Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Nanosonics	AuditPro	A697132	20-Jul-2021
Question ID	Question		See note
DOC-1	Manufacturer Name	Nanosonics	
DOC-2	Device Description	Nanosonics AuditPro is	
	•		
DOC-3	Device Model	AuditPro	
DOC-4	Document ID	A697132	Accompanies CIN 139 (A699025)
DOC-5	Manufacturer Contact Information	(02) 8063 1600	
		The intended use of mobile	
		scanning device is to collect data	
		from trophon2 and send data to	
	Intended use of device in network-connected	AuditPro database in cloud by	
DOC C			
DOC-6	environment:	establising secure connection	
DOC-7	Document Release Date	20/07/2021	
	Coordinated Vulnerability Disclosure: Does the		
	manufacturer have a vulnerability disclosure program		
DOC-8	for this device?	No	
000-8	for this device:		
	ISAO: Is the manufacturer part of an Information		Not currently part of an ISAO - looking to change
DOC-9	Sharing and Analysis Organization?	No	this moving forward
	Diagram: Is a network or data flow diagram available		
	that indicates connections to other system		
DOC-10	components or expected external resources?	Yes	Contained within product packaging
DOC-10	components of expected external resources?	res	Contained within product packaging
	SaMD: Is the device Software as a Medical Device (i.e		AuditPro is a class one medical device exempt from
DOC-11	software-only, no hardware)?	Yes	FDA filing - hardware is supplied (honeywell device).
			Android device operating system which is
DOC-11.1	Does the SaMD contain an operating system?	Yes	maintained by Nanosonics remotely
000 11.1			
	Does the SaMD rely on an owner/operator provided		It uses the honeywell operating system running on
DOC-11.2	operating system?	No	the Android platform.
	Is the SaMD hosted by the manufacturer?		The application is hosted in secure AWS HIPAA
DOC-11.3		Yes	compliant facilities
	is the CoMD hasted by the system of 2		compliant facilities
DOC-11.4	Is the SaMD hosted by the customer?	No	
		Yes, No,	
		N/A, or	
		See Note	Note #
	MANAGEMENT OF PERSONALLY IDENTIFIABLE		
	INFORMATION		
	Can this device display, transmit, store, or modify		AuditPro collects PII e.g. t2/AuditPro users name (if
	personally identifiable information (e.g. electronic		they chose to use their names), position,
MPII-1	Protected Health Information (ePHI))?	See Notes	department, facility name, address, mobile#
	Door the douise maintain nersenally identificate		Voc. AudtiDro maintains the DII data in the second
	Does the device maintain personally identifiable		Yes. AudtiPro maintains the PII data in the secured
MPII-2	information?	See Notes	cloud database and the data is regularly back up.
	Does the device maintain personally identifiable		AuditPro mobile scanning device temporily maintain
	information temporarily in volatile memory (i.e., until		the PII in its internal memory until the data is sent
MPII-2.1	cleared by power-off or reset)?	Yes	successfully sent to the cloud.
IVIF 11-2.1	cleared by power-on or resely:	103	
			If operators chose to use their real name, then yes,
	Does the device store personally identifiable		PII is termorarily stored on the MSD before being
MPII-2.2	information persistently on internal media?	See Notes	sent to the cloud application

MPII-2.3Is personally identifiable information preserved in the
device's non-volatile memory until explicitly erased?NoMPII-2.4Does the device store personally identifiable
information in a database?See NotesDoes the device allow configuration to automatically
delete local personally identifiable information after
it is stored to a long term solution?No

The mobile application does not collect or store and PII, however the cloud application collects, stores and displays PII related to the user accounts.

Nanosonics	AuditPro	A697132	20-Jul-2021
	Does the device import/export personally identifiable		
	information with other systems (e.g., a wearable		If users chose to use their names as enerator IDs
MPII-2.6	monitoring device might export personally	See Notes	If users chose to use their names as operator IDs,
MP11-2.6	identifiable information to a server)?	See Notes	then yes, Imported PII (t2 user names, ID) from t2
	Does the device maintain personally identifiable information when powered off, or during power		
MPII-2.7	service interruptions?	Yes	
WII II-2.7	Does the device allow the internal media to be		Device doesn't allow internal media to be removed.
	removed by a service technician (e.g., for separate		Once user is unsubscribed, device will be clean
MPII-2.8	destruction or customer retention)?	See Notes	wiped by service techician
	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		
MPII-2.9	storage location)?	No	
	Does the device have mechanisms used for the		
	transmitting, importing/exporting of personally		
MPII-3	identifiable information?	Yes	
	Does the device display personally identifiable		
MPII-3.1	information (e.g., video display, etc.)?	Yes	
	Does the device generate hardcopy reports or images		
MPII-3.2	containing personally identifiable information?	Yes	User accounts only
	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,		
MPII-3.3	CF/SD card, memory stick, etc.)?	No	
	Does the device transmit/receive or import/export		
	personally identifiable information via dedicated		
	cable connection (e.g., RS-232, RS-423, USB,		
MPII-3.4	FireWire, etc.)?	No	
	Does the device transmit/receive personally		
	identifiable information via a wired network		
MPII-3.5	connection (e.g., RJ45, fiber optic, etc.)?	No	
	Does the device transmit/receive personally		
	identifiable information via a wireless network		
	connection (e.g., WiFi, Bluetooth, NFC, infrared,	No.	Only if users chose to use their own names as
MPII-3.6	cellular, etc.)?	Yes	operator IDs
	Does the device transmit/receive personally identifiable information over an external network		If the cloud application is used by customers to view
MPII-3.7		Vac	or modify email address, data will be transmitted over internet
MIP11-3.7	(e.g., Internet)?	Yes	overinternet
	Does the device import personally identifiable		
MPII-3.8	information via scanning a document?	No	
	Does the device transmit/receive personally		Only if users chose to use their own names as
MPII-3.9	identifiable information via a proprietary protocol?	Yes	operator IDs
	Does the device use any other mechanism to		
	transmit, import or export personally identifiable		
MPII-3.10	information?	No	
Management of I	Private Data notes:		

Yes

No

AUTOMATIC LOGOFF (ALOF)

The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time. Yes

Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before autologoff/screen lock user or administrator configurable? Idle log off time is 20 minutes 2 minute screen lock for mobile device

