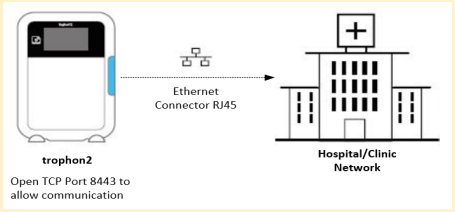
Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Nanosonics Limited | trophon2 - Software Version: v1.6 | Objective ID: A601330 | 24-Apr-2023

Question ID	Question		See note
DOC-1	Manufacturer Name	Nanosonics Limited	—
DOC-2	Device Description	Automated High Level Disinfection System for Ultrasound Probes	—
DOC-3	Device Model	trophon2 - Software Version: v1.6	—
DOC-4	Document ID	Objective ID: A601330	—
DOC-5	Manufacturer Contact Information	7-11 Talavera Road, Macquarie Park NSW 2113 Australia T: +61 2 8063 1600, E: customerservice@nanosonics.com.au	—
DOC-6	Intended use of device in network-connected environment:	The trophon2 device is a stand-alone high-level disinfection medical device with embedded software. The device does not store electronic Protected Health Information (ePHI). There are no other related software or other components that need to be installed or configured for the device to operate. Data about the disinfection cycles completed by the trophon2 device are stored in the device and accessible (read only) via a thermal printer, download to USB Drive, or via a network connection. Data is accessible (read only) to 3rd party applications over the network. Security is provided via user-level authentication with TLS and X.509 certificates.	—
DOC-7	Document Release Date	24/04/2023	—
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	Nanosonics is an ISO 27001 compliant organisation and has existing vulnerability management policies and procedures as part of its Information Security Management System (ISMS).
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	No	
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?		—
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	
DOC-11.1	Does the SaMD contain an operating system?	N/A	
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.4	Is the SaMD hosted by the customer?	N/A	—
		Yes, No, N/A, or See Note	Note #
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	The trophon2 device does not maintain ePHI, however it does maintain PII, as the Operator Name is recorded with each disinfection cycle when the AcuTrace feature is enabled.
MPII-2	Does the device maintain personally identifiable information?	Yes	The trophon2 device does not maintain ePHI, however it does maintain PII, as the Operator Name is recorded with each disinfection cycle when the AcuTrace feature is enabled.
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	—
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	—
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	—
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	—
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	No	—
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)?	No	—
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	Disinfection records for recently completed HLD cycles can be reviewed on the trophon2 device, where the Operator Name is recorded.
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	A service technician is able to retrieve a copy of HLD cycle logs, which contain the Operator Name as part of the cycle, probe, operator data for each cycle.

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330	24-Apr-2023

MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	Using the 3rd party web service interface, customer can retrieve the information and store in their server.
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	The trophon2 device allows for the export of HLD cycle logs in a .csv format via USB connection. The cycle logs contain the Operator Name allocated to different steps of each cycle.
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	—
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	Yes	—
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	Yes	—
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	Yes	—
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, 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.)?	No	—
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	—
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	Yes	Customer-facing HLD cycle logs can be downloaded via USB and Technical HLD cycle logs can be downloaded via S&M.
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	Yes	Customer-facing HLD cycle logs can be downloaded via USB and Technical HLD cycle logs can be downloaded via S&M.

Management of Private Data notes:

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.

ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	N/A	The trophon2 device does not use passwords to restrict access to system operation upon initial login. Passwords are not used to facilitate operation of the trophon2 device.
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	N/A	The trophon2 device does not use passwords to restrict access to system operation upon initial login. Passwords are not used to facilitate operation of the trophon2 device.

AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the device.

AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	The trophon2 device produces customer-facing HLD logs that can be downloaded via USB in a .csv file format. These cycle logs can be used for audit purposes.
AUDT-1.1	Does the audit log record a USER ID?	Yes	—
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	—
AUDT-2.1	Successful login/logout attempts?	N/A	—
AUDT-2.2	Unsuccessful login/logout attempts?	N/A	—
AUDT-2.3	Modification of user privileges?	N/A	—
AUDT-2.4	Creation/modification/deletion of users?	N/A	—
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	No	—
AUDT-2.6	Creation/modification/deletion of data?	Yes	—
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	—
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	—
AUDT-2.8.1	Remote or on-site support?	Yes	—
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	—
AUDT-2.9	Emergency access?	N/A	—
AUDT-2.10	Other events (e.g., software updates)?	Yes	—
AUDT-2.11	Is the audit capability documented in more detail?	Yes	The trophon2 device produces technical HLD cycle logs which can be downloaded by an authorised technician via S&M.
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330	24-Apr-2023
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	—
AUDT-4.1	Does the audit log record date/time?	Yes	—
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	—
AUDT-5	Can audit log content be exported?	Yes	—
AUDT-5.1	Via physical media?	Yes	—
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	N/A	—
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	Yes	—
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	No	—
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	—
AUDT-7	Are audit logs protected from modification?	Yes	—
AUDT-7.1	Are audit logs protected from access?	No	—
AUDT-8	Can audit logs be analyzed by the device?	No	Audit logs can be displayed on the trophon2 display screen.

