBOM-4 is the even update process or the software components identified?  268 SBOM-3 components identified?  269 SBOM-3 components identified?  270 SBOM-4 is the even update process for the software components identified?  270 SBOM-4 is the even update process for the software intensity checking is perform bot up on the software intensi			Donath manufacture in the state of		
Bost					
Does the manufacturer maintain a web page or other source of information on software support dates and updates?  ROMIP-3  Does the manufacturer have a plan for managing third-party component end of-life?  Yes  PSS  SOFTWARE BILL OF MATERIALS (SBOM)  A Software Bill of Material (SBOM) is a lift the software components that ore increptored into the device being described for the pumpse of operational security planning by the healthcare definery organization. This section supports controls in the ROMP section.  ROMP section.  253  SBOM-1  SBOM-2  SBOM-2  Are the software components identified?  Does the SboM follow a standard or common  Web SBOM-2  Are the software components? Yes  SBOM-2  Are the software components? Yes  SBOM-2  Are the software components (sentified?  Are the major version numbers of the software components? Yes  SBOM-2  Are any additional descriptive elements identified?  Does the device include a command of process method available to generate a list of software components included to the device with the software components included to the device of the software components included to software components included to software components included to software components included to t	247	RDMP-2		Yes	
Source of information on software support dates and updates?   Ves	L-11				
ROMP-3   Updates?   Ves			· -		
RDMP-4   third-party component end-of-life?   Yes	248	RDMP-3		Yes	_
SOFTWARE BILL OF MATERIALS (SBOM)   Software Sill of Material (SBOM)   Stat 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.			Does the manufacturer have a plan for managing		https://www.sonosite.com/support/sonosite-
SOFTWARE BILL OF MATERIALS (SboM)  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.  SSOM-2 Is the SBoM for this product available?  Yes  Does the SBoM follow a standard or common mended in describing software components?  Wes  SBOM-2.1 Are the software components identified?  Are the device prefrom software integrity checking is perform boot up  SBOM-2.2 components identified?  Are the major version numbers of the software components identified?  Yes  Are the major version numbers of the software components identified?  SBOM-2.3 components identified?  Are any additional descriptive elements identified? Yes  Does the device include a command or process method available to generate a list of software components identified?  SBOM-3 is there an update process for the SBOM?  SSOM-4 is there an update process for the SBOM?  SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and molware.  Is the device received any cybersecurity certifications?  Does the device received any cybersecurity certifications?  Does the device received any cybersecurity certifications?  SAHD-1 industry standards?  Yes  SAHD-3 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed offware in simulacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed offware is manufacturer-authorized?  Can the owner/operator perform software integrity checking is perform boot up  Can the owner/operator perform software integrity checking is perform boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	249	RDMP-4	third-party component end-of-life?	Yes	product-retirement-schedule
SOFTWARE BILL OF MATERIALS (SBOM)   Stat 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.				Yes	
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.  253   SBOM-1   Is the SBoM for this product available?   Yes			COSTWARE DUL OF ALATERIANS (CO. CC.)		
