

MEDICAL DEVICE
DISCLOSURE STATEMENT
FOR MEDICAL DEVICE
SECURITY
Aixplorer MACH30 and
MACH20 SW V3.X

Titre / Title* Manufacturer Disclosure Statement for Medical Device Security

Rev.B* Page 2 / 2 03/06/2021

Document #*: RD.REC.071



DOCUMENT CONFIDENTIEL
CONFIDENTIAL DOCUMENT

| | | Manufacturer Disclosu | re Statement for Medical | Device Sec | urity – MC | OS ² |
|--------------------------------------|--|--|--------------------------------------|---------------|---------------------------------|---|
| | | | DEVICE DESCRIPTION | | | |
| Device Cate | gory | Manufacturer | Document ID | Document Rel | ease Date | |
| Ultrasound i | maging modality | SuperSonic Imagine | RD.DD.533 | 20201109 | | |
| Device Mode | | Software Revision | | Software Rele | ase Date | |
| Aixplorer M Aixplorer M | | V3.X | | 20201115 | | |
| • | SuperSonic Im | agine | Manufacturer Contact Information | on . | | |
| Manufacture Representati | r or ve | | | | | |
| Contact Info | mation Representative | Name/Position | | | | |
| The device i - a PACS ii - a Worklis | s an ultrasound scanne n order to archive the in t server in order to rece | connected environment: r. It is intended to be connected to mages acquired by the device; ar eive patient and exam informaton evice to query exam an retrieve in | nd | DATA | | |
| | | IVIAIN | AGEWENT OF PRIVATE | DATA | | |
| Refer | to Section 2.3.2 of this | standard for the proper interpreta | tion of information requested in th | nis form. | Yes, No, N/A, or See Note | Note # |
| | | nsmit, or maintain private data (in | cluding electronic Protected He | alth | | |
| | mation [ePHI])? | ents that can be maintained by the | · device: | | Yes | If a hacker gains access to the patient's database hosted by the Medical Equipment, there is typically no Social Security numbers, addresses, credit cards or other potentially lucrative personal information stored in it. A more likely scenario would be that Medical Equipment could be used to provide a "backdoor" into the PACS, or hospital information system to shut that down and use it as a potential ransomware threat. Ultrasound devices are less likely to be targeted as they are not 100% up and running. This Medical Equipment has no remote port opened except the DICOM one which do not provide remote access on the Ultrasound device. Thanks to design decision, an attack on this port would only limit the capability to receive image and not affect the capability to produce and exchange images with the PACS. |
| | • | • | | | V | |
| B.1 B.2 | Medical record (e.g., | name, address, location, unique id medical record #, account #, test | | ication | Yes Yes | _ |
| B.3 | | ic (e.g., photo/radiograph, test res | sults, or physiologic data with iden | ntifying | Yes | _ |
| D 4 | characteristics)? | out ontared by device year/eners | stor? | | | - |
| B.4 | Open, unstructured to | ext entered by device user/opera | itor ? | | Yes | Operator can save text in annotation displayed on images |
| B.5 | Biometric data? | armatian? | | | No | _ |
| B.6 C Maint | Personal financial inf taining private data - C | | | | No | _ |
| C.1 | | a temporarily in volatile memory (i | .e., until cleared by power-off or r | reset)? | Yes | _ |
| C.2 | Store private data p | ersistently on local media? | | | Yes | _ |
| C.3 | Import/export private | e data with other systems? | | | Yes | Export Exam to PACS, and removable media |
| C.4 D Mech | | a during power service interruption insmitting, importing/exporting of page 1 | | | Yes | _ |

| D.1 | Display private data (e.g., video display, etc.)? | Yes | |
|-----|--|-----|-----------------|
| D.2 | Generate hardcopy reports or images containing private data? | Yes | |
| D.3 | Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)? | Yes | |
| D.4 | Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)? | Yes | _ |
| D.5 | Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)? | Yes | _ |
| D.6 | Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)? | Yes | _ |
| D.7 | Import private data via scanning? | Yes | Barcode scanner |
| D.8 | Other? | No | _ |

| 9- | | | | | | |
|----------------|--------------------------------------|--|-------------------------------------|------------------------------|---------------------------------|--|
| | Category ound imaging modality | Manufacturer SuperSonic Imagine | Document ID RD.DD.533 | Document Re 20201109 | elease Date | |
| | Model | Software Revision | 10.00.333 | Software Rele | naco Dato | |
| | orer Mach30 | V3.X | | 20201115 | case Date | |
| | orer Mach20 | | | | | |
| | | <u>:</u> | SECURITY CAPAB | ILITIES | | |
| | Refer to Section 2.3.2 of this | s standard for the proper interp | pretation of information reques | sted in this form. | Yes, No, N/A, or See Note | Note # |
| 1 | AUTOMATIC LOGOFF (AI | LOF) | | | | |
| | The device 's ability to prev | ent access and misuse by una | uthorized users if device is le | eft idle for a period of tir | ne. | |
| 1-1 | • | red to force reauthorization of I session lock, password protec | | etermined length of | Yes | _ |
| | | tivity time before auto-logoff/so for configurable range] in note | | or configurable? | | |
| | ` - | | , | | Yes | Configurable to the following values 10 |
| | | | | | | Configurable to the following values 10 min (default), 20 min, 30min or never |
| | 1-1.2 Can auto-logoff/scretthe user? | een lock be manually invoked (| e.g., via a shortcut key or pro | ximity sensor, etc.) by | Yes | _ |
| ALOF notes: | | | | | | |
| 2 | AUDIT CONTROLS (AUD | T) | | | | |
| | The ability to reliably audit a | activity on the device . | | | | |
| 2-1 | Can the medical device cr | reate an audit trail ? | | | Yes | The audit logs are stored on the device. Their are not exported to an audit repository |
| 2-2 | Indicate which of the followi | ing events are recorded in the | audit log: | | | repository |
| | 2-2.1 Login/logout | | · · | | Yes | |
| | 2-2.2 Display/presentation | n of data | | | Yes | |
| | 2-2.3 Creation/modification | on/deletion of data | | | Yes | _ |
| | 2-2.4 Import/export of dat | ta from removable media | | | Yes | <u> </u> |
| | 2-2.5 Receipt/transmission | on of data from/to external (e.g | ., network) connection | | Yes | <u></u> |
| | 2-2.5.1 Remote serv | ice activity | | | No | <u></u> |
| | 2-2.6 Other events? (desi | cribe in the notes section) | | | Yes | The following event are logged: - Instance deleted (when exam are deleted from device) - Study used (when an exam is reviewed) - Security alert (when setup are changed) -Actor start/stop -Audit Log used |
| 2-3 | Indicate what information is | used to identify individual eve | nts recorded in the audit log: | | | |
| | 2-3.1 User ID | • | • | | Yes | |
| | 2-3.2 Date/time | | | | Yes | |
| | | | | | | |
| AUDT notes: | | | | | | |
| 3 | AUTHORIZATION (AUTH) | | ueare | | | |
| 3,1 | - | determine the authorization of | | or other mechanism? | | |
| 3-1 | Can the device prevent acc | cess to unauthorized users the | ough user login requirements | or other mechanism? | | |
| | | | | | Yes | |
| | | | | | | |