Idle log off time is 20 minutes 2 minute screen lock for mobile device

Meets OWASP standard

ALOF-1

ALOF-2

AuditPro A697132 20-Jul-2021 Nanosonics AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or AUDT-1 Cloud based application stores full system logs reports beyond standard operating system logs? Yes USER IDs are recorded for any information updates AUDT-1.1 Does the audit log record a USER ID? Yes / edits. Does other personally identifiable information exist AUDT-1.2 in the audit trail? Yes Currently any changes to editable fields within the Are events recorded in an audit log? If yes, indicate application will be logged, more features will be which of the following events are recorded in the AUDT-2 audit log: Yes available in the next release. AUDT-2.1 Successful login/logout attempts? See Notes Have for login, not for logout AUDT-2.2 Unsuccessful login/logout attempts? Yes 5 attempts AUDT-2.3 Modification of user privileges? Managed by the facility Admin Yes Deletion of users is not allowed as AuditPro is tracking software. Users can be anonymised. Users AUDT-2.4 Creation/modification/deletion of users? Yes can modify their own accounts Presentation of clinical or PII data (e.g. display, AUDT-2.5 print)? No Modification and creation are logged. Deletion of Creation/modification/deletion of data? AUDT-2.6 Yes data is not allowed. Import/export of data from removable media (e.g. N/A AUDT-2.7 USB drive, external hard drive, DVD)? Receipt/transmission of data or commands over a Important data - yes, not for commands (e.g. a get AUDT-2.8 network or point-to-point connection? See Notes call). Remote support provided by Nanosonics service AUDT-2.8.1 Remote or on-site support? Yes team Application Programming Interface (API) and similar AUDT-2.8.2 activity? Yes Yes, use mobile and cloud APIs AUDT-2.9 Emergency access? No No emergency access allowed AUDT-2.10 Other events (e.g., software updates)? Yes AUDT-2.11 Is the audit capability documented in more detail? Audit and Logging Policy Yes Can the owner/operator define or select which 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 AUDT-4.1 Does the audit log record date/time? Yes Can date and time be synchronized by Network Time Timezone comes from user input during registration AUDT-4.1.1 Protocol (NTP) or equivalent time source? No (passed from cloud to mobile device) AUDT-5 Can audit log content be exported? Yes AUDT-5.1 Via physical media? Yes e.g. Can be printed Via IHE Audit Trail and Node Authentication (ATNA) AUDT-5.2 profile to SIEM? No Via Other communications (e.g., external service AUDT-5.3 device, mobile applications)? No Are audit logs encrypted in transit or on storage AUDT-5.4 media? Yes Can audit logs be monitored/reviewed by

AUDT-7.1	
AUDT-8	

AUDT-6

AUDT-7

AUTH-1

AUTH-1.1

Are audit logs protected from access? Can audit logs be analyzed by the device?

Are audit logs protected from modification?

Yes No

Yes

Yes

AUTHORIZATION (AUTH)

owner/operator?

The ability of the device to determine the
authorization of users.Does the device prevent access to unauthorized users
through user login requirements or other
mechanism?YesCan the device be configured to use federated
credentials management of users for authorization
(e.g., LDAP, OAuth)?No

Nanosonics	AuditPro	A697132	20-Jul-2021
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	
AUTH-1.3	Are any special groups, organizational units, or group policies required? Can users be assigned different privilege levels based	No	
AUTH-2	on 'role' (e.g., user, administrator, and/or service, etc.)?	See Notes	Cloud application - yes, mobile scanning device - no, only one password per device
	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access		
AUTH-3	operating system or application via local root or administrator account)? Does the device authorize or control all API access	No	
AUTH-4	requests? Does the device run in a restricted access mode, or	Yes	
AUTH-5	'kiosk mode', by default?	Yes	

CYBER SECURITY PRODUCT UPGRADES (CSUP)

	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.	
	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	
CSUP-1	in this section.	
	Does the device contain an Operating System? If yes,	
CSUP-2	complete 2.1-2.4. Yes	
	Does the device documentation provide instructions	
	for owner/operator installation of patches or	
CSUP-2.1	software updates? Yes	
0001 2.1		
	Does the device require vendor or vendor-authorized	
CSUP-2.2	service to install patches or software updates? No	
C30F-2.2		
	Does the device have the capability to receive remote	
CSUP-2.3		
C30P-2.3	installation of patches or software updates? Yes	
	Does the medical device manufacturer allow security	
	updates from any third-party manufacturers (e.g.,	
	Microsoft) to be installed without approval from the	
CSUP-2.4	manufacturer? No	
	Does the device contain Drivers and Firmware? If yes,	
CSUP-3	complete 3.1-3.4. Yes	
	Does the device documentation provide instructions	
	for owner/operator installation of patches or	
CSUP-3.1	software updates? Yes	
	Does the device require vendor or vendor-authorized	
CSUP-3.2	service to install patches or software updates? No	
	Does the device have the capability to receive remote	
CSUP-3.3	installation of patches or software updates? Yes	
	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? No	
	Does the device contain Anti-Malware Software? If	
CSUP-4	yes, complete 4.1-4.4. See Not	tes
-	Does the device documentation provide instructions	
	for owner/operator installation of patches or	
CSUP-4.1	software updates? N/A	
	Does the device require vendor or vendor-authorized	
CSUP-4.2	service to install patches or software updates? N/A	

No software, managed by MDM. Device is set up to only be used in KIOSK mode for security.

Nanosonics	AuditPro	A697132 20-Jul-2021
	Does the device have the capability to receive remote	
CSUP-4.3	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 manufacturer?	
CSUP-4.4	Does the device contain Non-Operating System	N/A
	commercial off-the-shelf components? If yes,	
CSUP-5	complete 5.1-5.4.	No
6301-3	Does the device documentation provide instructions	
	for owner/operator installation of patches or	
CSUP-5.1	software updates?	N/A
	Does the device require vendor or vendor-authorized	
CSUP-5.2	service to install patches or software updates?	N/A
	Does the device have the capability to receive remote	
CSUP-5.3	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-5.4	manufacturer?	N/A
	Does the device contain other software components	
	(e.g., asset management software, license	
	management)? If yes, please provide details or	
CSUP-6	refernce in notes and complete 6.1-6.4.	Νο
	Does the device documentation provide instructions	
	for owner/operator installation of patches or	
CSUP-6.1	software updates?	N/A
	Does the device require vendor or vendor-authorized	
CSUP-6.2	service to install patches or software updates?	N/A
	Does the device have the capability to receive remote	
CSUP-6.3	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-6.4	manufacturer?	N/A
	Does the manufacturer notify the customer when	
CSUP-7	updates are approved for installation?	Yes
	Does the device perform automatic installation of	
CSUP-8	software updates?	Yes
	Does the manufacturer have an approved list of third	-
CSUP-9	party software that can be installed on the device?	Yes
	Can the owner/operator install manufacturer-	
	approved third-party software on the device	
CSUP-10	themselves?	No
	Does the system have mechanism in place to prevent	
CSUP-10.1	installation of unapproved software?	Yes
	Does the manufacturer have a process in place to	
CSUP-11	assess device vulnerabilities and updates?	Yes
	Doos the manufacturer provide sustemars with	

		Does the manufacturer provide customers with
С	SUP-11.1	review and approval status of updates?
С	SUP-11.2	Is there an update review cycle for the device?

HEALTH DATA DE-IDENTIFICATION (DIDT)

The ability of the device to directly remove information that allows identification of a person.