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.  253 SBOM-1 Is the SBOM for this product available? Yes Does the SBOM follow a standard or common whe method in describing software components? Yes Are the developers/manufacturers of the software components identified? Yes Carbon Are the major variety of the software components identified? Yes Are the developers/manufacturers of the software Yes SBOM-2.1 Are the major variety on the software Components identified? Yes Carbon Are the major variety of the software Yes SBOM-2.2 Are the developers/manufacturers of the software Yes SBOM-2.3 Are any additional descriptive elements identified? Yes Carbon SBOM-3 Components identified? Yes Carbon SBOM-4 Is there any quade for process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is there any quade process for the SBOM? Yes SBOM-4 Is the device Process for the SBOM? Yes SBOM-4 Is the device Process for the SBOM? Yes SBOM-4 Is the device Process for the SBOM? Yes SBOM-4 Is the device Process for the SBOM? Yes SBOM-4 Is the device Process for the SBOM? Yes SBOM-4	252				
dewice being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.  254   \$80.M-1   Is the \$80.M for this product available? Yes					
security planning by the healthcare delivery organization. This section supports controls in the RDMP section.  253 SBOM-1 Is the SBOM for this product available?  254 SBOM-2 method in describing software components?  255 SBOM-2.1 Are the software components identified?  257 SBOM-2.2 components identified?  258 SBOM-2.1 Are the major version numbers of the software components identified?  259 SBOM-2.2 components identified?  259 SBOM-2.3 Are the major version numbers of the software components identified?  259 SBOM-2.4 Are any additional descriptive elements identified?  250 SBOM-2.4 Are any additional descriptive elements identified?  260 SBOM-3 components installed on the device?  261 SBOM-4 Is there an update process method available to generate a list of software components installed on the device?  261 SBOM-4 Is there an update process for the SBOM?  262 SSYSTEM AND APPLICATION HARDENING (SAHD)  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 The device's inherent resistance to cyber attacks and molware.  265 SAHD-1 Industry standards?  266 SAHD-2 certifications?  267 SAHD-3 Software integrity checking  268 SAHD-3 Software integrity checking  269 SAHD-3.1 Does the device employ any mechanism for system and Integerity checking is perform boot up  269 SAHD-3.1 Ones the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  269 SAHD-3.2 Can the owner/operator perform software integrity checking to perform boot up  270 SAHD-3 authorized updates?  280 Can the owner/operator perform software integrity check (e.g., verify that the system has not been modified or tampered with!?)  270 SAHD-4 modified or tampered with!? No					
253   SBOM-1   Is the SBoM for this product available?   Yes					
253   ROMP-section.   Is the SBoM for this product available?   Yes			,, , , , , , , , , , , , , , , , , , , ,		
254   SBOM-1   Is the SBOM follow a standard or common method in describing software components?   Yes	253				
255 S80M-2.1 Are the software components? Yes 256 S80M-2.1 Are the software components identified? Yes 257 S80M-2.2 components identified? Yes 258 S80M-2.3 Are the developers/manufacturers of the software 259 S80M-2.3 Are the major version numbers of the software 259 S80M-2.4 Are any additional descriptive elements identified? Yes 259 S80M-2.4 Are any additional descriptive elements identified? Yes 260 S80M-3 Des the device include a command or process method available to generate a list of software 261 S80M-4 Is there an update process for the S80M? Yes 261 S80M-4 Is there an update process for the S80M? Yes 263 SYSTEM AND APPLICATION HARDENING (SAHD) 264 SAHD-1 Industry standards? Yes 265 SAHD-1 Industry standards? Yes 266 SAHD-2 certifications? Yes 267 SAHD-3 Software integrity checking is perform boot up 268 SAHD-3 Software integrity checking is perform authorized? Yes 269 SAHD-3.1 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software integrity checking (signature, etc.) to ensure the installed software integrity checking (signature, etc.) to ensure the installed software integrity checking (signature, etc.) to ensure the installed software integrity checking (signature, etc.) to ensure the installed software integrity checking (signature, etc.) to ensure the installed software integrity checking is perform boot up 269 SAHD-3.1 authorized? Can the owner/operator perform software integrity checking is perform boot up 269 SAHD-3.2 SAHD-3.4 can the owner/operator perform software integrity checking is perform boot up		SBOM-1		Yes	_
256 S80M-2.1 Are the software components identified?  257 S80M-2.2 Components identified?  258 S80M-2.3 Components identified?  259 S80M-2.4 Are any additional descriptive elements identified?  259 S80M-2.4 Are any additional descriptive elements identified?  260 S80M-3 components installed on the device?  261 S80M-3 components installed on the device?  262 Yes  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 SAHD-1 Industry standards?  265 SAHD-1 Industry standards?  266 SAHD-2 certifications?  267 SAHD-3 Software integrity checking is perform boot up  268 SAHD-3.1 Does the device employ any mechanisms (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software integrity checks in sperform authorized years of the software integrity checks in sperform software integrity check			Does the SBoM follow a standard or common		