| 3-2 | Can users be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular users , power users , administrators, etc.)? Can the device owner/ operator obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)? | Yes | 3 roles are defined: Emergency access can only acquire images, Sonographer create, review, delete, export exams and admin can configure the device in addition to what a sonographer can do. User interface does not allow user to interact with operating system. There is no access for a user to the underlying OS |
|----------------|--|-----|--|
| AUTH notes: | | | |

| | | | | | | raye i |
|----------------|-----------------------------------|---|---|----------------------------|---------------------------------|--|
| | Category ound imaging modality | Manufacturer SuperSonic Imagine | Document ID RD.DD.533 | Document F 20201109 | Release Date | |
| | Model | Software Revision | נני.עע.עז | | elease Date | |
| | rer Mach30 | V3.X | | 20201115 | | |
| | Refer to Section 2.3.2 of the | nis standard for the proper inter | pretation of information request | ed in this form. | Yes, No, N/A, or See Note | Note # |
| 4 | CONFIGURATION OF SE | ECURITY FEATURES (CNFS) | | | | |
| | | | abilities to meet users' needs. | | | |
| 4-1 CNFS | Can the device owner/ope | erator reconfigure product secu | irity capabilities? | | Yes | Only admin users can change securit features |
| notes: | | | | | | |
| 5 | | DUCT UPGRADES (CSUP) ce staff, remote service staff, o | r authorized customer staff to ir | stall/upgrade devic | e 's security pa | tches. |
| 5-1 | Can relevant OS and dev i | ice security patches be applied | to the device as they become | available? | Yes | Quick installe: Security patch are applyied by SSI's Field service engineers. |
| | 5-1.1 Can security patch | nes or other software be installe | d remotely? | | Yes | For Online service contact SSI |
| CSUP notes: | | | | | | |
| 6 | HEALTH DATA DE-IDEN | , , | at allows identification of a pers | | | |
| 6-1 | Does the device provide a | an integral capability to de-ideni | ify private data? | | Yes | For Logs: Clear logs in system config For non DICOM export on USB/CD/DVD: -Jpeg export of US images are anonymised (as soon as operator does not entre PHI in annotation) - screenshot of patient folder are not anonymised (patient name, DoB, Patient ID, accession# may be visible) - report are not anonymised (patient name, DoB, Patient ID, accession# may be visible) For printed images: no anonymisation (patient name, DoB, Patient ID, accession# are visible) For DICOM: |
| DIDT | | | | | | Basic Profile, for US images being exported on DICOM Store and DICO Media no anonymisation for - DICOM Print (patient name, DoB, Patient ID, accession# will be visible) - screenshot of patient folder are not anonymised (patient name, DoB, Patient ID, accession# may be visible) - report are not anonymised (patient name, DoB, Patient ID, accession# may be visible) be visible) |
| notes: | | | | | | |
| 7 | | SASTER RECOVERY (DTBK) I damage or destruction of devi | i ce data, hardware, or software | | | |
| 7-1 | - | integral data backup capability | (i.e., backup to remote storage | | Yes | Export to DICOM Backup Restore |
| DTBK notes: | | | | | | |

| 8 | EMERGENCY ACCESS (EMRG) | | |
|----------------|--|--------------|---------------------------------------|
| | The ability of device users to access private data in case of an emergency situation that requires immediate acc | ess to store | ed private data. |
| 8-1 | Does the device incorporate an emergency access ("break-glass") feature? | Yes | |
| EMRG | | | |
| notes: | | | |
| 9 | HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) | | |
| | How the device ensures that data processed by the device has not been altered or destroyed in an unauthorized | manner and | d is from the originator. |
| 9-1 | Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology? | Yes | The mechanisms are provided by the OS |
| IGAU notes: | | | |

| Device | e Category | Manufacturer | Document ID | Document Re | elease Date | |
|----------------|---|--------------------------------------|--|------------------------|---------------------------------|---|
| | ound imaging modality | SuperSonic Imagine | RD.DD.533 | 20201109 | Sicaso Dato | |
| | | | KD.DD.333 | | | |
| | e Model | Software Revision | | Software Rel | ease Date | |
| Aixplo | orer Mach30 | V3.X | | 20201115 | | |
| | Refer to Section 2.3.2 of this | standard for the proper inte | rpretation of information requested | d in this form. | Yes, No, N/A, or See Note | Note # |
| 10 | MALWARE DETECTION/P | ROTECTION (MLDP) | | | | |
| | The ability of the device to e | effectively prevent, detect ar | d remove malicious software (ma | ilware). | | |
| 10-1 | Does the device support the | e use of anti-malware softw | are (or other anti-malware mech | anism)? | | |
| | | | | | Yes | Malicious code protection mechanisms by: - Use of secure Open-source operating system - Pervasive configuration management and comprehensive software integrity controls are used to prevent execution of unauthorized code - secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended |
| | 10-1.1 Can the user indepe | ndently re-configure anti-ma | alware settings? | | No | _ |
| | 10-1.2 Does notification of r | | - | | No | <u> </u> |
| | | | r systems when malware has bee | en detected? | | |
| | , | | • | | Yes | |
| 10-2 | Can the device owner install | or update anti-virus softw | are? | | No | |
| | | • | pdate virus definitions on manufa | cturer-installed anti- | | |
| | virus software? | , ,, ,, | | | No | <u></u> |
| MLDP notes: | | | | | | |
| 11 | NODE AUTHENTICATION | ` ' | | | | |
| 11-1 | The ability of the device to a Does the device provide/su | | partners/nodes. thentication that assures both the | sender and the | | |
| | recipient of data are known | to each other and are author | ized to receive transferred inform | ation? | No | _ |
| NAUT notes: | | | | | | |
| 12 | Ability of the device to author | | | | | |
| 12-1 | Does the device support us | er/operator-specific userna | me(s) and password(s) for at least | st one user? | Yes | _ |
| | 12-1.1 Does the device sup | port unique user/operator- | specific IDs and passwords for mu | ultiple users? | No | 4 accounts exists: emergency access, sonographer, admin and service |
| 12-2 | Can the device be configure Active Directory, NDS, LDA | | ough an external authentication se | rvice (e.g., MS | No | _ |
| 12-3 | Can the device be configure | ed to lock out a user after a | certain number of unsuccessful lo | gon attempts? | No | _ |
| 12-4 | Can default passwords be c | hanged at/prior to installatio | n? | | Yes | _ |
| 12-5 | Are any shared user IDs us | ed in this system? | | | Yes | _ |
| 12-6 | • | ed to enforce creation of use | er account passwords that meet e | stablished | No | |
| | complexity rules? | | | | 140 | |
| 12-7 | Can the device be configure | ed so that account password | s expire periodically? | | No | _ |
| PAUT notes: | | | | | | |
| 13 | PHYSICAL LOCKS (PLOK Physical locks can prevent u device or on removable me | unauthorized users with phy | sical access to the device from co | ompromising the inte | grity and con | fidentiality of private data stored on the |
| 13-1 | Are all device components cannot remove without tools | | her than removable media) phys | ically secure (i.e., | Yes | _ |