IGAU-2

Nanosonics	AuditPro	A697132	20-Jul-2021
DIDT-1	Does the device provide an integral capability to de- identify personally identifiable information?	Yes	
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de- identification?	No	DICOM is a standard for medical imaging communication and in AuditPro we mask the user with facility id and request id received by service
	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)? Does the device have a "factory reset" function to	Yes	The cloud application does, mobile scanning device does not.
DTBK-2	restore the original device settings as provided by the manufacturer? Does the device have an integral data backup	Yes	
DTBK-3	capability to removable media? Does the device have an integral data backup	No	
DTBK-4	capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and	No	
DTBK-5	software restoration?	No	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	
	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.		
EMRG-1	Does the device incorporate an emergency access (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 altered or destroyed in a non- authorized manner and is from the originator.		
IGAU-1	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	Yes	Deduus quailable for the aloud explication

See Notes

MALWARE DETECTION/PROTECTION (MLDP)

recovery mechanisms for stored health data (e.g.,

The ability of the device to effectively prevent, detect and remove malicious software (malware).

 MLDP-1
 Is the device capable of hosting executable software? Yes

 Does the device support the use of anti-malware software (or other anti-malware mechanism)?

 MLDP-2
 Provide details or reference in notes.

RAID-5)?

Only APK

Backup available for the cloud application

Not available for the mobile application

Nanosonics	AuditPro	A697132	20-Jul-2021
MLDP-2.1 MLDP-2.2	Does the device include anti-malware software by default? 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	No No	
MLDP-2.3	software? Can the device owner/operator independently (re-	No	
MLDP-2.4)configure anti-malware settings? Does notification of malware detection occur in the	No	
MLDP-2.5	device user interface?	No	
MLDP-2.6 MLDP-2.7	Can only manufacturer-authorized persons repair 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)?	N/A	
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	Yes	Using MDM for device security. Device is set up to only be used in KIOSK mode for security.
MLDP-4 MLDP-5	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device? Does the device employ a host-based intrusion detection/prevention system?	Yes No	
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	Νο	
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Νο	
	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)?	Yes	Web API using SSL to authenticate, cloud infrastructure uses network segmentation and whitelisting to identify authorised requests.
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)? Is the firewall ruleset documented and available for	See Notes	Mobile device: No Cloud application: Yes, we have white listing and a segmented network design. Mobile device is proprietary and managed by
NAUT-2.1 NAUT-3	review? Does the device use certificate-based network connection authentication?	N/A Yes	reputable vendor HEM.

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.	
	Does the device have hardware connectivity	
CONN-1	capabilities?	No
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?	No
	Does the device support other wireless network	
CONN-1.1.3	connectivity (e.g. LTE, Zigbee, proprietary)?	No

Device supports bluetooth but disabled by Nanosonics

PAUT-6

Nanosonics	AuditPro	A697132	20-Jul-2021
	Does the device support other wireless connections		
CONN-1.1.4	(e.g., custom RF controls, wireless detectors)?	Yes	NFC
CONN-1.2	Does the device support physical connections?	Yes	Charging / usb connection
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	No	Micro USP 2.0 just for charging purposes (locked
CONN-1.2.2	Does the device have available USB ports?	Yes	Micro USB 2.0 - just for charging purposes (locked out of any other feature)
	Does the device require, use, or support removable		
CONN-1.2.3	memory devices?	No	
CONN-1.2.4	Does the device support other physical connectivity? Does the manufacturer provide a list of network	No	
	ports and protocols that are used or may be used on		
CONN-2	the device?	Yes	
	Can the device communicate with other systems		
CONN-3	within the customer environment?	Yes	
	Can the device communicate with other systems		
	external to the customer environment (e.g., a service	No.	
CONN-4 CONN-5	host)? Does the device make or receive API calls?	Yes Yes	
CONN-5	Does the device require an internet connection for its		
CONN-6	intended use?	Yes	
	Does the device support Transport Layer Security		
CONN-7	(TLS)?	Yes	
CONN-7.1	Is TLS configurable?	No	
	Does the device provide operator control		
	functionality from a separate device (e.g.,		
CONN-8	telemedicine)?	No	
	PERSON AUTHENTICATION (PAUT)		
	The ability to configure the device to authenticate		
	<i>users.</i> Does the device support and enforce unique IDs and		
	passwords for all users and roles (including service		Cloud application - yes, mobile scanning device - no,
PAUT-1	accounts)?	See Notes	only one password per device
	Does the device enforce authentication of unique IDs		Cloud application - yes through email verification,
	and passwords for all users and roles (including		mobile scanning device - no, only one password per
PAUT-1.1	service accounts)?	See Notes	device, no verification
	Is the device configurable to authenticate users		
	through an external authentication service (e.g., MS	Ne	
PAUT-2	Active Directory, NDS, LDAP, OAuth, etc.)?	No	
	Is the device configurable to lock out a user after a		
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?	Yes	
	Is the device configurable to enforce creation of user		

	Does the device support account passwords that		
PAUT-7	expire periodically?	Yes	
PAUT-8	Does the device support multi-factor authentication?	Yes	
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?	No	
	Does the device support physical tokens (e.g. badge		
PAUT-12	access)?	No	
	Does the device support group authentication (e.g.		
PAUT-13	hospital teams)?	No	
	Does the application or device store or manage		
PAUT-14	authentication credentials?	See Notes	Cloud application - yes, mobile scanning device - no

Yes

account passwords that meet established

(organization specific) complexity rules?

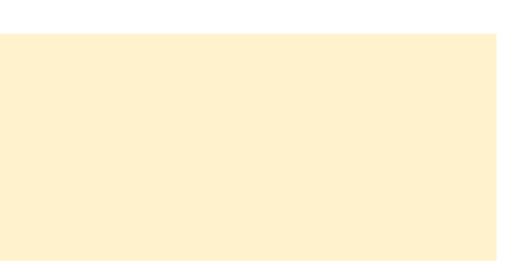
Nanosonics	AuditPro	A697132	20-Jul-2021
PAUT-14.1	Are credentials stored using a secure method?	See Notes	Cloud application - yes, mobile scanning device - no
	PHYSICAL LOCKS (PLOK) Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media		
			There is a physical Mobile Scanning Device, however the product is a software package on this
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section. Are all device components maintaining personally identifiable information (other than removable	Yes	device. Without access, there is no information that can be leaked.
PLOK-2	media) physically secure (i.e., cannot remove without tools)? Are all device components maintaining personally identifiable information (other than removable	N/A	
PLOK-3	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	N/A	
PLOK-4	media?	N/A	

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

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?



