Manufacturer Disclosure Statement for Medical Device Security -- MDS2

BBImaging

N/A

N/A

1-Mar-2022

Question ID	Question		See note
DOC-1	Manufacturer Name	BBImaging	
2001		Telescan Computer and	_
DOC-2	Device Description	Software Suite	
DOC-3	Device Model	N/A	_
DOC-4	Document ID	N/A	_
DOC-5	Manufacturer Contact Information	info@bbimaging.net	_
		Upload glucose	_
	Intended use of device in network-connected	measurement history to	
DOC-6	environment:	patient records	
DOC-7	Document Release Date	2022-03-01	_
	Coordinated Vulnerability Disclosure: Does the		_
	manufacturer have a vulnerability disclosure program for		
DOC-8	this device?	No	
2000	ISAO: Is the manufacturer part of an Information Sharing		_
DOC-9	and Analysis Organization?	No	
	Diagram: Is a network or data flow diagram available that		_
	indicates connections to other system components or		
DOC-10	expected external resources?	Yes	See Note 1
20010	SaMD: Is the device Software as a Medical Device (i.e.		
DOC-11	software-only, no hardware)?	See Notes	
DOC-11.1	Does the SaMD contain an operating system?	Yes	_
	Does the SaMD rely on an owner/operator provided		_
DOC-11.2	operating system?	No	
DOC-11.3	Is the SaMD hosted by the manufacturer?	Yes	_
DOC-11.4	Is the SaMD hosted by the customer?	Yes	
Yes, No,			
N/A, or			
See Note			Note#
	MANAGEMENT OF PERSONALLY IDENTIFIABLE		
	INFORMATION		
	Can this device display, transmit, store, or modify		
	personally identifiable information (e.g. electronic		
MPII-1	Protected Health Information (ePHI))?	Yes	_
	Does the device maintain personally identifiable		
MPII-2	information?	Yes	
	Does the device maintain personally identifiable		
	information temporarily in volatile memory (i.e., until		
MPII-2.1	cleared by power-off or reset)?	Yes	_
	Does the device store personally identifiable information		
MPII-2.2	persistently on internal media?	No	
	Is personally identifiable information preserved in the		
MPII-2.3	device's non-volatile memory until explicitly erased?	No	
	Does the device store personally identifiable information		
MPII-2.4	in a database?	Yes	_

BBImaging	N/A	N/A	1-Mar-2022
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	_
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	No	_
	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or	-	_
MPII-2.8	customer retention)? 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	Yes _	_
MPII-2.9	storage location)? Does the device have mechanisms used for the transmitting, importing/exporting of personally	No	
MPII-3	identifiable information? Does the device display personally identifiable	Yes _	_
MPII-3.1 MPII-3.2	information (e.g., video display, etc.)? Does the device generate hardcopy reports or images containing personally identifiable information?	Yes 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, CF/SD card,	· · · · ·	_
MPII-3.3	memory stick, etc.)? Does the device transmit/receive or import/export	No _	_
MPII-3.4	personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)? Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45,	Yes	-
MPII-3.5	fiber optic, etc.)?	Yes _	_
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	Yes	_
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)? Does the device import personally identifiable	Yes	_
MPII-3.8	information via scanning a document?	No	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol? Does the device use any other mechanism to transmit,	No	
MPII-3.10	import or export personally identifiable information?	No	

	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.
	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password
ALOF-1	protected screen saver)?
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?

Yes	_
Yes	_

AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the device.

	Can the medical device create additional audit logs or		
AUDT-1	reports beyond standard operating system logs?	Yes	
AUDT-1.1	Does the audit log record a USER ID?	Yes	
	Does other personally identifiable information exist in		
AUDT-1.2	the audit trail?	No	
	Are events recorded in an audit log? If yes indicate which		
	Are events recorded in an audit log? If yes, indicate which		
AUDT-2	of the following events are recorded in the audit log:	Yes	
AUDT-2.1	Successful login/logout attempts?	Yes	
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	
AUDT-2.3	Modification of user privileges?	Yes	
AUDT-2.4	Creation/modification/deletion of users?	Yes	
AUD1 2.4		<u> </u>	
AUDT-2.5	Procentation of clinical or DU data (o.g. display, print)?	No	
AUD1-2.5	Presentation of clinical or PII data (e.g. display, print)?	NO	
AUDT-2.6	Creation/modification/deletion of data?	No	
	Import/export of data from removable media (e.g. USB		
AUDT-2.7	drive, external hard drive, DVD)?	N/A	
	Receipt/transmission of data or commands over a		
AUDT-2.8	network or point-to-point connection?	No	
		_	
AUDT-2.8.1	Remote or on-site support?	No	
	Application Programming Interface (API) and similar		
		Vec	
AUDT-2.8.2	activity?	Yes	
	_	/.	
AUDT-2.9	Emergency access?	N/A	