AUTHORIZATION (AUTH)

The ability of the device to determine the authorization of users.

AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	See Notes	Operators require a programmed (RFID) 'trophon AcuTrace Operator Card' to initiate disinfection cycles if AcuTrace is utilized, otherwise this can be done via the device touch screen.
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	N/A	—
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	N/A	—
AUTH-1.3	Are any special groups, organizational units, or group policies required?	N/A	—
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	No	—
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	No	—
AUTH-4	Does the device authorize or control all API access requests?	Yes	Communication via API is protected by certificates.
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?	No	Security-related updates will be made as required. To update the device, an authorized service technician will be required to perform a software upgrade manually on the device. Software upgrades to the latest firmware is a mandatory requirement for devices undergoing an annual preventative maintenance and/or repair process.
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?	No	—
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?	N/A	—
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	—
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	—
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—

Nanosonics Limited | trophon2 - Software Version: v1.6 | Objective ID: A601330 | 24-Apr-2023

CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	No	—
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	Security-related updates will be made as required. To update the device, an authorized service technician will be required to perform a software upgrade manually on the device. Software upgrades to the latest firmware is a mandatory requirement for devices undergoing an annual preventative maintenance and/or repair process.
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—
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?	N/A	—
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?	No	—
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?	No	—
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	—
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	—
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	See Notes	Security-related updates will be made as required. To update the device, an authorized service technician will be required to perform a software upgrade manually on the device. Software upgrades to the latest firmware is a mandatory requirement for devices undergoing an annual preventative maintenance and/or repair process.
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	Customers are notified after the software of their device has been upgraded. Security-related updates will be made as required. To update the device, an authorized service technician will be required to perform a software upgrade manually on the device. Software upgrades to the latest firmware is a mandatory requirement for devices undergoing an annual preventative maintenance and/or repair process.
CSUP-8	Does the device perform automatic installation of software updates?	No	—
CSUP-9	Does the manufacturer have an approved list of third-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?	N/A	—
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	—
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	—
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	—
CSUP-11.2	Is there an update review cycle for the device?	Yes	

HEALTH DATA DE-IDENTIFICATION (DIDT)

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330		24-Apr-2023

	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?	No	—
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	N/A	—
	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)?	Yes	The trophon2 device maintains long term primary storage of PII of the device operator in the form of the 'Operator Name' recorded in trophon HLD cycle logs.
DTBK-2	Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?	Yes	—
DTBK-3	Does the device have an integral data backup capability to removable media?	No	—
DTBK-4	Does the device have an integral data backup capability to remote storage?	No	
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes	The trophon2 device maintains storage of cycle data following a software upgrade, however Nanosonics recommends that customers perfom a manual export of cycle logs prior to preventative maintenance/ annual service of the device.
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	N/A	—
	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?	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 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)?	N/A	—
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	N/A	—
	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?	N/A	—
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	No	—
MLDP-2.1	Does the device include anti-malware software by default?	No	—
MLDP-2.2	Does the device have anti-malware software available as an option?	No	—
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	N/A	—
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	—
MLDP-2.5	Does notification of malware detection occur in the device user interface?	N/A	—
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	N/A	—
MLDP-2.7	Are malware notifications written to a log?	N/A	—
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	N/A	—

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330	24-Apr-2023
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	By product design, access to the system is protected by the front cover of the trophon2 device. Users would have to physically damage the device front cover to obtain access to the system, which is password-protected.
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	N/A	__
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	N/A	__
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	__
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	N/A	__
	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	Using mutual authentication with TLS and X.509 certificates.
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	See Notes	Only white-listed ports are enabled.
NAUT-2.1	Is the firewall ruleset documented and available for review?	See Notes	Only white-listed ports are enabled.
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	__
	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	Ethernet cable
CONN-1.1	Does the device support wireless connections?	No	__
CONN-1.1.1	Does the device support Wi-Fi?	No	__
CONN-1.1.2	Does the device support Bluetooth?	No	__
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	__
CONN-1.1.4	Does the device support other wireless connections (e.g., 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	__
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	__
CONN-1.2.4	Does the device support other physical connectivity?	No	__
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	(HTTPS) TCP port 8443 (NTP) UDP port 123 (NDS) UDP port 53
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	The trophon2 device can connect with the facility network (e.g. with the NTP within the customer environment), however this is not a requirement to facilitate operation of the device.
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	__
CONN-5	Does the device make or receive API calls?	Yes	__
CONN-6	Does the device require an internet connection for its intended use?	No	__
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	__
CONN-7.1	Is TLS configurable?	No	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	__
	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)?	N/A	Operators require a programmed (RFID) 'trophon AcuTrace Operator Card' to initiate disinfection cycles if AcuTrace is utilized, otherwise this can be done via the device touch screen. No passwords are required.