SBOM-1	Is the SBoM for this product available?	No
	Does the SBoM follow a standard or common	
SBOM-2	method in describing software components?	N/A
SBOM-2.1	Are the software components identified?	N/A
	Are the developers/manufacturers of the software	
SBOM-2.2	components identified?	N/A
	Are the major version numbers of the software	
SBOM-2.3	components identified?	N/A
SBOM-2.4	Are any additional descriptive elements identified?	N/A
	Does the device include a command or process	
	method available to generate a list of software	
SBOM-3	components installed on the device?	N/A
SBOM-4	Is there an update process for the SBoM?	N/A

STRUE Towers resolution involvesState device residence in update actacks and involvesNoSUD-1In the device framework in a state actack and involvesYesWesSUD-2Does the device analysis any metanions for is actack actack in a state actack actack is actack actack in a state actack actack actack is actack actack actack in a state actack actack actack in a state is actack actack actack actack actack actack actack is actack actack actack actack actack actack actack is actack actack actack actack actack actack actack actack is actack actack actack actack actack actack actack is actack actack actack actack actack actack actack actack is actack actack actack actack actack actack actack is actack actack actack actack actack is actack actack actack actack actack actack is actack actack actack actack actack actack actack is actack actack actack actack actack actack is actack actack actack actack actack actack actack is actack actack actack actack actack actack actack actack is actack actack actack actack actack actack actack actack is actack actack actack actack actack actack actack actack actack is actack	Nanosonics	AuditPro	A697132	20-Jul-2021
Pic device indexed in accordance with any markawa Yes Avs compliances SMD-1 In the device indexed in accordance with any markawa Yes Avs compliances SMD-2 conflication? Yes Avs compliances SMD-3 Dows the device readewid any opter numbrions for the service indication (e.g., release grant in the interplay any markawa (e.g., release grant in the interplay any markawa (e.g., release grant in the interplay any markawa (e.g., release grant interplay and release grant interplay any markawa (e.g., release grant interplay any markawa		SYSTEM AND APPLICATION HARDENING		
nature setup Add Sconglismes SMD-1 Bits device index with any modust y stundurds Yes Add Sconglismes SMD-2 Certificators ² Yes Add Sconglismes SMD-3 Does the device index yary mechanism for software integrity devices Yes Add Sconglismes SMD-3.1 Does the device index yary mechanism for software integrity devices Yes Yes SMD-3.1 Does the device index yary mechanism for software integrity ware interfactures Yes SMD-3.2 Can the device index yary mechanism (e.g., release) Yes SMD-3.1 Can the device index yary mechanism (e.g., release) Yes SMD-3.2 Can the device index yary mechanism (e.g., release) Yes SMD-5.1 Does the device provide role based access controle Yes SMD-6.1 Are any system or user accounts retricted or dasabed by the manufacturer at yary method user provide dasabed controle Yes SMD-6.2 Provide dasabed controle Yes SMD-6.3 Are any system or user accounts retricted or dasabed by the manufacturer at yary method user are at yary device index yary method user of the device provide dasabed? Yes SMD-6.1 Are any				
Bithe device hardered in accordinace with any Has the device received any obserseury SAHD 2 AVXS compliances OVXASP PEN testing carried out on web application of advace integrit without point device employ any mechanism for source advace integrit with the source from software integrit advaced updates? Yes SMID-5.1 Does the device employ any mechanism for source advaced integrit with the source from software integrit point dataset source advaced integrit with the source from modified or tampeed with? Yes SMID-5.1 Does the device provide rule-based access control? Yes SMID-6.1 And samy system or user accounts retricted or sources, the software integrit with any ear advaced retricting certain system or ear advaced retricting certain system or ea				
SMD-1 Industry standards? Yes Aves compliances SAID-2 Bits the device endpoy any methanism for software integrity theshing authorized Yes Bidevice application SAID-3 Does the device endpoy any methanism for software integrity theshing authorized Yes Bidevice application SAID-3 Does the device endpoy any methanism for software integrity theshing authorized Yes SAID-3.1 Does the device endpoy any methanism for software updates are the manufacturer. The device the integrity the filter integrity authorized Yes SAID-3.1 Does the device anglog any methanism for software updates are the manufacturer. The device the polyter integrity the integrity device is a withorized updates? Yes SAID-4 Can the owner/operator perform software integrity integriter integrity that the system on tool teem implementation of file-level, autent level, or other implementation of file-level, autent level, or other integriter integrity the integriter integrity device is a withorized updates? Yes SAID-5.1 Does the device application tools with the file is a system or user accounts, tools are accounts on tignate the integrity disalded by the manufacturer at system or user accounts, tools are accounts on tignate the integrity disalded by the manufacturer at system or user accounts, tools are accounts on tignate the integrity disalded are on system or user accounts on tignate the integrity disalded are manufacturer at system or user accounts, tools are accounts on tignate the integrity disalded accounts, tools are accounts on tignate the integrity disalded accounts, tools are accounts on tignate accounts, to				
SAHD 2. certification? Yes 8 device application SAHD 3. Does the device mayby any nethanism for software materially checking to pussible device mayby any nethanism (e.g., release specific hash key, thecksum, fight signature, rel.) Yes SAHD 3.1 Does the device public and the mandature authorized? Yes SAHD 4.1 Can the comerciporator perform software integrity thecks (i.g., werfly that the system has not beam implementation of fiele-well, pistem control Yes SAHD 4.1 Can the comerciporator perform software integrity thecks (i.g., werfly that the system has not beam implementation of fiele-well, pistem control Yes SAHD 5.1 Does the device provide and control Yes SAHD 5.1 Does the device from software integrity thecks (i.g., werfly that the system has not beam implementation of fiele-well, pistem control Yes SAHD 6.1 Does the device from software integrity thecks (i.g., werfly that the system for user accounts, such as service technicity, to least accounts, s	SAHD-1		Yes	AWS compliances
Does the device employ any mechanism for obstivate integrity decising Decisite device employ any mechanism (e.g., release specific balk ver, decisions, dig instruce, etc.) We setting instruction (e.g., release specific balk ver, decisions, dig instruce, etc.) SAID-3.1 automized pecific balk ver, decisions, dig instruce, etc.) We setting instruction (e.g., release specific balk ver, decisions, dig instruce, etc.) We setting instruction (e.g., release specific balk ver, decisions, dig instruce, etc.) SAID-3.2 Can the conter/operator perform software integrity the decision (e.g., weif) that the isom has no bears integrity that the specific decision (e.g., weif) that the isom has no bears integrity that the specific decision (e.g., weif) that the specific decision (e.g., the specif				
SAHD-3 softwere integrity checking Yes SAHD-3.1 Does the device employ any mechanism (e.g., release- sequefic, hash key, checksum, digital signature, etc.) Yes SAHD-3.2 authorized? Yes SAHD-3.2 Can the owner/operator perform software indigitations, digital signature, etc.) Yes SAHD-3.1 Can the owner/operator perform software indigitations, digital signature, etc.) Yes SAHD-3.2 Can the owner/operator perform software indigitations, digital signature, etc.) Yes SAHD-3.1 Can the owner/operator perform software indigitations, digital signature, etc.) Yes SAHD-5.1 Does the device provide role-based access controle? Yes SAHD-6.1 Are any system or user accounts instricted or access controle? Yes SAHD-6.2 Are any system or user accounts instricted or access controle? Yes SAHD-6.2 Are any system or user accounts instricted or access controle? Yes SAHD-6.2 Are any system or user accounts instricted or access controle? Yes SAHD-6.2 Are any system or user accounts instricted or access controle? Yes SAHD-6.2 Are any system or user accounts contriguible to the device or hold work are an interview or the interded use of the device or hold work are an interview or the interded use of the device or hold work are an interview or the interded use of the device or hold work are an interview or hold work are an in	SAHD-2		Yes	& device application
Does the device proplex promote hand in leg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on ploy any mechanism (eg., release - south base of the device on the manufacture on the released access controls? Yes SAHD-5.1 Does the device provide role-based access controls? Yes SAHD-5.1 Does the device provide role-based access controls? Yes SAHD-5.1 Does the device provide role-based access controls? Yes SAHD-6.1 end service (eg., file, sheet) which are user accound singulable the device on view accound singu	SAHD-3		Vec	
subcit subcit subcit subcit SAID-3.1 authorized? ves SAID-3.2 Can the owner/doperator perform software integrity checks (i.e. writh that the system is not been modified or tampeed with?? No SAID-5.1 Does the device provide role-based access controls? Yes SAID-5.1 Does the device provide role-based access controls? Yes SAID-6.1 e.g. non work emails (public emails blocked) Yes SAID-6.2 Are any system or user accounts rolificated provide role-based access controls? Yes SAID-6.1 Does the device envide role-based access controls? Yes SAID-6.2 Are any system or user accounts rolificated provide role-based access controls? Yes SAID-6.1 end user after intended use of the device post init configurable to the system delvers? N/A SAID-6.2 provinger access/secs/secs/secs/secs/secs/secs/sec	5410-5			