Are the developers/manufacturers of the software components identified? Yes  258 SBOM-2.2 Are the major version numbers of the software components identified? Yes  259 SBOM-2.4 Are any additional descriptive elements identified? Yes  260 SBOM-3 Components identified? Yes  261 SBOM-4 Is there an update process for the SBOM? Yes  262 SSOM-4 Is there an update process for the SBOM? Yes  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 SAHD-1 Is the device hardened in accordance with any industry standards? Yes  265 SAHD-1 Industry standards? Yes  266 SAHD-2 certifications? Yes  267 SAHD-3 Software integrity checking Yes  268 SAHD-3 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  269 SAHD-3.2 AHD-4 SAHD-4 Can the owner/operator perform software integrity checking is perform authorized? Yes  260 SAHD-4 Can the owner/operator perform software integrity checking is perform authorized? Yes  269 SAHD-3.2 Can the owner/operator perform software integrity checking is perform authorized? Yes  269 SAHD-3.4 Can the owner/operator perform software integrity checking is perform authorized? Yes  270 SAHD-4 modified or tampered with!? No					_
257 SBOM-2.2 components identified?  258 SBOM-2.3 components identified?  259 SBOM-2.4 Are any additional descriptive elements identified?  259 SBOM-2.4 Are any additional descriptive elements identified?  260 SBOM-3 components intelled on the device?  261 SBOM-4 Is there an update process for the SBOM?  262 SSOM-4 Is there an update process for the SBOM?  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 "The device's inherent resistance to cyber attacks and malware.  265 SAHD-1 is the device hardened in accordance with any industry standards?  266 SAHD-2 certifications?  267 SAHD-3 Does the device employ any mechanisms for Software integrity checking  268 SAHD-3.1 authorized?  269 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  269 SAHD-3.2 authorized?  260 SAHD-3.2 Can the owner/operator perform software integrity checking is perform boot up  260 SAHD-3.4 can be manufacturer-authorized play any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software updates are the manufacturer-authorized play any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software updates are the manufacturer-authorized updates?  269 SAHD-3.2 Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with!)?  270 SAHD-4 modified or tampered with!?	256	SBOM-2.1	,	Yes	-
Are the major version numbers of the software components identified?  259 SBOM-2.4 Are any additional descriptive elements identified?  260 SBOM-3 method available to generate a list of software components installed on the device?  261 SBOM-4 Is there an update process for the SBOM?  263 SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and malware.  264 malware.  265 SAHD-1 industry standards?  Has the device received any cybersecurity certifications?  266 SAHD-2 certifications?  Does the device employ any mechanism for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  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?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates?  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	257	SDOM 2.2		Vos	
258 SBOM-2.3 components identified?  259 SBOM-2.4 Are any additional descriptive elements identified?  Does the device include a command or process method available to generate a list of software components installed on the device?  260 SBOM-3 components installed on the device?  261 SBOM-4 is there an update process for the SBOM?  262 SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and malware.  263 SYSTEM evice hardened in accordance with any industry standards?  15 the device hardened in accordance with any industry standards?  265 SAHD-1 is the device received any cybersecurity  266 SAHD-2 certifications?  Does the device employ any mechanisms for software integrity checking  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  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?  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?  SAHD-3.2 authorized updates?  Can the owner/operator perform software integrity check in the system has not been modified or tampered with)?  No	231	JUOIVI-7.7	•	165	
Are any additional descriptive elements identified?  Does the device include a command or process method available to generate a list of software components installed on the device?  Yes	258	SBOM-2.3		Yes	
Does the device include a command or process method available to generate a list of software components installed on the device? Yes  261 SBOM-4 Is there an update process for the SBOM? Yes  262 SYSTEM AND APPLICATION HARDENING (SAHD)  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 The device's inherent resistance to cyber attacks and mailware.  265 SAHD-1 Is the device hardened in accordance with any industry standards? Yes  266 SAHD-2 certifications? Yes Security tested organization  267 SAHD-3 software integrity checking Software integrity checking is perform boot up  268 SAHD-3.1 authorized?  269 SAHD-3.1 authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  269 SAHD-3.2 authorized updates?  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No		-			
