# MANUFACTURER DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY

# TOMTEC-ARENA TTA2.50

© 2021 TOMTEC Imaging Systems GmbH
All rights reserved.

TOMTEC-ARENA is a trademark of TOMTEC Imaging Systems GmbH.
All other trademarks are the property of their respective owners.

# Table of contents

# 1 OVERVIEW

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) provides information about the security controls that are implemented in a medical device in order to protect health information (PHI) transmitted or stored by the medical device.

This document is based on ANSI/NEMA HN 1-2019 American National Standard for Manufacturer Disclosure Statement for Medical Device Security.

# 2 DISCLOSURE STATEMENT

## 2.1 DEVICE DESCRIPTION

| Question ID | Question | Answer | Note |
|---|---|---|---|
| DOC-1 | Manufacturer Name | TOMTEC Imaging Systems GmbH | |
| DOC-2 | Device Description | TOMTEC-ARENA is a clinical software package for reviewing, quantifying and reporting digital medical data. The software can be integrated into third party platforms.<br><br>Platforms enhance the workflow by providing the database, import, export and other services. All analyzed data and images will be transferred to the platform for archiving, reporting and statistical quantification purposes.<br><br>TOMTEC-ARENA consists of the following optional clinical application packages:<br>• IMAGE-COM<br>• 4D LV-ANALYSIS<br>• 4D RV-FUNCTION<br>• 4D CARDIO-VIEW<br>• 4D MV-ASSESSMENT<br>• 4D SONO-SCAN<br>• 2D CPA<br>• FETAL 2D CPA<br>• AutoStrain LV / SAX / RV / LA<br>• REPORTING<br>• TOMTEC DATACENTER (incl. STUDYLIST, DATA MAINTANANCE, WEB REVIEW) | |
| DOC-3 | Device Model | TOMTEC-ARENA TTA2.50.xx | |
| DOC-4 | Document ID | D.39.0266-01 | |
| DOC-5 | Manufacturer Contact Information | TOMTEC Imaging Systems GmbH<br>Freisinger Strasse 9<br>85716 Unterschleissheim<br>Germany | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| | | Phone: +49 89 321 75 500<br>Fax: +49 89 321 75 750<br>Support Hotline: + 49 89 321 75 740<br>E-Mail: support@tomtec.de<br><br>See also A.17.0313-01 MD Label Information TTA2.50 for a detailed list of local representatives. | |
| DOC-6 | Intended use of device in network-connected environment | TOMTEC-ARENA software is a clinical software package designed for review, quantification and reporting of structures and function based on multi-dimensional digital medical data acquired with different modalities.<br><br>TOMTEC-ARENA is not intended to be used for reading of mammography images. | |
| DOC-7 | Document Release Date | 2021-11-08 | |
| DOC-8 | Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device? | Yes | TOMTEC discloses vulnerabilities with security risk MEDIUM or higher directly to the affected customers. |
| 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? | Yes | See Administration Guide document for information. |
| DOC-11 | SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)? | Yes | |
| DOC-11.1 | Does the SaMD contain an operating system? | No | |
| DOC-11.2 | Does the SaMD rely on an owner/operator | Yes | See Technical Specification |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| | provided operating system? | | document for information. |
| DOC-11.3 | Is the SaMD hosted by the manufacturer? | No | |
| DOC-11.4 | Is the SaMD hosted by the customer? | Yes | |

## 2.2 MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION

*How personally identifiable information is handled on or by the device.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| MPII-1 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? | Yes | |
| MPII-2 | Does the device maintain personally identifiable information? | Yes | |
| 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? | Yes | |
| MPII-2.6 | Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)? | Yes | |
| MPII-2.7 | Does the device maintain personally identifiable information when powered off, or during power service interruptions? | 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)? | Yes | |
| 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)? | Yes | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | |
| 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.)? | No | |
| 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.)? | Yes | |
| 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? | No | |
| MPII-3.10 | Does the device use any other mechanism to transmit, import or export personally identifiable information? | No | |

## 2.3 AUTOMATIC LOGOFF

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | See Administration Guide document for information. |

| | | | |
|---|---|---|---|
| ALOF-2 | Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? | Yes | See Administration Guide document for information. |

## 2.4 AUDIT CONTROLS

*The ability to reliably audit activity on the device.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| AUDT-1 | Can the medical device create additional audit logs or reports beyond standard operating system logs? | Yes | |
| 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? | 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 | |
| AUDT-2.1 | Successful login/logout attempts? | Yes | |
| AUDT-2.2 | Unsuccessful login/logout attempts? | Yes | |
| AUDT-2.3 | Modification of user privileges? | No | |
| AUDT-2.4 | Creation/modification/deletion of users? | No | |
| AUDT-2.5 | Presentation of clinical or PII data (e.g. display, print)? | Yes | |
| AUDT-2.6 | Creation/modification/deletion of data? | Yes | The audit log records the following events:<br>• Study Creation<br>• Study Deletion<br>• Patient Creation<br>• Patient Update<br>• Patient Merge<br>• Patient Deletion<br>• Order Creation<br>• Order Update<br>• Order Deletion |
| AUDT-2.7 | Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)? | No | |
| 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? | No | |
| 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)? | No | |
| AUDT-2.11 | Is the audit capability documented in more detail? | Yes | See Administration Guide document for information. |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | See Administration Guide document for information. |
| 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? | No | |
| AUDT-5.1 | Via physical media? | No | |
| 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? | 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? | Yes | Access to audit log requires administrator privileges. |
| AUDT-8 | Can audit logs be analysed by the device? | No | |