| PLOK | | |
|--------|--|--|
| notes: | | |
| | | |

| Device | Category | Manufacturer | Document ID | Document R | elease Date | |
|----------------|--|---|----------------------------------|------------------------|---------------------------------|--|
| | ound imaging modality | SuperSonic Imagine | RD.DD.533 | 20201109 | cicase Date | |
| | Model | Software Revision | | Software Rel | ease Date | |
| Aixplo | orer Mach30 | V3.X | | 20201115 | | |
| | Refer to Section 2.3.2 of th | is standard for the proper inter | pretation of information reques | ted in this form. | Yes, No, N/A, or See Note | Note # |
| 14 | | PARTY COMPONENTS IN DE | , , | | | |
| | | ecurity support of 3rd party cor | | | | |
| 14-1 | - including version number | e provided or required (separa (s). | ely purchased and/or delivered | d) operating system(s) | Yes | <u></u> |
| 14-2 | Is a list of other third party | applications provided by the m | anufacturer available? | | Yes | Fusion (purcheasble option) Debian GNU/Linux |
| RDMP notes: | | | | | | |
| 15 | | FION HARDENING (SAHD) o cyber attacks and malware. | | | | |
| 15-1 | | any hardening measures? Plea | se indicate in the notes the lev | el of conformance to | | The following compensation are |
| 45.2 | any industry-recognized ha | | | . An Alexandra de | Yes | implemented to harden system - Single-function system: US - Address space layout randomization (ASLR) - Protected database link (only local access enabled, password protection)Unused services disabled - Remote loging service disabled - Use of Mandatory Access Control (MAC) mecanism - Least privilege principle - Least functionality principle |
| 15-2 | | any mechanism (e.g., release-s s the manufacturer-authorized | | etc.) to ensure the | Yes | All the software included in the medical device are provided by a trusted source provider (GNU/Linux Debian). The Debian packages that are included on the medical devices are digitally signed by SuperSonic Imagine. Debian package is a tamper-evident packaging format. |
| 15-3 | Does the device have ext | ernal communication capability | (e.g., network, modem, etc.)? | | | External communication capability: |
| | | | | | Yes | Network: used for DICOM communication |
| 15-4 | Does the file system allow (NTFS) for MS Windows p | the implementation of file-leve | access controls (e.g., New Te | echnology File System | Yes | ReiserFS |
| 15-5 | ` ' | not required for the intended | use of the device disabled or | deleted, for both | Yes | ACIONI D |
| 15-6 | • | e.g., file shares) which are not | required for the intended use | of the device , | Yes | The system does not used any shared resources. |
| 15-7 | Are all communication por | ts which are not required for th | e intended use of the device | closed/disabled? | Yes | The DICOM port is the only port opened. Its use is documented in the DICOM Conformance Statement |
| 15-8 | | et, file transfer protocol [FTP], i use of the device deleted/disa | | , etc.), which are not | Yes | Those services are not installed on the Medical Devices |
| 15-9 | • • • • • • | S applications as well as OS-inc the intended use of the devic | | ternet Explorer, etc.) | Yes | Only essentials packages are installed on the medical device. No web browse are installed. |
| 15-10 | Can the device boot from memory component)? | uncontrolled or removable me | dia (i.e., a source other than a | n internal drive or | No | Booting from external device is not authorized |
| 15-11 | Can software or hardware use of tools? | not authorized by the device n | nanufacturer be installed on the | e device without the | No | _ |

| 16 | SECURITY GUIDANCE (SGUD) | | |
|------|--|---------|--|
| | The availability of security guidance for operator and administrator of the system and manufacturer sales and so | ervice. | |
| 16-1 | Are security-related features documented for the device user ? | Yes | Security information are included in th User Guide |
| 16-2 | Are instructions available for device /media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)? | No | Permanent deletion of data require storage device destruction. |

HN 1-2013 Page 22

| Device | Category | Manufacturer | Document ID | Document Re | elease Date | |
|----------------|---|---|--------------------------------------|--------------------------|---------------------------------|--|
| | ound imaging modality | SuperSonic Imagine | RD.DD.533 | 20201109 | | |
| | e Model | | | Software Rel | oooo Doto | |
| | orer Mach30 | Software Revision V3.X | | 20201115 | ease Date | |
| Aixpic | orei Maciiso | V 3.A | | 20201113 | | |
| | Refer to Section 2.3.2 of this | s standard for the proper inter | pretation of information reques | sted in this form. | Yes, No, N/A, or See Note | Note # |
| 17 | | ensure unauthorized access of | | rity and confidentiality | of private data | a stored on device or removable media. |
| 17.1 | O th- decise | 440 | | | | |
| STCF notes: | Can the device encrypt dat | a at rest? | | | Yes | e-PHI contained in database, DICOM objects, native archives and logs are stored on an encrypted partition using TPM1.2 |
| <u> </u> | TRANSMISSION CONFID | ENITIAL ITY (TYCE) | | | | |
| 18 | TRANSMISSION CONFIDI | ` ' | | | | |
| ١ | • | ensure the confidentiality of tr | • | | | |
| | • | nitted only via a point-to-point | | | No | |
| 18-2 | Is private data encrypted p notes which encryption star | | vork or removable media ? (If | yes, indicate in the | No | |
| 18-3 | • | n restricted to a fixed list of ne | etwork destinations? | | Yes | _ _ |
| TXCF notes: | | | | | | |
| 19 | TRANSMISSION INTEGRI | TY (TXIG) | | | | |
| | The ability of the device to | ensure the integrity of transm | itted private data. | | | |
| 19-1 | | ny mechanism intended to ensection how this is achieved.) | sure data is not modified durin | g transmission? (If | Yes | DICOM TLS |
| TXIG notes: | | | | | | |
| 20 | OTHER SECURITY CONS | IDERATIONS (OTHR) | | | | |
| | Additional security conside | rations/notes regarding medi- | cal device security. | | | |
| 20-1 | Can the device be serviced | d remotely? | | | Yes | |
| 20-2 | Can the device restrict rem IP addresses)? | note access to/from specified | devices or users or network le | ocations (e.g., specific | Yes | _ |
| | , | configured to require the local | user to accept or initiate rem | ote access? | Yes | Local user acceptance is mandatory to initiate a remote access |
| OTHR notes: | | | | | | |