BBImaging	N/A	N/A	1-Mar-2022
AUDT-2.10	Other events (e.g., software updates)?	Yes	
AUDT-2.11	Is the audit capability documented in more detail?	Yes	
	Can the owner/operator define or select which events are		
AUDT-3	recorded in the audit log?	Yes	
	Is a list of data attributes that are captured in the audit		
AUDT-4	log for an event available?	No	
AUDT-4.1	Does the audit log record date/time?	Yes	
	Can date and time be synchronized by Network Time		
AUDT-4.1.1	Protocol (NTP) or equivalent time source?	Yes	
AUDT-5	Can audit log content be exported?	No	
AUDT-5.1	Via physical media?	No	
	Via IHE Audit Trail and Node Authentication (ATNA)		
AUDT-5.2	profile to SIEM?	No	
	Via Other communications (e.g., external service device,		
AUDT-5.3	mobile applications)?	No	
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	Yes	
	Can audit logs be monitored/reviewed by		
AUDT-6	owner/operator?	Yes	
AUDT-7	Are audit logs protected from modification?	Yes	
AUDT-7.1	Are audit logs protected from access?	Yes	
AUDT-8	Can audit logs be analyzed by the device?	No	

AUTHORIZATION (AUTH)

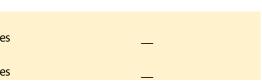
AUTH-1Does the device prevent access to unauthorized usersYesAUTH-1through user login requirements or other mechanism?YesCan the device be configured to use federated credentials management of users for authorization (e.g., LDAP,NoAUTH-1.1OAuth)?NoCan the customer push group policies to the device (e.g., Can the customer push group policies to the device (e.g., AUTH-1.2NoAUTH-1.2Active Directory)?NoAutrH-1.3policies required?YesAUTH-2'role' (e.g., user, administrator, and/or service, etc.)?YesAUTH-2'role' (e.g., user, administrator, and/or service, etc.)?YesCan the device owner/operator grant themselvesYes		The ability of the device to determine the authorization of users.	
Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP,AUTH-1.1OAuth)?NoCan the customer push group policies to the device (e.g., Can the customer push group policies to the device (e.g., AUTH-1.2NoAUTH-1.2Active Directory)?NoAUTH-1.3policies required? Can users be assigned different privilege levels based on Can users, administrator, and/or service, etc.)?YesAUTH-2'role' (e.g., user, administrator, and/or service, etc.)?Yes		Does the device prevent access to unauthorized users	
AUTH-1.1OAuth)? Can the customer push group policies to the device (e.g., Can the customer push group policies to the device (e.g., AUTH-1.2NoAUTH-1.2Active Directory)? Are any special groups, organizational units, or group AuTH-1.3NoAUTH-1.3policies required? Can users be assigned different privilege levels based on Can user, administrator, and/or service, etc.)?YesAUTH-2'role' (e.g., user, administrator, and/or service, etc.)?Yes	AUTH-1	through user login requirements or other mechanism?	Yes
AUTH-1.1OAuth)?No		Can the device be configured to use federated credentials	
Can the customer push group policies to the device (e.g., Image: Can the customer push group policies to the device (e.g., AUTH-1.2 Active Directory)? No Image: Can the customer push group policies to the device (e.g., AUTH-1.3 policies required? Yes Image: Can users be assigned different privilege levels based on AUTH-2 'role' (e.g., user, administrator, and/or service, etc.)? Yes Image: Can user Section Se		management of users for authorization (e.g., LDAP,	
AUTH-1.2 Active Directory)? No	AUTH-1.1	OAuth)?	No
Are any special groups, organizational units, or group Are any special groups, organizational units, or group AUTH-1.3 policies required? Yes Can users be assigned different privilege levels based on AUTH-2 AUTH-2 'role' (e.g., user, administrator, and/or service, etc.)? Yes		Can the customer push group policies to the device (e.g.,	
AUTH-1.3 policies required? Yes	AUTH-1.2	Active Directory)?	No
Can users be assigned different privilege levels based on AUTH-2 'role' (e.g., user, administrator, and/or service, etc.)? Yes		Are any special groups, organizational units, or group	
AUTH-2 'role' (e.g., user, administrator, and/or service, etc.)? Yes	AUTH-1.3	policies required?	Yes
Can the device owner/operator grant themselves	AUTH-2	'role' (e.g., user, administrator, and/or service, etc.)?	Yes
		Can the device owner/operator grant themselves	
unrestricted administrative privileges (e.g., access		unrestricted administrative privileges (e.g., access	
operating system or application via local root or		operating system or application via local root or	
AUTH-3 administrator account)? Yes	AUTH-3	administrator account)?	Yes
Does the device authorize or control all API access		Does the device authorize or control all API access	
AUTH-4 requests? Yes	AUTH-4	requests?	Yes