method available to generate a list of software components installed on the device?  261  SBOM-4  Is there an update process for the SBoM?  263  SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any industry standards?  Asth D-1  Has the device received any cybersecurity certifications?  Does the device employ any mechanisms for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  SAHD-3.2  Method available to generate a list of software integrity checking?  Yes  —————————————————————————————————	259	SBOM-2.4	Are any additional descriptive elements identified?	Yes	_
260 SBOM-3 components installed on the device? Yes					
261 SBOM-4 Is there an update process for the SBOM? Yes  262 SYSTEM AND APPLICATION HARDENING (SAHD)  263 SYSTEM AND APPLICATION HARDENING (SAHD)  264 "The device's inherent resistance to cyber attacks and malware.  265 SAHD-1 Is the device hardened in accordance with any industry standards? Yes  266 SAHD-2 certifications? Yes Security tested organization  267 Does the device employ any mechanisms for System and Integerity checking is perform software integrity checking (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized? Yes boot up  268 SAHD-3.1 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software updates are the manufacturer-authorized updates? Yes  269 SAHD-3.2 authorized updates? Yes  270 SAHD-4 Modified or tampered with)? No	0.55		· ·		
262  263  SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any industry standards?  Has the device received any cybersecurity  certifications?  Yes  266  SAHD-2  Certifications?  Does the device employ any mechanisms for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-yes  SAHD-3.1  SAHD-3.2  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	-				_
SYSTEM AND APPLICATION HARDENING (SAHD)  The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any  265 SAHD-1 industry standards?  Has the device received any cybersecurity  266 SAHD-2 certifications?  Does the device employ any mechanisms for software integrity checking is perform boot up  SAHD-3.1 authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  SAHD-3.1 authorized?  Yes  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 perform software integrity checking is perform boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	-	JDUIVI-4	is there all update process for the SBOWL!	ies	
The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any industry standards?  Has the device received any cybersecurity  266 SAHD-1 Has the device received any cybersecurity  267 SAHD-3 Does the device employ any mechanism for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-  268 SAHD-3.1 authorized? Yes boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-  269 SAHD-3.2 authorized updates?  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	۲۵۲				
The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any industry standards?  Has the device received any cybersecurity  266 SAHD-1 Has the device received any cybersecurity  267 SAHD-3 Does the device employ any mechanism for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-  268 SAHD-3.1 authorized? Yes boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-  269 SAHD-3.2 authorized updates?  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	263		SYSTEM AND APPLICATION HARDENING (SAHD)		
264 malware.  1s the device hardened in accordance with any industry standards?  265 SAHD-1 Has the device received any cybersecurity certifications?  266 SAHD-2 certifications?  267 SAHD-3 Does the device employ any mechanisms for software integrity checking is perform boot up  268 SAHD-3 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  268 SAHD-3.1 Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software updates are the manufacturer-authorized updates?  269 SAHD-3.2 authorized updates?  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No					
Is the device hardened in accordance with any industry standards?  Has the device received any cybersecurity certifications? Yes Security tested organization  Does the device employ any mechanisms for System and Integerity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?  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 specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?  SAHD-3.2 SAHD-3.2 SAHD-4 modified or tampered with)?  No	264		•		
Has the device received any cybersecurity  certifications?  Does the device employ any mechanisms for software integrity checking  SAHD-3  SAHD-3  SAHD-3  SAHD-3  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- boot up  SAHD-3.1  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksums, digital signature, etc.)  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No					