Manufacturer Disclosure Statement for Medical Device Security - MDS²

| | Aixplorer MACH30 V3.X | | |
|--------------------|-----------------------|-----------|-------------|
| superSonic imagine | Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 |

| Question ID | Question | | See note | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
|--|---|--|--|-----------------------|-----------------------|----------------------------------|
| DOC-1 | Manufacturer Name | SuperSonic imagine | _ | | | .55 27 552.2525 |
| DOC-2 | Device Description | Ultrasound imaging modality | _ | | | |
| | | Aixplorer MACH30 V3.X | _ | | | |
| DOC-3 | Device Model | Aixplorer MACH20 V3.X | _ | | | |
| DOC-4 | Document ID | RD.DD.533 | _ | | | |
| DOC-5 | Manufacturer Contact Information | Cybersecurity questions shall be asked to cybersecurity@supersonicimagine.com For other inquiries please contact your local representative. The device is an ultrasound scanner. It is intended to be connected to: - a PACs in order to archive the images acquired by the device; and | _ | | | |
| DOC-6 DOC-7 | Intended use of device in network-connected environment: Document Release Date | a Worklist server in order to receive patient and exam information. A purchasable option also allow device to query exam an retrieve images archived on the PACS. | _ | | | |
| DOC-8 | Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device? | Yes | Vulnerabilities information available at: https://www.supersonicimagine.Com/security | | | |
| DOC-9 | ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization? | Yes | _ | | | |
| DOC-10 | Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources? | Yes | see Network and Data Flow Diagram | | | |
| 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? Does the SaMD rely on an owner/operator provided | N/A | _ | | | |
| DOC-11.2 | operating system? Is the SaMD hosted by the manufacturer? | N/A | _ | | | |
| DOC-11.3 DOC-11.4 | Is the SaMD hosted by the customer? | N/A N/A | _ | | | |
| | MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION | Yes, No, N/A, or See Note | Note # | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | | | | | | |
| | | | This device download, display, transmit and store the following PII: • Patient Name • Patient II | IEC IN 00001-2-2.2012 | NIST SP 800-33 Rev. 4 | 130 27002.2013 |
| MDU 1 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic | Vec | the following PII: Patient Name Patient ID Patient Age | IEC IN 60001-2-2.2012 | | |
| MPII-1 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable | Yes | the following PII: Patient Name Patient ID | iec in 60001-2-2.2012 | AR-2 | A.15.1.4 |
| MPII-1 MPII-2 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable information? Does the device maintain personally identifiable | Yes | the following PII: Patient Name Patient ID Patient Age | iec in 60001-2-2,2012 | | |
| | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health information (ePHI))? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? | Yes | the following PII: Patient Name Patient ID Patient Age | IEC IN 00001-2-2.2012 | AR-2 | A.15.1.4 |
| MPII-2 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information tomporarily in volatile memory (i.e., until | Yes | the following PII: Patient Name Patient ID Patient Age | IEC IN 00001-2-2.2012 | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| MPII-2 MPII-2.1 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI)? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? Does the device store personally identifiable | Yes Yes | the following PII: Patient Name Patient ID Patient Age | IEC IN 00001-2-2.2012 | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| MPII-2.1 MPII-2.2 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHII)? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? Does the device store personally identifiable information persistently on internal media? Is personally identifiable information preserved in the | Yes Yes | the following PII: Patient Name Patient ID Patient Age Date of birth | IEC IN 00001-2-2.2012 | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| MPII-2.1 MPII-2.2 MPII-2.3 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset!?) Does the device store personally identifiable information persistently on internal media? Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased? Does the device store personally identifiable | Yes Yes Yes | the following PII: Patient Name Patient ID Patient Age Date of birth By default, the exams must be manually deleted. However the device can be configured to delete: all the exams after a configurable period of time all the archived exams after a configurable period of time | EC IN 60001-2-2.2012 | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| MPII-2.1 MPII-2.2 MPII-2.3 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? Does the device store personally identifiable information persistently on internal media? Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased? Does the device store personally identifiable information in a database? Does the device allow configuration to automatically delete local personally identifiable information after i is stored to a long term solution? Does the device import/export personally identifiable information after i is stored to a long term solution? | Yes Yes Yes Yes Yes | the following PII: Patient Name Patient ID Patient Age Date of birth By default, the exams must be manually deleted. However the device can be configured to delete: all the exams after a configurable period of time all the archived exams after a configurable period of time all the exams archived and committed after a configurable period of time the oldest exams when disk is full after a configurable period of time | EC IN 00001-2-2.2012 | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| MPII-2.1 MPII-2.2 MPII-2.3 MPII-2.4 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHII)? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? Does the device store personally identifiable information persistently on internal media? Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased? Does the device store personally identifiable information in a database? Does the device store personally identifiable information after it is stored to a long term solution? 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!? Does the device maintain personally identifiable information to a server!? | Yes Yes Yes Yes Yes | the following PII: Patient Name Patient ID Patient Age Date of birth By default, the exams must be manually deleted. However the device can be configured to delete: all the exams after a configurable period of time all the archived exams after a configurable period of time all the exams arker a configurable period of time the didset sexams when disk is full after a | IEC IN 00001-2-2.2012 | AR-2 AR-2 AR-2 | A.15.1.4 A.15.1.4 A.15.1.4 |
| MPII-2.1 MPII-2.2 MPII-2.3 MPII-2.4 | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? Does the device maintain personally identifiable information? Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)? Does the device store personally identifiable information persistently on internal media? Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased? Does the device store personally identifiable information in a database? Does the device allow configuration to automatically delete local personally identifiable information after i is stored to a long term solution? 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 Yes Yes Yes Yes | the following PII: Patient Name Patient ID Patient Age Date of birth By default, the exams must be manually deleted. However the device can be configured to delete: all the exams after a configurable period of time all the archived exams after a configurable period of time will be exams after a configurable period of time the device can be configurable period of time the device will query PII from the modality worklist server, and transmit PHI on PACS and on removable | IEC IN 00001-2-2.2012 | AR-2 AR-2 AR-2 | A.15.1.4 A.15.1.4 A.15.1.4 |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|--|--|---|---|--|--|---|
| | 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 | | The PHI are stored on a dedicated crypted partition | | | |
| MPII-2.9 | storage location)? Does the device have mechanisms used for the | Yes | separated from the device's Operating System. e-PHI can be transmitted over DICOM Storage | | AR-2 | A.15.1.4 |
| | transmitting, importing/exporting of personally | | service, exportation on removable device and | | | |
| MPII-3 | identifiable information? Does the device display personally identifiable | Yes | backup restore | | AR-2 | A.15.1.4 |
| MPII-3.1 | information (e.g., video display, etc.)? | Yes | e-PHI are displayed on main screen | | AR-2 | A.15.1.4 |
| | Does the device generate hardcopy reports or images | | | | | |
| MPII-3.2 | containing personally identifiable information? Does the device retrieve personally identifiable | Yes | The device can record PII to USB removable HDD, | | AR-2 | A.15.1.4 |
| | information from or record personally identifiable information to removable media (e.g., removable- | | USB Memory, DVD-R/RW, CD-R/RW. The device can also import and display PHI from the | | | |
| | HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD | | above-mentioned device (but it is a purchasable | | | |
| MPII-3.3 | Does the device transmit/receive or import/export | Yes | option) | | AR-2 | A.15.1.4 |
| | personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, | | | | | |
| MPII-3.4 | etc.)? | No | _ | | AR-2 | A.15.1.4 |
| | Does the device transmit/receive personally identifiable information via a wired network | | | | | |
| MPII-3.5 | connection (e.g., RJ45, fiber optic, etc.)? Does the device transmit/receive personally | Yes | The device can connect to Ethernet networks | | AR-2 | A.15.1.4 |
| | identifiable information via a wireless network | | The device can connect to Wi-Fi (this is a | | | |
| MPII-3.6 | connection (e.g., Wi-Fi, Bluetooth, NFC, infrared, cellular, etc.)? | Yes | purchasable option) | | AR-2 | A.15.1.4 |
| | Does the device transmit/receive personally identifiable information over an external network | | The device can be remote-serviced (this is a purchasable option). During such connection an | | | |
| MPII-3.7 | (e.g., Internet)? | Yes | operator may access to PII. | | AR-2 | A.15.1.4 |
| 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 | | | | |
| | Does the device use any other mechanism to transmit, | | Device's information (that may or may not include PII) can be backed up and restored. Both actions | | | |
| | | | | | | |
| MPII-3.10 | import or export personally identifiable information? | Yes | require USB access and admin role. | | AR-2 | A.15.1.4 |
| MPII-3.10 Management of Priva | | Yes | require USB access and admin role. | | AR-2 AR-2 | A.15.1.4 A.15.1.4 |
| | te Data notes: | Yes | require USB access and admin role. | IFC TR 80001-2-2:2012 | AR-2 | A.15.1.4 |
| | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent access and misuse by | Yes | require USB access and admin role. | IEC TR 80001-2-2:2012 | | |
| | te Data notes: AUTOMATIC LOGOFF (ALOF) | Yes | require USB access and admin role. | IEC TR 80001-2-2:2012 | AR-2 | A.15.1.4 |
| | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. | Yes | | IEC TR 80001-2-2:2012 | AR-2 | A.15.1.4 |
| | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of | Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked | IEC TR 80001-2-2:2012 | AR-2 | A.15.1.4 |
| | te 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. Can the device be configured to force reauthorization | Yes | upon a configurable period of time, a screen saver | IEC TR 80001-2-2:2012 Section 5.1, ALOF | AR-2 | A.15.1.4 |
| Management of Priva | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent occess and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password | | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another | | AR-2 NIST SP 800-53 Rev. 4 | A.15.1.4 |
| Management of Priva | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? | Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. | | AR-2 NIST SP 800-53 Rev. 4 | A.15.1.4 |
| Management of Priva | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent access and misuse by unauthorized users if device is left lalle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? | Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min | Section 5.1, ALOF Section 5.1, ALOF | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 | A.15.1.4 ISO 27002:2013 None A.11.2.8, A.11.2.9 |
| Management of Priva | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent access and misuse by unauthorized users if device is left lalle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto- | Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min | Section 5.1, ALOF | AR-2 NIST SP 800-53 Rev. 4 AC-12 | A.15.1.4 ISO 27002:2013 None |
| Management of Priva ALOF-1 ALOF-2 | te 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. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or | Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 | AC-12 AC-11 NIST SP 800-53 Rev. 4 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, |
| Management of Priva | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent occess and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? | Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never | Section 5.1, ALOF Section 5.1, ALOF | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 | A.15.1.4 ISO 27002:2013 None A.11.2.8, A.11.2.9 ISO 27002:2013 |
| Management of Priva ALOF-1 ALOF-2 | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? | Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 | AC-12 AC-11 NIST SP 800-53 Rev. 4 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 | te 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. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? | Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never — Audit logs are compliant to DICOM Specific Audit Messages Actor-start-stop, Begin-storing-instances, Instances- | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 AUDT-1.2 | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitty to prevent occess and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably oudit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit trail? Does other personally identifiable information exist in the audit trail? | Yes Yes Yes No | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 | A.15.1.4 ISO 27002:2013 None A.11.2.8, A.11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? Are events recorded in an audit log? If yes, indicate | Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.2 AUDT-2 AUDT-2.1 AUDT-2.1 AUDT-2.1 AUDT-2.2 | te 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. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log: Successful login/logout attempts? | Yes Yes Yes Yes Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 AU-2 AU-2 AU-2 AU-2 AU-2 AU-2 AU-2 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A12.1.1, A18.1.1, A.18.2.2 None None None None None |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 AUDT-1.2 AUDT-2 AUDT-2.1 | te 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. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit traig! Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit viag: | Yes Yes Yes Yes Yes Yes Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT Section 5.2, AUDT Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 AU-2 AU-2 AU-2 | A.15.1.4 ISO 27002:2013 None A.11.2.8, A.11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 None None |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 AUDT-1.2 AUDT-2.1 AUDT-2.2 AUDT-2.2 AUDT-2.3 | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's oblitly to prevent access and misuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log: Successful login/logout attempts? Unsuccessful login/logout attempts? Unsuccessful login/logout attempts? Unsuccessful or user privileges? | Yes Yes Yes Yes Yes Yes No Yes Yes Yes N/A N/A | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 None None None None None None |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 AUDT-1.2 AUDT-2 AUDT-2 AUDT-2 AUDT-2 AUDT-2.3 AUDT-2.4 | te 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. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log: Successful login/logout attempts? Modification of user privileges? Creation/modification/deletion of users? Presentation of clinical or PII data (e.g. display, print)? Creation/modification/deletion of data? | Yes Yes Yes Yes Yes Yes No Yes Yes Yes N/A N/A | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 AU-2 | A15.1.4 ISO 27002:2013 None A11.2.8, A11.2.9 ISO 27002:2013 A.5.1.1, A.51.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 None None |
| ALOF-1 ALOF-2 AUDT-1 AUDT-1.1 AUDT-1.2 AUDT-2.1 AUDT-2.2 AUDT-2.3 AUDT-2.4 AUDT-2.5 | te Data notes: AUTOMATIC LOGOFF (ALOF) The device's ability to prevent access and missuse by unauthorized users if device is left idle for a period of time. Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? AUDIT CONTROLS (AUDT) The ability to reliably audit activity on the device. Can the medical device create additional audit logs or reports beyond standard operating system logs? Does the audit log record a USER ID? Does other personally identifiable information exist in the audit trail? Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log: Successful login/logout attempts? Unsuccessful login/logout attempts? Unsuccessful login/logout attempts? Creation/modification/deletion of users? Presentation of clinical or PII data (e.g. display, print)? | Yes Yes Yes Yes Yes Yes Yes No No Yes Yes Yes Yes Yes Yes Yes N/A N/A N/A Yes | upon a configurable period of time, a screen saver will hide screen information and lock session. Locked sessions can be terminated to give access to another user. Configurable to the following values 10 min (default), 20 min, 30min or never —————————————————————————————————— | Section 5.1, ALOF Section 5.1, ALOF IEC TR 80001-2-2:2012 Section 5.2, AUDT Section 5.2, AUDT | AR-2 NIST SP 800-53 Rev. 4 AC-12 AC-11 NIST SP 800-53 Rev. 4 AU-1 AU-2 | A.15.1.4 ISO 27002:2013 None A.11.2.8, A.11.2.9 ISO 27002:2013 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 None |