SAHD-3.1autorized?YesSAHD-3.2Control device analyse any enhancing e.g. releases a section hash key, checksom, digital signature, etc. John and been manufacture etc. John and been etc. John and been etc. John and been etc. John and been etc. John and been and been etc. John and been etc		specific hash key, checksums, digital signature, etc.)		
Does the dovice employ any mechanism (e.g., release- specific hash (e.g., herkesswa, digital signature, etc.) to ensure the software updates are the manufacure authorized updates?NoSAID-3.2Can the cover/operator perform software integrity (hecks (e.g., verify that the system configurable to allow the implementation of file-level, patient level, or other (hecks (e.g., verify that the system configurable to allow the implementation of file-level, patient level, or other (hecks (e.g. verify that the system configurable to allow the implementation of file-level, patient level, or other (hecks (e.g. verify that the system configurable to allow the implementation of file-level, patient level, or other (hashed System configurable to allow the implementation of file-level, patient level, or other (hashed System configurable to allow the implementation in system or user accounts configurable to the verify that the system configurable to the verify that the system configurable to the system configurable to the verify that the system configurable to the system configurable to the verify that the system configurable to the system configurable to the verify that the system configurable to the system configurable to the system verify that the system configurable to the system configurable to the system configurable to the system verify that the system configurable to the system config				
specific hash key, checksums, digital signature, etc.) to ensure the owner/operator perform software integring checks (i.e., work (with that the system integring) to the system or user accounts integringNoSAHD-41Can the owner/operator perform software integring integring (i.e., being of access controls ?NoSAHD-51Dest the device provide role based access controls ?YesSAHD-61Are any system or user accounts restricted or databel by the manufacture at system deliver?YesSAHD-61Are any system or user accounts restricted or databel by the manufacture at system deliver?YesSAHD-62Provide role based access controls ?YesSAHD-63and are any system or user accounts restricted or obset this induce retricting certain system or user accounts, such as service technicians, to least accounts, such as service technicians, to least a disabel?N/ASAHD-64end treaduce of the device a disabel?N/ASAHD-74disabel?N/ASAHD-74readistrols (e.g., tientaffer protocol tiented du so of the device a disabel?N/ASAHD-74readistrols (e.g., tientaffer protocol tiented du so of the device a disabel?N/ASAHD-75disabel?N/ASAHD-76and service (e.g., file shares) which are not required for the intended use of the device a disabel?N/ASAHD-70disabel?N/ASAHD-71con trequired for the intended use of the device a disabel?N/A	SAHD-3.1			
SAND-3.2 to ensure the software updates are the manufacture set of the system configurable to allow the integreted with system configurable to the ways the integreted with system configurable to the ways the integrete with system configurable to the ways the integrete with system configurable to the integrete with system configurable to the integreted with a service technical system configurable to the device not the device of t				
SARD-4Can the owner/operator perform software integrity checks (i.e., writy that the system has not been indified at more dwith?) Is the system configurable to allow the implementation of Hier-Veto, patient level, or other YesNoSARD-51Dees the device provide role-based access controls?YesSARD-61Are any system or user accounts configurable by the end user after india configurable by the acceunts, such a service technicians, to least YesYesSARD-6.1Are any system or user accounts configurable by the end user after india configurable by the acceunts, such a service technicians, to least YesYesSARD-6.2privileged access? Are all advice fractions of the device of disabled?NoSARD-7disabled? Are all advice fractions of the device of disabled?NoSARD-8access (a.g., telnet), file transfer protocol included againstore (i.g., its shares) which are not required for the intended use of the device of disabled?NASARD-8acte all advices (a.g., telnet), file transfer protocol which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the in			-	
SAID-14endified or tangered with a system has not been modified or tangered with a system configurable to allow the implementation of file-level, patient level, or other magered with a system or user accounts restricted or disabled by the manufacturer at system deliver??YesSAID-61Does the device provide role-based access controls?YesSAID-61.0Are any system or user accounts restricted or disabled by the manufacturer at system deliver??YesSAID-61.0Obest the induce restricting carrier in system or user accounts, such as service technicians, to least accounts, such access? Are all spruces (e.g., tile shared) which are not required for the intended use of the device active and technicans, to least access accounts, such as service technicans, to least accounts, such as service technicans, to least accounts, such as service technicans, to least accounts, such access?N/ASAHD-10Carl the device prohibit toot from uncontrolled or 	SAHD-3.2	authorized updates?	Yes	
SAID-14endified or tangered with a system has not been modified or tangered with a system configurable to allow the implementation of file-level, patient level, or other implementation of file-level, patient level, or other setNoSAID-51Does the device provide role-based access controls?YesSAID-61Are any system or user accounts restricted or disabled by the manufacturer at system deliver?? en user accel rain system or user accounts, such as service technicians, to least accounts, such as service technicians,		Can the owner/onerator perform software integrity		
SAHD-4modified or tampered with ? is the system configurable to allow the implementation of file level, patient level, or other system or user accounts restricted or disabled by the manufacture at system delivery?NoSAHD-5.1Does the device provider role-based access controls?YesSAHD-6.1Are any system or user accounts configurable by the are any system or user accounts configurable by the Does this include restricting certain system or user accounts, such as service technicians, to least accounts, such as service technicians, to least are accounts, such as service technicians, to least are accounts, such as service technicians, to least are an trequired for the intended use of the device are not required for the intended use of the device accounts, such as a service technicians, to least are accounts, such as service technicians, to least are accounts, such as a service technician technicians, to least are accounts, such as a service technicians, to least are accounts, such as a service technician technicians, accounts, such as a service technician te				
SAHD-5Implementation of file-level, patient level, or other types of access controls?vesSAHD-5.1Does the device provide role-based access controls?YesSAHD-6Are any system or user accounts configurable by the rate any system or user accounts configurable by the ned user after initial configurable by the rate any system or user accounts configurable by the rate any system or user accounts configurable by the rate and user after initial configurable by the rate and the after role constructions and protocols that are not required for the intended use of the device disbled?N/ASAHD-6.1Are all communication ports and protocols that are not required for the intended use of the device adsbaled?N/ASAHD-7Are all services (e.g., thent, file transfer protocol (FPP), internet information as well as OS- include applications, e.g. White manufacture as a service (e.g., the shrees the tother are not required for the intended use of the device adstabed?N/ASAHD-10Can the device applications as well as OS- include applications, e.g. White manufacture as a service (e.g. the shrees the tother and the device adstabed?N/ASAHD-11Can the device application as a device and applications, e.g. and the advice adstabe?N/ASAHD-12Can the device applications as evel as OS- include applications, e.g. white manufacture as a service advice a source other than an an on trequired for the intended use of the device deleted/disable?N/ASAHD-11Can the device applications accords as well as OS- include applicatio	SAHD-4		No	
SAHD-3 types of access controls? Yes SAHD-5.1 Does the device provide role-based access controls? Yes SAHD-6 Are any system or user accounts certificted or dasheld by the manufacturer at system deliver?? Yes e.g. non work emails (public emails blocked) SAHD-6.1 end user after initial configuration? Yes e.g. non work emails (public emails blocked) SAHD-6.2 provideg access? Yes e.g. non work emails (public emails blocked) SAHD-7 disabled? Yes e.g. non work emails (public emails blocked) SAHD-7 accounts, such as service technicians, to least Yes SAHD-7 disabled? N/A Are all shared resources (e.g., file shares) which are not required for the intended use of the device and the device which are not required for the intended use of the device and the				
SAHD-5.1 Does the device provide role-based access controls? Yes SAHD-6 Are any system or user accounts restricted or disabled by the manufacturer at system deliver?? Are any system or user accounts configurable by the end user after initial configurable? Yes SAHD-6.1 e.g. non work emails (public emails blocked) Yes SAHD-6.2 privileged access? Yes SAHD-7 disabled? Yes SAHD-8 disabled? N/A Are all some for the intended use of the device all shared resources (e.g., file shares) which are nor required for the intended use of the device disabled? N/A SAHD-8 disabled? N/A Are all communication ports and protocols IFTP), internet informations ener (IIS), etc.), which are not required for the intended use of the device vicit are not required for the intended use of the device are not required for the intended use of the device vicit are not required for the intended use of the device vicit are not required for the intended use of the device vicit are not required for the intended use of the device vicit are not required for the intended use of the device vicit are not required for the intended use of the device vicit are not required for the intended use of the move delicted/disabled? N/A SAHD-10 Can the device probibit boot from uncontrolled or removable media (i.e., a source other than an internal dive or memory component)? Yes SAHD-13 Does the product documentation include information on operational network security scaning by user? No SAHD-			No.	
