# 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 | |
| DOC-6 | Intended use of device in network-connected environment: | The intended use of mobile scanning device is to collect data from trophon2 and send data to AuditPro database in cloud by establising secure connection | |
| DOC-7 | Document Release Date | 20/07/2021 | |
| DOC-8 | Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device? | No | |
| DOC-9 | ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization? | No | Not currently part of an ISAO - looking to change this moving forward |
| DOC-10 | Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources? | Yes | Contained within product packaging |
| DOC-11 | SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)? | Yes | AuditPro is a class one medical device exempt from FDA filing - hardware is supplied (honeywell device). |
| DOC-11.1 | Does the SaMD contain an operating system? | Yes | Android device operating system which is maintained by Nanosonics remotely |
| DOC-11.2 | Does the SaMD rely on an owner/operator provided operating system? | No | It uses the honeywell operating system running on the Android platform. |
| DOC-11.3 | Is the SaMD hosted by the manufacturer? | Yes | The application is hosted in secure AWS HIPAA 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** | | |
| MPII-1 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? | See Notes | AuditPro collects PII e.g. t2/AuditPro users name (if they chose to use their names), position, department, facility name, address, mobile# |
| MPII-2 | Does the device maintain personally identifiable information? | See Notes | Yes. AudtiPro maintains the PII data in the secured cloud database and the data is regularly back up. |
| MPII-2.1 | Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? | Yes | AuditPro mobile scanning device temporily maintain the PII in its internal memory until the data is sent successfully sent to the cloud. |
| MPII-2.2 | Does the device store personally identifiable information persistently on internal media? | See Notes | If operators chose to use their real name, then yes, PII is termorarily stored on the MSD before being sent to the cloud application |
| MPII-2.3 | Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased? | No | |
| MPII-2.4 | Does the device store personally identifiable information in a database? | See Notes | The mobile application does not collect or store and PII, however the cloud application collects, stores and displays PII related to the user accounts. |
| 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)? | See Notes | If users chose to use their names as operator IDs, then yes, Imported PII (t2 user names, ID) from t2 |
| MPII-2.7 | Does the device maintain personally identifiable information when powered off, or during power service interruptions? | Yes | |
| 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)? | See Notes | Device doesn't allow internal media to be removed. Once user is unsubscribed, device will be clean wiped by service techician |
| 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 | |
| MPII-3 | Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information? | Yes | |
| 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 | User accounts only |
| 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.)? | No | |
| MPII-3.4 | Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)? | No | |
| MPII-3.5 | Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)? | No | |
| MPII-3.6 | Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)? | Yes | Only if users chose to use their own names as operator IDs |
| MPII-3.7 | Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)? | Yes | If the cloud application is used by customers to view or modify email address, data will be transmitted over internet |
| 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 | Only if users chose to use their own names as operator IDs |
| MPII-3.10 | Does the device use any other mechanism to transmit, import or export personally identifiable information? | No | |

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.* | Yes | Idle log off time is 20 minutes<br>2 minute screen lock for mobile device |
| ALOF-1 | Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? | Yes | Idle log off time is 20 minutes<br>2 minute screen lock for mobile device |
| ALOF-2 | Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? | No | Meets OWASP standard |

## 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 | Cloud based application stores full system logs |
| AUDT-1.1 | Does the audit log record a USER ID? | Yes | USER IDs are recorded for any information updates / edits. |
| AUDT-1.2 | Does other personally identifiable information exist in the audit trail? | Yes | |
| AUDT-2 | Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log: | Yes | Currently any changes to editable fields within the application will be logged, more features will be 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? | Yes | Managed by the facility Admin |
| AUDT-2.4 | Creation/modification/deletion of users? | Yes | Deletion of users is not allowed as AuditPro is tracking software. Users can be anonymised. Users can modify their own accounts |
| AUDT-2.5 | Presentation of clinical or PII data (e.g. display, print)? | No | |
| AUDT-2.6 | Creation/modification/deletion of data? | Yes | Modification and creation are logged. Deletion of data is not allowed. |
| AUDT-2.7 | Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)? | N/A | |
| AUDT-2.8 | Receipt/transmission of data or commands over a network or point-to-point connection? | See Notes | Important data - yes, not for commands (e.g. a get call). |
| AUDT-2.8.1 | Remote or on-site support? | Yes | Remote support provided by Nanosonics service team |
| AUDT-2.8.2 | Application Programming Interface (API) and similar 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? | Yes | Audit and Logging Policy |
| AUDT-3 | Can the owner/operator define or select which events are recorded in the audit log? | No | |
| 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? | No | Timezone comes from user input during registration (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 |
| AUDT-5.2 | Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM? | No | |
| AUDT-5.3 | Via Other communications (e.g., external service device, mobile applications)? | No | |
| AUDT-5.4 | Are audit logs encrypted in transit or on storage media? | Yes | |
| 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? | Yes | |
| AUDT-8 | Can audit logs be analyzed by the device? | No | |