| | Aixplorer MACH30 V3.X | | | | | |
|------------------------|---|-----------|--|--|-----------------------|----------------|
| SuperSonic imagine | Aixplorer MACH20 V3.X | RD.DD.533 | 15-No | v-2020 | | |
| | Receipt/transmission of data or commands over a | | | | | |
| AUDT-2.8 | network or point-to-point connection? Remote or on-site support? | Yes No | _ | Section 5.2, AUDT Section 5.2, AUDT | AU-2 AU-2 | None None |
| AUDT-2.8.1 | Application Programming Interface (API) and similar | NO | _ | Section 5.2, AUDI | AU-Z | None |
| AUDT-2.8.2 | activity? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.9 | Emergency access? | Yes | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.10 AUDT-2.11 | Other events (e.g., software updates)? Is the audit capability documented in more detail? | No No | _ | Section 5.2, AUDT Section 5.2, AUDT | AU-2 AU-2 | None None |
| A0D1-2.11 | Can the owner/operator define or select which events | | _ | Section 5.2, AOD1 | AU-2 | None |
| AUDT-3 | are recorded in the audit log? | No | | Section 5.2, AUDT | AU-2 | None |
| | Is a list of data attributes that are captured in the | | | | | |
| AUDT-4 AUDT-4.1 | audit log for an event available? Does the audit log record date/time? | No Yes | _ | Section 5.2, AUDT Section 5.2, AUDT | AU-2 AU-2 | None None |
| A0D1-4.1 | Can date and time be synchronized by Network Time | res | _ | Section 5.2, AODT | AU-2 | None |
| AUDT-4.1.1 | Protocol (NTP) or equivalent time source? | Yes | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-5 | Can audit log content be exported? | Yes | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-5.1 | Via physical media? Via IHE Audit Trail and Node Authentication (ATNA) | Yes | _ | | | |
| AUDT-5.2 | profile to SIEM? | No | | | | |
| | Via Other communications (e.g., external service | | _ | | | |
| AUDT-5.3 | device, mobile applications)? | No | _ | | | |
| AUDT-5.4 | Are audit logs encrypted in transit or on storage media? | No | | | | |
| 1001-3.4 | Can audit logs be monitored/reviewed by | | _ | | | |
| AUDT-6 | owner/operator? | No | _ | | | |
| AUDT-7 | Are audit logs protected from modification? | Yes | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-7.1 AUDT-8 | Are audit logs protected from access? Can audit logs be analyzed by the device? | Yes No | | Section 5.2, AUDT | AU-2 | None |
| AUDI-8 | can addit logs be analyzed by the device: | NO | _ | Section 5.2, AODT | A0-2 | None |
| | | | | | | |
| | AUTHORIZATION (AUTH) The ability of the device to determine the | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | authorization of users. | | | | | |
| | | | | | | |
| | Does the device prevent access to unauthorized users | | | | | |
| AUTH-1 | through user login requirements or other mechanism? Can the device be configured to use federated | ? Yes | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | credentials management of users for authorization | | | | | |
| AUTH-1.1 | (e.g., LDAP, OAuth)? | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | Can the customer push group policies to the device | | | 5 vi 50 turu | | |
| AUTH-1.2 | (e.g., Active Directory)? Are any special groups, organizational units, or group | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| AUTH-1.3 | policies required? | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | | | 3 roles are defined: Emergency access can only | | | |
| | Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, | | acquire images , Sonographer create, review, d export exams and admin can configure the dev | | | |
| AUTH-2 | etc.)? | Yes | addition to what a sonographer can do. | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| 7,01112 | Can the device owner/operator grant themselves | | addition to what a sonographer can do. | Section 5.5,710111 | 21.2 | 713.2.2 |
| | unrestricted administrative privileges (e.g., access | | | | | |
| AUTH-3 | operating system or application via local root or administrator account)? | No | | Costics F.2 AUTH | IA-2 | A.9.2.1 |
| AUTH-3 | Does the device authorize or control all API access | No | _ | Section 5.3, AUTH | IA-Z | A.9.2.1 |
| AUTH-4 | requests? | Yes | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | Does the device run in a restricted access mode, or | | The user has no access to the underlaying open | rating | | |
| AUTH-5 | 'kiosk mode', by default? | Yes | system | | | |
| | | | | | | |
| | | | | | | |
| | CYBER SECURITY PRODUCT UPGRADES (CSUP) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade | | | | | |
| | staff, or authorized customer staff to install/upgrade device's security patches. | | | | | |
| | Does the device contain any software or firmware | | | | | |
| | which may require security updates during its | | | | | |
| | operational life, either from the device manufacturer or from a third-party manufacturer of the | | | | | |
| | software/firmware? If no, answer "N/A" to questions | | | | | |
| CSUP-1 | in this section. | Yes | _ | | | |
| | Does the device contain an Operating System? If yes, | w. | | | | |
| CSUP-2 | complete 2.1-2.4. Does the device documentation provide instructions | Yes | - | | | |
| | for owner/operator installation of patches or software | e | | | | |
| CSUP-2.1 | updates? | Yes | Remote update is described in User Guide | | | |
| | | | | | | |
| CSUP-2.2 | Does the device require vendor or vendor-authorized service to install patches or software updates? | Yes | | | | |
| C3UF=2.2 | service to instail pateries of software updates? | rea | _ | | | |