## 2.5 AUTHORIZATION

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| AUTH-1 | Does the device prevent access to unauthorized users through user login requirements or other mechanism? | Yes | Username and password are required for access. |
| AUTH-1.1 | Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)? | No | |
| 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.)? | Yes | |
| 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)? | Yes | TOMTEC-ARENA supports more than one privileged account. There are no restrictions on users |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| | | | regarding the use of administrator accounts. |
| 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 | Login is always required to use TOMTEC-ARENA. |

## 2.6 CYBERSECURITY PRODUCT UPGRADES

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | TOMTEC-ARENA uses third party software libraries to implement various features. |
| CSUP-2 | Does the device contain an Operating System? If yes, complete 2.1-2.4. | No | |
| CSUP-2.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates? | n/a | |
| CSUP-2.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | n/a | |
| CSUP-2.3 | Does the device have the capability to receive remote installation of patches or software updates? | n/a | |
| 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. | No | |
| CSUP-3.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates? | n/a | |
| CSUP-3.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | n/a | |
| CSUP-3.3 | Does the device have the capability to receive remote installation of patches or software updates? | n/a | |
| 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? | n/a | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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? | 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 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? | 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? | No | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| CSUP-9 | Does the manufacturer have an approved list of third-party software that can be installed on the device? | n/a | |
| 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? | n/a | |
| 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? | No | |

## 2.7 HEALTH DATA DE-IDENTIFICATION

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| DIDT-1 | Does the device provide an integral capability to de-identify personally identifiable information? | Yes | See User Manual document for information. |
| DIDT-1.1 | Does the device support de-identification profiles that comply with the DICOM standard for de-identification? | No | |

## 2.8 DATA BACKUP AND DISASTER RECOVERY

*The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| DTBK-1 | Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? | No | |
| 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 | |

## 2.9 EMERGENCY ACCESS

*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.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| EMRG-1 | Does the device incorporate an emergency access (i.e. "break-glass") feature? | No | |

## 2.10 HEALTH DATA INTEGRITY AND AUTHENTICITY

*How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| IGAU-1 | Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? | No | |
| IGAU-2 | Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? | No | |

## 2.11 MALWARE DETECTION/PROTECTION

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| MLDP-1 | Is the device capable of hosting executable software? | No | |
| MLDP-2 | Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes. | Yes | See Technical Specification document for information. |
| 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? | Yes | See Technical Specification document for information. |
| MLDP-2.4 | Can the device owner/operator independently (re-) configure anti-malware settings? | Yes | |
| MLDP-2.5 | Does notification of malware detection occur in the device user interface? | No | See documentation of the anti-malware software you are using. |
| MLDP-2.6 | Can only manufacturer-authorized persons repair systems when malware has been detected? | No | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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)? | No | |
| 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? | n/a | |
| 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? | No | |
| 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 | |

## 2.12 NODE AUTHENTICATION

*The ability of the device to authenticate communication partners/nodes.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | See Administration Guide document for information. |
| NAUT-2 | Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)? | No | |
| NAUT-2.1 | Is the firewall ruleset documented and available for review? | n/a | |
| NAUT-3 | Does the device use certificate-based network connection authentication? | No | |

## 2.13 CONNECTIVITY CAPABILITIES

*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.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| CONN-1 | Does the device have hardware connectivity capabilities? | No | |
| CONN-1.1 | Does the device support wireless connections? | n/a | |
| CONN-1.1.1 | Does the device support Wi-Fi? | n/a | |
| CONN-1.1.2 | Does the device support Bluetooth? | n/a | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| CONN-1.1.3 | Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? | n/a | |
| CONN-1.1.4 | Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? | n/a | |
| CONN-1.2 | Does the device support physical connections? | n/a | |
| CONN-1.2.1 | Does the device have available RJ45 Ethernet ports? | n/a | |
| CONN-1.2.2 | Does the device have available USB ports? | n/a | |
| CONN-1.2.3 | Does the device require, use, or support removable memory devices? | n/a | |
| CONN-1.2.4 | Does the device support other physical connectivity? | n/a | |
| CONN-2 | Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? | Yes | See Administration Guide and Technical Specification documents for information. |
| CONN-3 | Can the device communicate with other systems within the customer environment? | Yes | See Administration Guide and Technical Specification documents for information. |
| 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 | See Administration Guide document for information. |
| CONN-7.1 | Is TLS configurable? | Yes | |
| CONN-8 | Does the device provide operator control functionality from a separate device (e.g., telemedicine)? | No | |