SAHD-6 Are any system or user accounts centricted or Yes e.g. non work emails (public emails blocked) SAHD-6.1 Bobs this include restricting certain system or user accounts, such as service technicians, to least Yes SAHD-6.2 privileged access? Yes Are all shored resources (e.g., file shares) which are not required for the intended use of the device and trequired for the intended use of the device disabled? N/A SAHD-8 disabled? N/A SAHD-9 Are all services (e.g., file shares) which are not required for the intended use of the device disabled? N/A SAHD-8 disabled? N/A SAHD-9 Are all communication ports and protocols that are not required for the intended use of the device file (file) shaled? N/A SAHD-9 Are all splications (CTS applications as well as Osiniculed applications, e.g., MS Internet Explorer, etc.) N/A SAHD-10 device deted/disabled? Yes SAHD-11 Can the device or phibit boot from uncontrolled or removable media (i.g., a source other than an internal diver or memory component)? Yes SAHD-13 Does the product documentation include information on operational network security scaning by users? No SAHD-14 Provided state? No No SAHD-14.1 <td< td=""><td>SAHD-5</td><td>types of access controls?</td><td>Yes</td><td></td></td<>	SAHD-5	types of access controls?	Yes	
SAHD-6disabled by the manufacturer at system delivery?YesSAHD-6.1Are 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 accounts, such as service technicians, to least at real shared resources (e.g., file shares) which are not required for the intended use of the device disabled?YesSAHD-7disabled? Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?N/ASAHD-8disabled? (FFP), internet information server [18], etc.), which are not required for the intended use of the device deleted/disabled?N/ASAHD-9disabled? (IFPE), internet information server [18], etc.), which are not required for the intended use of the device deleted/disabled?N/ASAHD-10can the device prohibit boot from uncontrolled or intrudi dive or memory component)?YesSAHD-11can the device prohibit boot from uncontrolled or on operational network security scanning by users?YesSAHD-12can unauthorized software or hardware be installed on the device behytical tools?N/ASAHD-13Does the product documentation include information on operational network security scanning by users?N/ASAHD-14Provided state? Doet shater Provide state?N/ASAHD-13Does the product documentation include information can the device behytem provem tacces to BIOS or other SAHD-13NoSAHD-14Provided state? Doet boders during boot?N/ASAHD-15bootboders during boot	SAHD-5.1	Does the device provide role-based access controls?	Yes	
SAHD-6 disabled by the manufacturer at system delivery? Yes e.g. non work emails (public emails blocked) SAHD-6.1 Does this include restricting certain system or user accounts, sochigurable by the end user after initial configuration? Yes SAHD-6.2 Privileged access? Yes SAHD-7 disabled? N/A Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? N/A SAHD-8 are not required for the intended use of the device disabled? N/A SAHD-9 disabled? N/A SAHD-10 device deleted/disable? N/A SAHD-10 device deleted/disable? N/A SAHD-10 can the device or the intended use of the device deleted/disable? N/A SAHD-10 can the device or heintended use of the device deleted/disable? N/A SAHD-10 can the device or heintended use of the device deleted/disable? N/A SAHD-11 can the device or hardware be installed or or memory component? Yes SAHD-13 Does the product documentation include information on operational network security scanning by users? No SAHD-14 Provide state? No SAHD-13 Does the product documentation include information on operational network security scanning by users? No SAHD-14 Provide sta				
Are any system or user accounts configurable by the accounts, such as service technicians, to least accounts, such as service technicians, to least accounts, such as service technicians, to leastYesSAHD-6.2privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device Are all communication ports and protocols that are not required for the intended use of the device (FTP), internet information server (IIS), etc.), which are not required for the intended use of the device Are all applications (COTS applications as well as DS- include applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device Are all applications (COTS applications as well as DS- include applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?N/ASAHD-10device deleted/disabled?YesSAHD-11internal drive or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on the device be hardened beyond the default provided state?NoSAHD-14Dees the product documentation include information are in provided state?NoSAHD-15Does the product documentation include information are in the device be hardened beyond the default provided state?NoSAHD-14Can the device be hardened beyond the default provided state?NoSAHD-15Does the product documentation include information are in provided state?NoSAHD-15Hardening?NoSAHD-16Hardening?NoSAHD-17Hardening?NoSAHD-16<			M	
SAHD-6.1end user after initial configuration?YesDoes this include restricting certain system or user accounts, such as service technicians, to least Are all sharder resources (e.g., file shares) which are not required for the intended use of the device disabled?YesSAHD-7disabled?N/AAre all communication ports and protocols that are not required for the intended use of the device disabled?N/ASAHD-8disabled?N/AAre 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 which are not required for the intended use of the device which are not required for the intended use of the device which are not required for the intended use of the deviceN/ASAHD-9deleted/disabled?N/ASAHD-10device deted/disabled?VesSAHD-11internal drive or memory componentl?YesSAHD-12on the device softhit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory componentl?YesSAHD-13Does the product documentation include information sAHD-14Does the product documentation include information sAHD-15NoSAHD-14provided state? Are instructions available from vendor for increased SAHD-13N/ASAHD-14provided state? Are instructions available from vendor for increased Are instructions available from vendor for increased SAHD-14NoSAHD-15hardening? Are all applications?NoSAHD-14provided state? Are instructions available from vendor f	SAHD-6		Yes	e.g. non work emails (public emails blocked)
Does this include restricting certain system or user accounts, such as service technicians, to leastYesSAHD-6.2privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device NAN/ASAHD-7disabled? Are all communication ports and protocols that are not required for the intended use of the device SAHD-8N/ASAHD-8disabled? Are all services (e.g., telnet, file transfer protocol [FFTP], internet information server (IIS), etc.), which 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 sAHD-9N/ASAHD-10device deleted/disabled?N/ASAHD-11internet information server (IIS), etc.), which are not required for the intended use of the device included 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?N/ASAHD-10device deleted/disabled?YesSAHD-11internal drive or memory component)?YesSAHD-12Can the device or hardware be installed on operational network security scanning by users?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14.1hardening? Are instructions available from vendor for increased SAHD-15NoSAHD-15.1bootoaders during boot?N/ASAHD-16.2Hardenling methods not included in YesSAHD-17.1hardening? Ar	SAHD-6.1		Yes	
SAHD-6.2privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device are all communication ports and protocols that are not required for the intended use of the deviceN/ASAHD-7Are all communication ports and protocols that are not required for the intended use of the device of the intended use of the device (FTP), internet information server (IIS), etc.), which are not required for the intended use of the device deleted/disabled?N/ASAHD-9Are 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?N/ASAHD-10device deleted/disabled?YesSAHD-11can the device orbhibit boot from uncontrolled or removable media (i.e., a source other than an internal five or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on operational network security scanning by users? SAHD-14NoSAHD-14.1provided state? Are instructions available from vendor for increased SAHD-15NoSAHD-15.4Boots during boot?YesHave additional hardening methods not included inNa		-		
Are all shared resources (e.g., flie shares) which are not required for the intended use of the device Are all communication ports and protocols that are not required for the intended use of the device (FTP), internet information server (IIS), etc.), which are not required for the intended use of the device SAHD-8N/ASAHD-8Are all services (e.g., telhet, file transfer protocol (FTP), internet information server (IIS), etc.), which are not required for the intended use of the device beleted/disabled?N/ASAHD-9deleted/disabled?N/ASAHD-10device deleted/disabled?N/ASAHD-10device deleted/disabled?YesSAHD-11internet splications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the removable media (i.e., a source other than an removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13on operational network security scanning by users?NoSAHD-14provided state? Are instructions available from vendor for increased Are instructions ava				
SAHD-7not required for the intended use of the device disabled?N/AAre all communication ports and protocols that are not required for the intended use of the device disabled?N/ASAHD-8disabled? Are all services (e.g., telnet, file transfer protocol are not required for the intended use of the device deleted/disabled?N/ASAHD-9deleted/disabled? deleted/disabled?N/ASAHD-10deleted/disabled? device deleted/disabled?N/ASAHD-10device deleted/disabled? device deleted/disabled?YesSAHD-11internol from uncontrolled or removable media (i.e., a source other than an internol drive or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on operational network security scanning by users? SAHD-14NoSAHD-14.1post the product documentation include information sort device be hardened beyond the default provided state?NoSAHD-14.1hardening? hardening the system prevent access to BIOS or other Have additional hardening methods not included inN/A	SAHD-6.2		Yes	