BBImaging	N/A	N/A	1-Mar-2022
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	N/A	
	CYBER SECURITY PRODUCT UPGRADES (CSUP) The ability of on-site service staff, remote service staff,		
	or authorized customer staff to install/upgrade device's security patches.		
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third- party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Νο	
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	N/A	
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	
	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the		
CSUP-3.4	manufacturer? Does the device contain Anti-Malware Software? If yes,	No	
CSUP-4	complete 4.1-4.4. Does the device documentation provide instructions for	Yes	
CSUP-4.1	owner/operator installation of patches or software updates?	Yes	
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	

BBImaging	N/A	N/A	1-Mar-2022
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes	
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security	Yes	
CSUP-5.4	updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	Yes	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote	Yes	
CSUP-6.3	installation of patches or software updates? Does the medical device manufacturer allow security	Yes	
CSUP-6.4	updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	N/A	
CSUP-8	Does the device perform automatic installation of software updates? Does the manufacturer have an approved list of third-	Yes	
CSUP-9	party software that can be installed on the device?	No	
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves? Does the system have mechanism in place to prevent	No	
CSUP-10.1	installation of unapproved software? Does the manufacturer have a process in place to assess	Yes	
CSUP-11 CSUP-11.1	device vulnerabilities and updates? Does the manufacturer provide customers with review and approval status of updates?	Yes	
CSUP-11.2	Is there an update review cycle for the device?	No	

EMRG-1

	The ability of the device to directly remove information that allows identification of a person.	
DIDT-1	Does the device provide an integral capability to de- identify personally identifiable information?	Ye
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Ye
	comply with the Dicowistanual u for de-identification:	ie.



DATA BACKUP AND DISASTER RECOVERY (DTBK)

	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.	
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	S
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	Y
DTBK-3	Does the device have an integral data backup capability to removable media?	Ν
DTBK-4	Does the device have an integral data backup capability to remote storage?	Ν
	Does the device have a backup capability for system configuration information, patch restoration, and	
DTBK-5	software restoration? Does the device provide the capability to check the	Ν
DTBK-6	integrity and authenticity of a backup?	Y

EMERGENCY ACCESS (EMRG)

The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information. Does the device incorporate an emergency access (i.e. "break-glass") feature?

No

N/A

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 nonauthorized manner and is from the originator.

1	See Notes	Note 2
•		
	Yes	_
	No	—
	No	
	No	
	Yes	

BBImaging	N/A	N/A	1-Mar-2022
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No	_
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID- 5)?	See Notes	See Note 3
	5):	Sections	Sectores

MALWARE DETECTION/PROTECTION (MLDP)

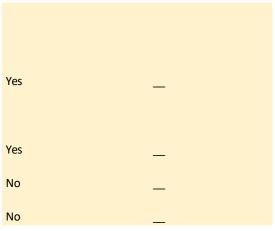
	The ability of the device to effectively prevent, detect and remove malicious software (malware).	
MLDP-1	Is the device capable of hosting executable software? Does the device support the use of anti-malware software	Yes
MLDP-2	(or other anti-malware mechanism)? Provide details or reference in notes.	Yes
MLDP-2.1	Does the device include anti-malware software by default?	Yes
MLDP-2.2	Does the device have anti-malware software available as an option?	N/A
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	Yes
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings? Does notification of malware detection occur in the	Yes
MLDP-2.5	device user interface? Can only manufacturer-authorized persons repair	Yes
MLDP-2.6 MLDP-2.7	systems when malware has been detected? Are malware notifications written to a log?	Yes No
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available? Does the device employ application whitelisting that	N/A
MLDP-4	restricts the software and services that are permitted to be run on the device?	Yes
MLDP-5	Does the device employ a host-based intrusion detection/prevention system? Can the host-based intrusion detection/prevention	Yes
MLDP-5.1	system be configured by the customer? Can a host-based intrusion detection/prevention system	Yes
MLDP-5.2	be installed by the customer?	Yes

es	
es	_
es	_
I/A	_
es	_
es	_
es	
es	
lo	
es	Purchase and Update on Windows
I/A	
es	_
es	_
es	_
es	<u> </u>

1-Mar-2022

NODE AUTHENTICATION (NAUT)

	The ability of the device to authenticate communication partners/nodes.
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?
	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a
NAUT-2	network connection white list)? Is the firewall ruleset documented and available for
NAUT-2.1	review? Does the device use certificate-based network
NAUT-3	connection authentication?