## 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? | Yes | |
| AUTH-1.1 | Can 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? | No | | |
| AUTH-2 | Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)? | See Notes | Cloud application - yes, mobile scanning device - no, only one password per device | |
| 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 | | |
| AUTH-5 | Does the device run in a restricted access mode, or 'kiosk mode', by default? | Yes | | |

**CYBER SECURITY PRODUCT UPGRADES (CSUP)**

*The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.*

| | | | |
|---|---|---|---|
| CSUP-1 | Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section. | Yes | |
| CSUP-2 | Does the device contain an Operating System? If yes, complete 2.1-2.4. | Yes | |
| CSUP-2.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates? | Yes | |
| CSUP-2.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | No | |
| CSUP-2.3 | Does the device have the capability to receive remote installation of patches or software updates? | Yes | |
| CSUP-2.4 | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? | No | |
| 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? | Yes | |
| CSUP-3.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | No | |
| CSUP-3.3 | Does the device have the capability to receive remote installation of patches or software updates? | Yes | |
| 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. | See Notes | No software, managed by MDM. Device is set up to only be used in KIOSK mode for security. |
| 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? | N/A | |

| | | | |
|---|---|---|---|
| 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. | No | |
| CSUP-5.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates? | N/A | |
| CSUP-5.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | N/A | |
| CSUP-5.3 | Does the device have the capability to receive remote installation of patches or software updates? | N/A | |
| 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? | N/A | |
| CSUP-6 | Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4. | No | |
| CSUP-6.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates? | N/A | |
| CSUP-6.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | N/A | |
| CSUP-6.3 | Does the device have the capability to receive remote installation of patches or software updates? | N/A | |
| 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? | N/A | |
| CSUP-7 | Does the manufacturer notify the customer when updates are approved for installation? | Yes | |
| CSUP-8 | Does the device perform automatic installation of software updates? | Yes | |
| CSUP-9 | Does the manufacturer have an approved list of third-party software that can be installed on the device? | Yes | |
| CSUP-10 | Can the owner/operator install manufacturer-approved third-party software on the device themselves? | No | |
| 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? | Yes | |
| CSUP-11.2 | Is there an update review cycle for the device? | Yes | |

**HEALTH DATA DE-IDENTIFICATION (DIDT)**

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

| | | | |
|---|---|---|---|
| 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)**<br>*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 cloud application does, mobile scanning device does not. |
| 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? | No | |
| DTBK-6 | Does the device provide the capability to check the integrity and authenticity of a backup? | No | |
| | **EMERGENCY ACCESS (EMRG)**<br>*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)**<br>*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)? | Yes | |
| IGAU-2 | Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? | See Notes | Backup available for the cloud application<br>Not available for the mobile application |
| | **MALWARE DETECTION/PROTECTION (MLDP)**<br>*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 | Only APK |
| 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? | No | |
| 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? | No | |
| MLDP-2.6 | Can only manufacturer-authorized persons repair systems when malware has been detected? | Yes | |
| MLDP-2.7 | Are malware notifications written to a log? | 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 | Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device? | Yes | |
| MLDP-5 | Does the device employ a host-based intrusion detection/prevention system? | No | |
| MLDP-5.1 | Can the host-based intrusion detection/prevention system be configured by the customer? | No | |
| MLDP-5.2 | Can a host-based intrusion detection/prevention system be installed by the customer? | No | |