SAHD-7disabled?N/AAre all communication ports and protocols that are not required for the intended use of the device disabled?N/ASAHD-8disabled?N/AAre all services (e.g., telnet, file transfer protocol (FFP), internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?N/ASAHD-9deleted/disabled?N/AAre all applications (CDTS applications as well as OS- included applications (CDTS applications as well as OS- included applications (CDTS 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?YesSAHD-10Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an removable media (i.e.,				
SAHD-8not required for the intended use of the device disabled7N/ASAHD-9Are 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 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?N/ASAHD-10device deleted/disabled?YesSAHD-10can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users? Are instructions available from vendor for increased SAHD-14.NoSAHD-14.1Are instructions available from vendor for increased SAHD-15.NoSAHD-15.bootloaders during boot?Yes	SAHD-7	•	N/A	
SAHD-8disabled? Are all services (e.g., telnet, file transfer protocol [FFP], internet information server (IIS), etc.), which are not required for the intended use of the device deleted/disabled?N/ASAHD-9Are all applications, c.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?N/ASAHD-10device deleted/disabled?YesSAHD-11internal drive or memory component)?YesSAHD-12Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an on operational network security scanning by users) on operational network security scanning by users?NoSAHD-14Does the product documentation include information on operational network security scanning by users? Are instructions available from vendor for increased Are instructions available from vendor for increased SAHD-14.1No Are instructions available from vendor for increased Are instructions available from vendor for increased BAHD-15.No Are instructions available from vendor for increased No Are instructions available from vendor for increased FAHD-14.No Are instructions available from vendor for increased No Are instructions available from vendor for increased FAHD-15.No Are instructions available from vendor for increased No Are instructions available from vendor for increased FAHD-14.No Are instructions available from vendor for increased FAHD-14.Have additional hardening methods not included in FAHD-15.Have additional hardening methods not included in FAHD-16.Have additional hardening methods not included in FAHD-16.Have additional hardening methods not included				
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 beleted/disabled?N/ASAHD-9deleted/disabled? 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?N/ASAHD-10device deleted/disabled? termovable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users? Are instructions available from vendor for increased Are instructions available from vendor for increased SAHD-14.NoSAHD-15Can the device be hardened beyond the default provided state? Are instructions available from vendor for increased SAHD-15NoSAHD-15bootloaders during boot?YesHave additional hardening methods not included in Have additional hardening methods not included in termovent access to BIOS or other SHAD-15NoHave additional hardening methods not included in Have additional hardening methods not included in Have additional hardening methods not included in Have additional hardening methods not included inYes	SAHD-8		N/A	
SAHD-9are not required for the intended use of the device deleted/disabled?N/ASAHD-9Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?N/ASAHD-10device deleted/disabled?YesSAHD-11can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14.1Can the device be hardened beyond the default provided state?NoSAHD-15.Con the system prevent access to BIOS or other bootloaders during boot?NoHAD-15.Have additional hardening methods not included in provided state?NoHAD-15.Have addition	57412 5			
SAHD-9deleted/disabled?N/AAre 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?YesSAHD-10Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an removable media (i.e., a source other than and internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14.1Are instructions available from vendor for increased Are instructions available from vendor for increased bootloaders during boot?NoSHD-15.Bootloaders during boot?NoHAD-15Have additional hardening methods not include ding provided state?NoHAD-15Have additional hardening methods not included inYes				
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 vesYesSAHD-10Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users? Can the device be hardened beyond the default provided state?NoSAHD-14Porovided state? Can the system prevent access to BIOS or other SHAD-15NoSHD-15bootloaders during boot?N/AHave additional hardening methods not included inYes		•	NI / A	
SAHD-10included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?YesSAHD-10Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users?NoSAHD-14provided state? Are instructions available from vendor for increased SAHD-15NoSHAD-15Dootloaders during boot?N/A Yes	SAHD-9		N/A	
SAHD-10which are not required for the intended use of the device deleted/disabled?YesSAHD-10Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users?NoSAHD-14Can the device be hardened beyond the default Are instructions available from vendor for increased SHAD-15NoSHAD-15Dootloaders during boot?N/AHave additional hardening methods not include inYes				
Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11internal drive or memory component)?YesSAHD-12Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14Can the device be hardened beyond the default Are instructions available from vendor for increased SAHD-14.1NoSAHD-15bootloaders during boot?N/AHave additional hardening methods not included inYes		•		
SAHD-11removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users? Can the device be hardened beyond the default provided state? Are instructions available from vendor for increasedNoSAHD-14.1hardening? Can the system prevent access to BIOS or other SHAD-15N/AHave additional hardening methods not included inYes	SAHD-10	device deleted/disabled?	Yes	
SAHD-11removable media (i.e., a source other than an internal drive or memory component)?YesSAHD-11Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users? Can the device be hardened beyond the default provided state? Are instructions available from vendor for increasedNoSAHD-14.1hardening? Can the system prevent access to BIOS or other SHAD-15N/AHave additional hardening methods not included inYes		Can the device prohibit boot from uncontrolled or		
SAHD-12Can unauthorized software or hardware be installed on the device without the use of physical tools?NoSAHD-12Does the product documentation include information on operational network security scanning by users?NoSAHD-13Can the device be hardened beyond the default provided state? Are instructions available from vendor for increased SAHD-14.1NoSAHD-14.1hardening? Can the system prevent access to BIOS or other SHAD-15N/AHave additional hardening methods not included inYes				
SAHD-12on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14Can the device be hardened beyond the default provided state? Are instructions available from vendor for increasedNoSAHD-14.1hardening? Can the system prevent access to BIOS or other SHAD-15N/AHave additional hardening methods not included inYes	SAHD-11	internal drive or memory component)?	Yes	
SAHD-12on the device without the use of physical tools?NoSAHD-13Does the product documentation include information on operational network security scanning by users?NoSAHD-14Can the device be hardened beyond the default provided state? Are instructions available from vendor for increasedNoSAHD-14.1hardening? Can the system prevent access to BIOS or other SHAD-15N/AHave additional hardening methods not included inYes		Can unauthorized software or hardware he installed		
SAHD-13Does the product documentation include information on operational network security scanning by users? Can the device be hardened beyond the default provided state? Are instructions available from vendor for increased SAHD-14.1 Can the system prevent access to BIOS or other SHAD-15NoSHAD-15bootloaders during boot?N/AHave additional hardening methods not included inYes	SAHD-12		No	
SAHD-13 on operational network security scanning by users? No Can the device be hardened beyond the default No SAHD-14 provided state? No Are instructions available from vendor for increased No SAHD-14.1 hardening? N/A Can the system prevent access to BIOS or other Yes SHAD-15 bootloaders during boot? Yes				
Can the device be hardened beyond the defaultNoSAHD-14provided state?NoAre instructions available from vendor for increasedN/ASAHD-14.1hardening?N/ACan the system prevent access to BIOS or otherYesSHAD-15bootloaders during boot?Yes				
SAHD-14 provided state? No Are instructions available from vendor for increased No SAHD-14.1 hardening? N/A Can the system prevent access to BIOS or other N/A SHAD-15 bootloaders during boot? Yes	SAHD-13		No	
Are instructions available from vendor for increased N/A SAHD-14.1 hardening? Can the system prevent access to BIOS or other V/A SHAD-15 bootloaders during boot? Have additional hardening methods not included in Ves	SAHD-14	•	No	
SHAD-15 Can the system prevent access to BIOS or other bootloaders during boot? Yes Have additional hardening methods not included in Yes				
SHAD-15 bootloaders during boot? Yes Have additional hardening methods not included in	SAHD-14.1	6	N/A	
Have additional hardening methods not included in			Ves	
	CT-UNITC	שטטנוסמעכוז עעוווא שטטני	100	
SAHD-16 2.3.19 been used to harden the device? N/A		Have additional hardening methods not included in		
	SAHD-16	2.3.19 been used to harden the device?	N/A	