CONNECTIVITY CAPABILITIES (CONN)

All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.

CONN-1	Does the device have hardware connectivity capabilities?	Yes
CONN-1.1	Does the device support wireless connections?	Yes
CONN-1.1.1	Does the device support Wi-Fi?	Yes
CONN-1.1.2	Does the device support Bluetooth?	Yes
	Does the device support other wireless network	
CONN-1.1.3	connectivity (e.g. LTE, Zigbee, proprietary)?	No
	Does the device support other wireless connections (e.g.,	
CONN-1.1.4	custom RF controls, wireless detectors)?	No
CONN-1.2	Does the device support physical connections?	Yes
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes
CONN-1.2.2	Does the device have available USB ports?	Yes
	Does the device require, use, or support removable	
CONN-1.2.3	memory devices?	Yes
CONN-1.2.4	Does the device support other physical connectivity?	Yes
	Does the manufacturer provide a list of network ports	
	and protocols that are used or may be used on the	
CONN-2	device?	No
	Can the device communicate with other systems within	
CONN-3	the customer environment?	Yes
	Can the device communicate with other systems external	
CONN-4	to the customer environment (e.g., a service host)?	Yes
CONN-5	Does the device make or receive API calls?	Yes

es			
es			
es			
es			
о			
о			
es			
es			
es			
0			
es			
es			
es			
-			
0			
es			
es			
es			

BBImaging	N/A	N/A	1-Mar-2022
	Does the device require an internet connection for its		
CONN-6	intended use?	Yes	
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	
CONN-7.1	Is TLS configurable?	Yes	
	Does the device provide operator control functionality		
CONN-8	from a separate device (e.g., telemedicine)?	Yes	

PERSON AUTHENTICATION (PAUT)

	The ability to configure the device to authenticate users.	
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes
-	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active	
PAUT-2	Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a	No
PAUT-3	certain number of unsuccessful logon attempts?	Yes
	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the	
PAUT-4	documentation?	Yes
PAUT-5	Can all passwords be changed? Is the device configurable to enforce creation of user	Yes
PAUT-6	account passwords that meet established (organization specific) complexity rules?	Yes
PAUT-7	Does the device support account passwords that expire periodically?	Yes
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
PAUT-11	Does the device support biometric controls? Does the device support physical tokens (e.g. badge	No
PAUT-12	access)? Does the device support group authentication (e.g.	No
PAUT-13	hospital teams)? Does the application or device store or manage	No
PAUT-14	authentication credentials?	Yes
PAUT-14.1	Are credentials stored using a secure method?	Yes

PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized users with
physical access to the device from compromising the
integrity and confidentiality of personally identifiable
information stored on the device or on removable
media

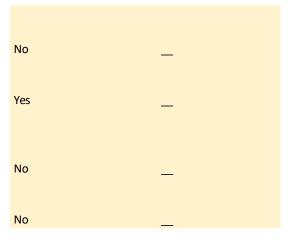
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?
	Does the device have an option for the customer to attach a physical lock to restrict access to removable
PLOK-4	media?

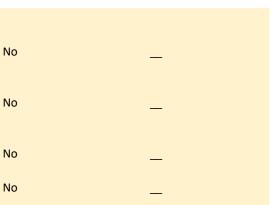
ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

	Manufacturer's plans for security support of third-party components within the device's life cycle.	
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	I
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	1
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	I
RDMP-4	Does the manufacturer have a plan for managing third- party component end-of-life?	I

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. Is the SBoM for this product available?





BBImaging	N/A	N/A
	Does the SBoM follow a standard or common method in	
SBOM-2	describing software components?	Yes
SBOM-2.1	Are the software components identified?	Yes
	Are the developers/manufacturers of the software	
SBOM-2.2	components identified?	Yes
	Are the major version numbers of the software	
SBOM-2.3	components identified?	Yes
SBOM-2.4	Are any additional descriptive elements identified?	N/A
	Does the device include a command or process method	
60014 Q	available to generate a list of software components	
SBOM-3	installed on the device?	No
SBOM-4	Is there an update process for the SBoM?	No

SYSTEM AND APPLICATION HARDENING (SAHD)

The device's inherent resistance to cyber attacks and malware.