266 SAHD-2 certifications? Yes Security tested organization  Does the device employ any mechanisms for software integrity checking  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-  268 SAHD-3.1 authorized?  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the obot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksims, digital signature, e	265	SAHD-1		Yes	_
Does the device employ any mechanisms for software integrity checking is perform boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-specific hash key, checksums, digital signature, etc.)  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.)  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-specific hash key, checksums, digital signature, etc.)  System and Integerity checking is perform software updates are the manufacturer-specific hash key, checksims, digital signature, etc.)  To ensure the software updates are the manufacturer-specific hash key, checking is perform software integrity checking is perform boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	255	CALID 3			This device has been tested by 3rd Party Cyber
267 SAHD-3 software integrity checking Yes boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- 268 SAHD-3.1 authorized? Yes boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No	266	SAHD-2		Yes	
Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- 268 SAHD-3.1 authorized? Yes boot up  Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No	267	SAHD-3		Yes	
specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- 268 SAHD-3.1 authorized? Yes boot up  Does the device employ any mechanism (e.g., release- specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No	201	5,110 5	· , ·		500t dp
to ensure the installed software is manufacturer- 268 SAHD-3.1 Does the device employ any mechanism (e.g., release- specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No			, , ,		
Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No					System and Integerity checking is performed during
specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No	268	SAHD-3.1			boot up
to ensure the software updates are the manufacturer- 269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No	]		, , ,		
269 SAHD-3.2 authorized updates? Yes boot up  Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? No			, , , , , , , , , , , , , , , , , , , ,		Contains and later and lat
Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  No	260	CVIID 3 3			System and Integerity checking is performed during
checks (i.e., verify that the system has not been modified or tampered with)?  No	269 :	JAΠU-3.2	authorized updates?	162	υσοι αρ
checks (i.e., verify that the system has not been modified or tampered with)?  No			Can the owner/operator perform software integrity		
270 SAHD-4 modified or tampered with)? No					
	270	SAHD-4	,	No	
is the system configurable to allow the			Is the system configurable to allow the		
implementation of file-level, patient level, or other			_		
271 SAHD-5 types of access controls? Yes	271	SAHD-5	types of access controls?	Yes	_
	<u> </u>				
272 SAHD-5.1 Does the device provide role-based access controls? Yes	272	SAHD-5.1	Does the device provide role-based access controls?	Yes	

	А	В	С	D
2	FUJIFILM SonoSite, Inc	SII	D19108	October, 2019
3				
		Are any system or user accounts restricted or		
273	SAHD-6	disabled by the manufacturer at system delivery?	Yes	
		Are any system or user accounts configurable by the		<del>_</del>
274	SAHD-6.1	end user after initial configuration?	Yes	
		Does this include restricting certain system or user		
		accounts, such as service technicians, to least		
275	SAHD-6.2	privileged access?	Yes	_
		Are all shared resources (e.g., file shares) which are not required for the intended use of the device		
276	SAHD-7	disabled?	Yes	
		Are all communication ports and protocols that are		_
		not required for the intended use of the device		
277	SAHD-8	disabled?	Yes	_
		Are all services (e.g., telnet, file transfer protocol		
		[FTP], internet information server [IIS], etc.), which		
278	SAHD-9	are not required for the intended use of the device deleted/disabled?	Yes	
270	JAND-3	Are all applications (COTS applications as well as OS-	ies	.—
		included applications, e.g., MS Internet Explorer, etc.)		
		which are not required for the intended use of the		
279	SAHD-10	device deleted/disabled?	Yes	_
		Can the device prohibit boot from uncontrolled or		
280	SAHD-11	removable media (i.e., a source other than an internal	Voc	
200	JAND-11	drive or memory component)?	Yes	-
		Can unauthorized software or hardware be installed		
281	SAHD-12	on the device without the use of physical tools?	No	_
		Does the product documentation include information		
282	SAHD-13	on operational network security scanning by users?	No	_
202	CALID 14	Can the device be hardened beyond the default	No	
283	SAHD-14	provided state?  Are instructions available from vendor for increased	No	_
284	SAHD-14.1	hardening?	NA	
		Can the system prevent access to BIOS or other		
285	SHAD-15	bootloaders during boot?	Yes	
200	CALID 4C	Have additional hardening methods not included in	V	
286 287	SAHD-16	2.3.19 been used to harden the device?	Yes	
288				
289		SECURITY GUIDANCE (SGUD)		
		Availability of security guidance for operator and		
		administrator of the device and manufacturer sales		
290		and service.		