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330		24-Apr-2023
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	N/A		
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	N/A		
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	N/A		
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	N/A		
PAUT-5	Can all passwords be changed?	N/A	The trophon2 device does not utilise passwords to facilitate device operation.	
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	N/A	The trophon2 device does not utilise passwords to facilitate device operation.	
PAUT-7	Does the device support account passwords that expire periodically?	N/A	The trophon2 device does not utilise passwords to facilitate device operation.	
PAUT-8	Does the device support multi-factor authentication?	N/A		
PAUT-9	Does the device support single sign-on (SSO)?	N/A		
PAUT-10	Can user accounts be disabled/locked on the device?	N/A		
PAUT-11	Does the device support biometric controls?	N/A		
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No		
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No		
PAUT-14	Does the application or device store or manage authentication credentials?	No		
PAUT-14.1	Are credentials stored using a secure method?	N/A		
	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.	No		
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes		
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	See Notes	By product design, access to the trophon2 device components is protected by the front cover. Users would have to physically damage the front cover to obtain access to the device components.	
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No		
	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?	Yes		
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes		
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes		
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes		
	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.			
SBOM-1	Is the SBoM for this product available?	Yes		
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes		
SBOM-2.1	Are the software components identified?	Yes		
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes		
SBOM-2.3	Are the major version numbers of the software components identified?	Yes		
SBOM-2.4	Are any additional descriptive elements identified?	N/A		

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330	24-Apr-2023
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No	—
SBOM-4	Is there an update process for the SBoM?	Yes	—
	SYSTEM AND APPLICATION HARDENING (SAHD) *The device's inherent resistance to cyber attacks and malware.*		
			The trophon2 device has been developed in compliance with IEC 62304:2006+AMD1:2015. Medical device software - Software life cycle processes. The trophon2 device has X.509 Certificates installed. The device accepts incoming connection using TLS and with mutual authentication. Ports used by the trophon2 device are white-listed and where appropriate are restricted to localhost.
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	
SAHD-2	Has the device received any cybersecurity certifications?	Yes	—
SAHD-3	Does the device employ any mechanisms for software 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?	Yes	—
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	—
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	—
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	—
SAHD-5.1	Does the device provide role-based access controls?	No	—
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	N/A	—
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	N/A	—
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	N/A	—
SAHD-7	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 all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	—
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	Yes	—
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?	N/A	—
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?	N/A	—
SAHD-14	Can the device be hardened beyond the default provided state?	No	—
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A	Security-related updates will be made as required. To update the device, an authorized service technician will be required to perform a software upgrade manually on the device. Software upgrades to the latest firmware is a mandatory requirement for devices undergoing an annual preventative maintenance and/or repair process.
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	See Notes	By product design, access to BIOS is prevented by the front cover of the trophon2 device. Users would have to physically damage the device front cover to obtain access.
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	N/A	—
	SECURITY GUIDANCE (SGUD)		

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330		24-Apr-2023
	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?	No	__	
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	No	__	
SGUD-3	Are all access accounts documented?	N/A	__	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	N/A	__	
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	N/A	__	
	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?	No	__	
STCF-1.1	Is all data encrypted or otherwise protected?	No		
STCF-1.2	Is the data encryption capability configured by default?	N/A		
STCF-1.3	Are instructions available to the customer to configure encryption?	N/A		
STCF-2	Can the encryption keys be changed or configured?	N/A	__	
STCF-3	Is the data stored in a database located on the device?	Yes	__	
STCF-4	Is the data stored in a database external to the device?	No	__	
	TRANSMISSION CONFIDENTIALITY (TXCF)			
	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.			
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	Yes	__	
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	Transmission via network is using TLS protocol while downloading to removable media is not encrypted. The downloaded data in removable media is in read-only mode.	
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	No	__	
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	N/A	__	
TXCF-4	Are connections limited to authenticated systems?	Yes	__	
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	N/A	__	
	TRANSMISSION INTEGRITY (TXIG)			
	The ability of the device to ensure the integrity of transmitted data.			
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes	Using mutual TLS authentication.	
TXIG-2	Does the device include multiple sub-components connected by external cables?	See Notes	The trophon Printer can be connected to the trophon2 device to support the printing of HLD cycle records for paper-based record-keeping. The trophon Printer is connected to the trophon2 device by external cables. The trophon Printer is an accessory to the trophon2 device.	

	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?	No	__
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	No	__
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A	__
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	N/A	__
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No	__

Nanosonics Limited	trophon2 - Software Version: v1.6	Objective ID: A601330	24-Apr-2023

RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes

OTHER SECURITY CONSIDERATIONS (OTHR)

NONE

Notes:

Note 1	Example note. Please keep individual notes to one cell. Please use separate notes for separate information