## 2.14 PERSON AUTHENTICATION

*The ability to configure the device to authenticate users.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| PAUT-1 | Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? | Yes | |
| PAUT-1.1 | Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? | Yes | |
| PAUT-2 | Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? | No | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| PAUT-3 | Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? | No | |
| 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? | No | |
| PAUT-7 | Does the device support account passwords that expire periodically? | No | |
| PAUT-8 | Does the device support multi-factor authentication? | No | |
| PAUT-9 | Does the device support single sign-on (SSO)? | No | |
| PAUT-10 | Can user accounts be disabled/locked on the device? | Yes | |
| PAUT-11 | Does the device support biometric controls? | 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? | Yes | |
| PAUT-14.1 | Are credentials stored using a secure method? | Yes | |

## 2.15 PHYSICAL LOCKS

*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*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| PLOK-1 | Is the device software only? If yes, answer "N/A" to remaining questions in this section. | Yes | |
| 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 | |

## 2.16 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE

*Manufacturer's plans for security support of third-party components within the device's life cycle.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| RDMP-1 | Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development? | Yes | IEC 62304 |
| 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 | |

## 2.17 SOFTWARE BILL OF MATERIALS

*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.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| SBOM-1 | Is the SBoM for this product available? | Yes | All third-party software components are documented internally in the Design History File. A license file containing information about all third-party software components is available to customers. |
| 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? | No | |
| 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 | |

## 2.18 SYSTEM AND APPLICATION HARDENING

*The device's inherent resistance to cyberattacks and malware*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| SAHD-1 | Is the device hardened in accordance with any industry standards? | No | |
| SAHD-2 | Has the device received any cybersecurity certifications? | No | |
| 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 | MD5 checksums are published to verify the integrity of installer packages. |
| 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 | MD5 checksums are published to verify the integrity of update packages. |
| 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? | n/a | |
| SAHD-6 | Are any system or user accounts restricted or disabled by the manufacturer at system delivery? | No | |
| 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? | n/a | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| SAHD-11 | Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? | n/a | |
| SAHD-12 | Can unauthorized software or hardware be installed on the device without the use of physical tools? | n/a | |
| 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? | n/a | |
| SAHD-14.1 | Are instructions available from vendor for increased hardening? | n/a | |
| SAHD-15 | Can the system prevent access to BIOS or other bootloaders during boot? | n/a | |
| SAHD-16 | Have additional hardening methods not included in 2.3.19 been used to harden the device? | n/a | |

## 2.19 SECURITY GUIDANCE

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| SGUD-1 | Does the device include security documentation for the owner/operator? | Yes | See Technical Specification document for information. |
| SGUD-2 | Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? | Yes | See User Manual and Technical Specification documents for information. |
| SGUD-3 | Are all access accounts documented? | Yes | |
| SGUD-3.1 | Can the owner/operator manage password control for all accounts? | Yes | See Administration Guide document for information. |
| SGUD-4 | Does the product include documentation on recommended compensating controls for the device? | No | |

## 2.20 DATA STORAGE CONFIDENTIALITY

*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.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| STCF-1 | Can the device encrypt data at rest? | No | BitLocker/OS level encryption can be used to encrypt data at rest. |
| STCF-1.1 | Is all data encrypted or otherwise protected? | n/a | |
| STCF-1.2 | Is the data encryption capability configured by default? | n/a | |

| Question ID | Question | Answer | Note |
|---|---|---|---|
| STCF-1.3 | Are instructions available to the customer to configure encryption? | n/a | |
| STCF-2 | Can the encryption keys be changed or configured? | No | |
| STCF-3 | Is the data stored in a database located on the device? | No | TOMTEC-ARENA does not incorporate a database of its own. However a database is required on the customers system to store data. |
| STCF-4 | Is the data stored in a database external to the device? | Yes | TOMTEC-ARENA uses MSSQL database that is provided and maintained by the customer. |

## 2.21 TRANSMISSION CONFIDENTIALITY

*The ability of the device to ensure the confidentiality of transmitted personally identifiable information.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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 | see CONN-7 |
| TXCF-2.1 | If data is not encrypted by default, can the customer configure encryption options? | Yes | See Administration Guide and Technical Specification documents for information. |
| TXCF-3 | Is personally identifiable information transmission restricted to a fixed list of network destinations? | No | |
| TXCF-4 | Are connections limited to authenticated systems? | No | |
| TXCF-5 | Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? | Yes | see CONN-7 |

## 2.22 TRANSMISSION INTEGRITY

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

| Question ID | Question | Answer | Note |
|---|---|---|---|
| TXIG-1 | Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? | No | |
| TXIG-2 | Does the device include multiple sub-components connected by external cables? | No | |

## 2.23 REMOTE SERVICE

*Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.*

| Question ID | Question | Answer | Note |
|---|---|---|---|
| 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? | n/a | |
| 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 | |
| RMOT-3 | Does the device have any other remotely accessible functionality (e.g. software updates, remote training)? | No | |