Nanosonics	AuditPro	A697132	20-Jul-2021
	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? Does the device have the capability, and provide instructions, for the permanent deletion of data from	Yes	
SGUD-2	the device or media?	No	
SGUD-3	Are all access accounts documented? Can the owner/operator manage password control	Yes	
SGUD-3.1	for all accounts?	See Notes	Cloud application - no, mobile scanning device - yes
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	? No	We have no critical or major vulnerabilities in the application and we haven't mitigated with alternative control for critical security features
	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?	Yes	
STCF-1.1	Is all data encrypted or otherwise protected? Is the data encryption capability configured by	Yes	
STCF-1.2	default? Are instructions available to the customer to	Yes	
STCF-1.3	configure encryption?	No	
STCF-2	Can the encryption keys be changed or configured?	No	
STCF-3	Is the data stored in a database located on the device? Is the data stored in a database external to the	See Notes	Mobile device, yes Cloud application information stored on server Mobile device, No
STCF-4	device?	See Notes	Cloud application, yes
	TRANSMISSION CONFIDENTIALITY (TXCF)		

	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.	
	Can personally identifiable information be	
	transmitted only via a point-to-point dedicated	
TXCF-1	cable?	No
	Is personally identifiable information encrypted prior	
TXCF-2	to transmission via a network or removable media?	Yes
	If data is not encrypted by default, can the customer	
TXCF-2.1	configure encryption options?	N/A

Is personally identifiable information transmission

TXCF-3 restricted to a fixed list of network destinations? Yes

TXCF-4 Are connections limited to authenticated systems? Yes

Are secure transmission methods

TXCF-5 supported/implemented (DICOM, HL7, IEEE 11073)? No

TRANSMISSION INTEGRITY (TXIG)

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

Nanosonics	AuditPro	A697132	20-Jul-2021
TXIG-1 TXIG-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?	Yes No	

	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?	Νο	
	Is there an indicator for an enabled and active		
RMOT-1.2	remote session? Can patient data be accessed or viewed from the	Yes	Procedure identifers may be, but they will be
RMOT-1.3	device during the remote session?	See Notes	hashed
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No	
	Does the device have any other remotely accessible functionality (e.g. software updates, remote		
RMOT-3	training)?	Yes	Updates can occur over the air / remotely

OTHER SECURITY CONSIDERATIONS (OTHR)

Notes:

Example note. Please keep individual notes to one cell. Please use separate notes for separate information

Note 1