Aixplorer MACH30 V3.X SuperSonic imagine Aixplorer MACH20 V3.X

RD.DD.533

15-Nov-2020

| South the models delayers assessment on the security of the se | | | | | | |
|--|-----------|--|------|--|--|--|
| Service of the service of service of the service of | | | | | | |
| South the models delayers assessment on the security of the se | | Does the device have the capability to receive remote | | | | |
| systems come you drop you whethere to be provided by the company of the company o | CSUP-2.3 | installation of patches or software updates? | Yes | Configurable option | | |
| systems come you drop you whethere to be provided by the company of the company o | | | | • | | |
| According to increased to increase of the control o | | | | | | |
| See 2.1 monitorizant monitoriza | | | | The Operating System is maintained by SuperSonic | | |
| Sour Process Control C | CSLIP=2 4 | | No. | | | |
| Sept. 1 Congress 3-3.4. Sept. 1 Congress 3-3.4. Sept. 1 Congress of the congre | C501 2.4 | | | magne | | |
| Occidence of process of commercial process of terrocordinary of the commercial process of the commercial process of terrocordinary of the commercial proce | CCLID 3 | | Vos | | | |
| to control/granted to the control/granted and column of processor and column o | C3UF=3 | | res | _ | | |
| March Marc | | | | Firm and delicer are least the delicer and | | |
| Description for factors are provided and section of the control of | 00110 0 4 | | | | | |
| Sign 1 2 service trained printing reverse representation of positions of proteins and proteins plant for people from the proteins and proteins protein and proteins and protei | CSUP-3.1 | updates? | NO | updates of software re-installation | | |
| Sign 1 2 service trained printing reverse representation of positions of proteins and proteins plant for people from the proteins and proteins protein and proteins and protei | | | | | | |
| Open the review for the control and produced interface or remote the review of the control and produced interface and the control and produced interface and the control and t | | | | | | |
| Supplies | CSUP-3.2 | service to install patches or software updates? | Yes | _ | | |
| Supplies | | | | | | |
| Desi the medical diverse manufacture of allow security significant and | | | | | | |
| Section of the control of the contro | CSUP-3.3 | | Yes | | | |
| Moreowith to be invited well-water approach in the control of the | | | | | | |
| Sign 1. See the device continue model methods are software for the process of the | | | | | | |
| Once the device control mote Manuer Software Followers Followe | | | | | | |
| Signed Section of the control of the | CSUP-3.4 | manufacturer? | No | _ | | |
| South the device deconnectation product intractification of patients or refined with the product of the product | | Does the device contain Anti-Malware Software? If | | | | |
| Some the device requires verder or repetite verder v | CSUP-4 | | No | _ | | |
| SUB-14 contained an intervent or reader without the reader of the device require verder or reader without the reader of the reader without the reader without the reader without the reader of the reader without the reader without the reader without the reader of the reader without the reader of the reader without the reader withou | | | | | | |
| SUB-14 contained an intervent or reader without the reader of the device require verder or reader without the reader of the reader without the reader without the reader without the reader of the reader without the reader without the reader without the reader of the reader without the reader of the reader without the reader withou | | for owner/operator installation of patches or software | | | | |
| Sign 4.2 across the device regular vendor or vendor authorized without approval from the commentation of particles or of three regular vendor or vendor authorized particles or of the commentation of particles o | CSUP-4.1 | | | _ | | |
| SUR-14 Service to local planether or enthrance application of profession | | | | | | |
| Does the device have the capability to receive remote installation of patches or software spoties or softw | | Does the device require vendor or vendor-authorized | | | | |
| Does the device have the capability to receive remote installation of patches or software spoties or softw | CSUP-4.2 | service to install patches or software updates? | N/A | | | |
| SUB-4.3 initialization of patches or software equipate? One site the medical evice manufacturer allow secondly with a medical evice manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates are specified evice manufacturer allows secondly updates are specified allows and the secondly updates are specified updates and manufacturer allows secondly updates are specified updates and manufa | | | | _ | | |
| SUB-4.3 initialization of patches or software equipate? One site the medical evice manufacturer allow secondly with a medical evice manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates from any third party manufacturer (e.g., with a manufacturer allows secondly updates are specified evice manufacturer allows secondly updates are specified allows and the secondly updates are specified updates and manufacturer allows secondly updates are specified updates and manufa | | Does the device have the capability to receive remote | | | | |
| Does the ended affecte manufacturer (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sproud from the Monzouth (e.g., Monzouth) to be installed without sprou | CSLIP-4 3 | | N/A | | | |
| updates from any hitele-party manufacturers (e.g., Macronoft) to be installed whou approved from the manufacturer (e.g., Macronoft) to be installed whou approved from the manufacturer (e.g., Macronoft) to be installed whou approved from the manufacturer (e.g., Macronoft) to be installed whose approved installation of patches or software updates? SUP-51 updates (e.g., soot manufacturer) Does the device documentation provide installation of patches or software updates? SUP-52 service to installation of patches or software updates? SUP-53 in containing a provide installation of patches or software updates? SUP-54 manufacturer (e.g., Macronoft) to be installed without appoint from the manufacturer and the software updates (e.g., Macronoft) to be installed without appoint from the manufacturer and the software updates (e.g., Soot manufacturer and updates) SUP-62 manufacturer (e.g., Soot manufacturer and updates) SUP-63 manufacturer (e.g., Soot manufacturer and updates) SUP-64 manufacturer (e.g., Soot manufacturer and updates) SUP-65 manufacturer (e.g., Soot manufacturer and updates) SUP-65 manufacturer (e.g., Soot manufacturer and updates) SUP-66 manufacturer (e.g., Soot manufacturer and updates) SUP-67 manufacturer (e.g., Soot manufacturer and updates) SUP-68 manufacturer (e.g., Soot manufacturer and updates) SUP-69 manufacturer (e.g., Soot manufacturer) SUP-69 manufacturer (e.g., Soot manufacturer) SUP-69 manufacturer (| | | ' | _ | | |
| Microsoft to be installed without approval from the manufacturer? Describe diver contain Non-Operating system common day of the white operating system common day of the white operation of partners or of the manufacturer of th | | | | | | |