## 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)? | See Notes | Mobile device: No<br>Cloud application: Yes, we have white listing and a segmented network design. |
| NAUT-2.1 | Is the firewall ruleset documented and available for review? | N/A | Mobile device is proprietary and managed by reputable vendor HEM. |
| 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? | 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 | Device supports bluetooth but disabled by Nanosonics |
| 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)? | 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 | |
| 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) |
| CONN-1.2.3 | Does the device require, use, or support removable memory devices? | No | |
| 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 | |
| CONN-3 | Can the device communicate with other systems within the customer environment? | Yes | |
| CONN-4 | Can the device communicate with other systems external to the customer environment (e.g., a service host)? | Yes | |
| CONN-5 | Does the device make or receive API calls? | Yes | |
| CONN-6 | Does the device require an internet connection for its intended use? | Yes | |
| 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)? | See Notes | Cloud application - yes, mobile scanning device - no, only one password per device |
| PAUT-1.1 | Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? | See Notes | Cloud application - yes through email verification, mobile scanning device - no, only one password per device, no verification |
| PAUT-2 | Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? | No | |
| PAUT-3 | Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? | Yes | |
| PAUT-4 | Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation? | Yes | |
| PAUT-5 | Can all passwords be changed? | Yes | |
| PAUT-6 | Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules? | Yes | Cloud application - yes, mobile scanning device - no |
| PAUT-7 | Does the device support account passwords that 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 | |
| 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? | See Notes | Cloud application - yes, mobile scanning device - no |

| | | | |
|---|---|---|---|
| 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)**<br>*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. | Yes | There is a physical Mobile Scanning Device, however the product is a software package on this device. Without access, there is no information that can be leaked. |
| PLOK-2 | Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)? | N/A | |
| PLOK-3 | Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device? | N/A | |
| PLOK-4 | Does the device have an option for the customer to attach a physical lock to restrict access to removable media? | N/A | |
| | **ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**<br>*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)**<br>*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? | No | |
| SBOM-2 | Does the SBoM follow a standard or common method in describing software components? | N/A | |
| SBOM-2.1 | Are the software components identified? | N/A | |
| SBOM-2.2 | Are the developers/manufacturers of the software components identified? | N/A | |
| SBOM-2.3 | Are the major version numbers of the software components identified? | N/A | |
| SBOM-2.4 | Are any additional descriptive elements identified? | N/A | |
| SBOM-3 | Does the device include a command or process method available to generate a list of software components installed on the device? | N/A | |
| SBOM-4 | Is there an update process for the SBoM? | N/A | |

| | | | |
|---|---|---|---|
| | **SYSTEM AND APPLICATION HARDENING (SAHD)**<br>*The device's inherent resistance to cyber attacks and malware.* | | |
| SAHD-1 | Is the device hardened in accordance with any industry standards? | Yes | AWS compliances |
| SAHD-2 | Has the device received any cybersecurity certifications? | Yes | OWASP. PEN testing carried out on web application & device application |
| SAHD-3 | Does the device employ any mechanisms for software integrity checking | Yes | |
| 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? | Yes | |
| 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 delivery? | Yes | e.g. non work emails (public emails blocked) |
| SAHD-6.1 | Are any system or user accounts configurable by the end user after initial configuration? | Yes | |
| SAHD-6.2 | Does this include restricting certain system or user accounts, such as service technicians, to least privileged access? | Yes | |
| 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? | N/A | |
| 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? | N/A | |
| SAHD-10 | Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? | Yes | |
| SAHD-11 | Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? | Yes | |
| SAHD-12 | Can unauthorized software or hardware be installed on the device without the use of physical tools? | No | |
| SAHD-13 | Does the product documentation include information on operational network security scanning by users? | No | |
| SAHD-14 | Can the device be hardened beyond the default provided state? | No | |
| SAHD-14.1 | Are instructions available from vendor for increased hardening? | N/A | |
| SHAD-15 | Can the system prevent access to BIOS or other bootloaders during boot? | Yes | |
| SAHD-16 | Have additional hardening methods not included in 2.3.19 been used to harden the device? | N/A | |

## 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? | Yes | |
| 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? | Yes | |
| SGUD-3.1 | Can the owner/operator manage password control 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? | Yes | |
| STCF-1.2 | Is the data encryption capability configured by default? | Yes | |
| STCF-1.3 | Are instructions available to the customer to 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? | See Notes | Mobile device, yes<br>Cloud application information stored on server |
| STCF-4 | Is the data stored in a database external to the device? | See Notes | Mobile device, No<br>Cloud application, yes |

## 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? | No | |
| TXCF-2 | Is personally identifiable information encrypted prior to transmission via a network or removable media? | Yes | |
| TXCF-2.1 | If data is not encrypted by default, can the customer configure encryption options? | N/A | |
| TXCF-3 | Is personally identifiable information transmission restricted to a fixed list of network destinations? | Yes | |
| TXCF-4 | Are connections limited to authenticated systems? | Yes | |
| TXCF-5 | Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? | No | |

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

**OTHER SECURITY CONSIDERATIONS (OTHR)**

*NONE*

**Notes:**

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