201	SCUP 4	Does the device include security documentation for		
291	SGUD-1	the owner/operator?	Yes	_
		Does the device have the capability, and provide instructions, for the permanent deletion of data from		
292	SGUD-2	the device or media?	Yes	
293	SGUD-3	Are all access accounts documented?	Yes	_
		Can the owner/operator manage password control		
294	SGUD-3.1	for all accounts?	Yes	_
		Does the product include documentation on		
295	SGUD-4	recommended compensating controls for the device?	Yes	
296	-	, and the device.		
297				
		HEALTH DATA STORAGE CONFIDENTIALITY		
298		(STCF)		
		The ability of the device to ensure unauthorized		
		access does not compromise the integrity and confidentiality of personally identifiable information		
299		stored on the device or removable media.		
$\overline{}$	STCF-1	Can the device encrypt data at rest?	Yes	_
-	STCF-1.1	Is all data encrypted or otherwise protected?	Yes	

	А	В	С	D
2	FUJIFILM SonoSite, Inc		D19108	October, 2019
3	i OJIFILIVI SUHOSITE, INC	, <del></del>	223100	000001, 2015
3		Is the data encryption capability configured by		
302	STCF-1.2	default?	Yes	
		Are instructions available to the customer to		
303	STCF-1.3	configure encryption?	NA	Device is already configured
304	STCF-2	Can the encryption keys be changed or configured?	No	
- 554	<u>-</u>	Is the data stored in a database located on the	***	
305	STCF-3	device?	Yes	_
		Is the data stored in a database external to the		
306 307	STCF-4	device?	Yes	_
308				
309		TRANSMISSION CONFIDENTIALITY (TXCF)		
		, ,		
		The ability of the device to ensure the confidentiality		
310		of transmitted personally identifiable information.		
		Can personally identifiable information be		
311	TXCF-1	transmitted only via a point-to-point dedicated cable?	No	
		and the second s	-	
		Is personally identifiable information encrypted prior		
312	TXCF-2	to transmission via a network or removable media?	Yes	
313	TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Vos	
313	1747-2.1	comigure end yphon ophons:	Yes	-
		Is personally identifiable information transmission		
314	TXCF-3	restricted to a fixed list of network destinations?	Yes	_
315	TXCF-4	Are connections limited to authenticated systems?	Yes	_
		Are secure transmission methods		
316	TXCF-5		Yes	
317		, , , , , , , , , , , , , , , , , , , ,		
318				
319		TRANSMISSION INTEGRITY (TXIG)		
220		The ability of the device to ensure the integrity of		
320		transmitted data.		Customers can order an optional FIPS 140-2
		Does the device support any mechanism (e.g., digital		validated WiFi module to ensure data confidentiality
		signatures) intended to ensure data is not modified		between the system and
321	TXIG-1	during transmission?	Yes	their access point.
222	TVIG-2	Does the device include multiple sub-components	No	
322 323	TXIG-2	connected by external cables?	No	
324				
325		REMOTE SERVICE (RMOT)		
		-		
		Remote service refers to all kinds of device		
336		maintenance activities performed by a service person		
326		via network or other remote connection.		The device does not have any remote service
		Does the device permit remote service connections		capability. All servicing requires physical access to
327	RMOT-1	for device analysis or repair?	No	the device
		Does the device allow the owner/operator to		
330	DMOT 1 1	initiative remote service sessions for device analysis	N/A	
328	RMOT-1.1	or repair? Is there an indicator for an enabled and active remote	NA	_
329	RMOT-1.2	session?	NA	
		Can patient data be accessed or viewed from the		
330	RMOT-1.3	device during the remote session?	NA	_
224	DNAOT 3	Does the device permit or use remote service	N/A	
331	RMOT-2	connections for predictive maintenance data?  Does the device have any other remotely accessible	NA	_
		functionality (e.g. software updates, remote		
332	RMOT-3	training)?	No	_
333				
334				
335 336				
		OTHER SECURITY CONSIDERATIONS (OTHR)		
337		OTHER SECORITY CONSIDERATIONS (OTHR)		

	Α	В	С	D
2	FUJIFILM SonoSite, Inc	SII	D19108	October, 2019
3				
338		NONE		
339				
340		Notes:		
341				
		Example note. Please keep individual notes to one		
		cell. Please use separate notes for separate		
342	Note 1	information		