SAHD-1	Is the device hardened in accordance with any industry standards?	No
SAHD-2	Has the device received any cybersecurity certifications? Does the device employ any mechanisms for software	No
SAHD-3	integrity checking	No
SAHD-3.1	Does the device employ any mechanism (e.g., release- specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer- authorized?	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?	No
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No
	Is the system configurable to allow the implementation of file-level, patient level, or other types of access	
SAHD-5	controls?	Yes
SAHD-5.1	Does the device provide role-based access controls? Are any system or user accounts restricted or disabled by	Yes
SAHD-6	the manufacturer at system delivery?	Yes

lo	_
10	—
lo	-
lo	—
lo	—
10	_
/es	
	_
′es	_

1-Mar-2022

BBImaging	N/A	N/A	1-Mar-2022
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration? Does this include restricting certain system or user accounts, such as service technicians, to least privileged	No	
SAHD-6.2	access?	No	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	No	
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	No	
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	No	
SAHD-10	Are all applications (COTS applications as well as OS- included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	No	
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes	
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	
SAHD-14	Can the device be hardened beyond the default provided state? Are instructions available from vendor for increased	No	
SAHD-14.1	hardening?	No	
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot? Have additional hardening methods not included in	No	
SAHD-16	2.3.19 been used to harden the device?	No	

SECURITY GUIDANCE (SGUD)

Availability of security guidance for operator and administrator of the device and manufacturer sales and service.

SGUD-1	Does the device include security documentation for the owner/operator?	Ye
	Does the device have the capability, and provide instructions, for the permanent deletion of data from the	
SGUD-2	device or media?	No
SGUD-3	Are all access accounts documented?	Yes

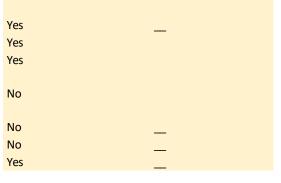
/es	_	
No		
/es		

BBImaging	N/A	N/A	1-Mar-2022
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes _	_
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	No _	_

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.

STCF-1	Can the device encrypt data at rest?
STCF-1.1	Is all data encrypted or otherwise protected?
STCF-1.2	Is the data encryption capability configured by default?
	Are instructions available to the customer to configure
STCF-1.3	encryption?
STCF-2	Can the encryption keys be changed or configured?
STCF-3	Is the data stored in a database located on the device?
STCF-4	Is the data stored in a database external to the device?



TRANSMISSION CONFIDENTIALITY (TXCF)

	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.	
	Can personally identifiable information be transmitted	
TXCF-1	only via a point-to-point dedicated cable?	
	Is personally identifiable information encrypted prior to	
TXCF-2	transmission via a network or removable media?	`
	If data is not encrypted by default, can the customer	
TXCF-2.1	configure encryption options?	1
	Is personally identifiable information transmission	
TXCF-3	restricted to a fixed list of network destinations?	`
TXCF-4	Are connections limited to authenticated systems?	`
	Are secure transmission methods	
TXCF-5	supported/implemented (DICOM, HL7, IEEE 11073)?	`

No	_
Yes	_
N/A	_
Yes	_
Yes	—
Yes	_

TRANSMISSION INTEGRITY (TXIG)

The ability of the device to ensure the integrity of transmitted data.

BBImaging	N/A	N/A	1-Mar-2022
	Does the device support any mechanism (e.g., digital		
	signatures) intended to ensure data is not modified		
TXIG-1	during transmission?	No	
	Does the device include multiple sub-components		—
TXIG-2	connected by external cables?	Yes	Note 4

	REMOTE SERVICE (RMOT)	
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.	
RMOT-1	Does the device permit remote service connections for device analysis or repair?	Yes
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes
RMOT-1.2	Is there an indicator for an enabled and active remote session?	Yes
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes

OTHER SECURITY CONSIDERATIONS (OTHR)

Notes:

Note 1	Diagram can be provided as needed.
	PII is stored encrypted in a database that maintains
Note 2	backups. Not PII is long-term stored on the devices.
	PII is stored encrypted in a database that maintains
Note 3	backups.
	The computer used in the exam room is connected to an
Note 4	ultrasound machine.