| SUP-5.4 manufacture? Does the device contain kno (perating System commercial off-the-shelf components) (Pt yes) SUP-5.1 update? Does the device retains the operating system commercial off-the-shelf components (Pt yes) SUP-5.1 update? Does the device require vendor or vendor-authorized yes at the software components (OS, OTS) are updated at once a provided to some device require vendor or vendor-authorized yes at the device known to approve the positive or software update? SUP-5.1 update? Does the device for require vendor or vendor-authorized yes accession of the patients or software update? Does the device to install patches or software update? Does the medical device manufacturers (E.g., Not yes a sea above note yes above note yes above note yes and the software components (Pt yes) and the patches or software update? SUP-5.4 control to be installated whoma approved whoma approved whoma approved whoma approved in the patches or software updates? SUP-5.4 control to be installated or patches or software updates? SUP-5.4 control to be installated or patches or software updates? SUP-5.4 control to be installated or patches or software updates? SUP-5.4 control to be installated or patches or software updates? SUP-5.4 control to be installated or patches or software updates? SUP-6.5 control to be installated or patches or software updates? SUP-6.1 control (Pt yes) please provide details or remark the patches or yes updates? Does the device documentation provide instructions for yes updates? SUP-6.2 control (Pt yes) please provide details or remark the yes updates? Does the device documentation provide instructions (Pt yes) please yes updates? NA Does the device for require vendor or vendor authorized whoma approved instructions (Pt yes) please yes updates? NA Does the device documentation patches or yes updates? NA Does the device for invalidation of patches or yes updates? NA Does the device for the updates? NA Does the device for invalidation of yes the yes updates? NA Does the devi | | | | | | |
| Does the device contain Non-Operating System complete \$1.54.8 Description of the device Congonental (Psychologous) Complete \$1.54.8 Description of the device Congonental provide instructions for owner (operation installation of patches or software yes SUP-5.1 Does the device Congonental provide instructions for owner (operation installation of patches or software yes SUP-5.2 Does the device require vendor or vendor authorized see above note Does the device have the capability to receive remote installation of patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device whose the capability to receive remote in the patches or software updates? No Does the device contain other software components (e.g., saxt management) if yes, please provide details or management) if yes, please provide details or management in tribus and complete a.5.4.8. No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting of the patches or software updates? No Does the device require vendor or vendor-authorized sorting or the patches or software updates? No Does the device require vendor or vendor-authorized sorting or the patches or software upd | CCLID 4.4 | | N/A | | | |
| Sup-5 commercial of the select congeneration provide instructions Does the device documentation provide instructions Sup-5.1 Does the device require vendor or wendor-authorized ventre to installation of particles or software updates? Sup-5.2 Does the device require vendor or wendor-authorized ventre to installation of particles or software updates? Sup-5.3 Does the device require vendor or wendor-authorized ventre to installation of particles or software updates? Does the device require vendor or wendor-authorized ventre to provide instructions for the medical device manufacturer (e.g., Microsoft) to be installation of particles or software updates? Sup-5.4 Does the device ventre medical device approved for the software provide instructions for the device approved in the software provide instructions for the device documentation provide instructions for the medical device approved in the software updates? Does the device documentation provide instructions for the software updates? Does the device or software updates? Does the device or software updates? Does the device or software updates? Does the device require vendor or vendor-authorized ventre provide instructions for the software updates? Does the device or software updates? Does the device require vendor or vendor-authorized ventre provide instructions for the software updates? Does the device or software updates? Does the device or software updates? Does the device or software updates? Does the manufacturer of the customer when updates or software updates? Does the manufacturer mostly the customer when updates are supprised und without approval from the software updates are supplied upon administrator or software updates are sup | C3UF=4.4 | | IVA | _ | | |
| Complete 5.1.5.4.3. Does the device documentation provide instructions for owner (prepartor installation of patches or software updates? Does the device have the capability to recover remote very device to installation of patches or software updates? Does the device have the capability to recover remote very device to installation of patches or software updates? Does the device have the capability to recover remote very device to installation of patches or software updates? Does the device have the capability to recover remote very device the remoted device involved proposed installation of patches or software updates? Does the device have the capability to recover remote very device of the device have the capability to recover the very device of the device have the capability to recover the very device of the device of the device have the device and the software components (e.g., seater managements)? If yee, please provide details or device to installation of patches or device the capability to recover the device require vendor or vendor-authorized software to installation of patches or device the patches or or or device updates? No. A complete patches or device the updates of the device percent updates or anyther updates or anythe | | | | | | |
| Does the device require vendor or vendor-authorities (PS, OTS) are updated at once SUP-5.1 update? Ves at once Does the device require vendor or vendor-authorities vendor or vendor-authorities (PS, OTS) are updated at once SUP-5.2 boes the device require vendor or vendor-authorities vendor or vendor-authorities vendor or vendor-authorities (PS, OTS) are updated vendor or vendor-authorities vendor or vendor-authorities (PS, OTS) are updated vendor vendor-authorities vendor or vendor-authorities (PS, OTS) are updated vendor vendor-authorities vendor vendor-authorities (PS, OTS) are updated vendor vendor-authorities vendor vendor-authorities (PS, OTS) are updated vendor-authorities (PS, OTS) are updat | CCLID E | | Vos | | | |
| for comer/poperator installation of patches or software y test at the software components (05, OTS) are updated at once Update? Update? Update? Update? Update require vendor or vendor-authorized yes see above note SUP-5.1 update require vendor or vendor-authorized yes see above note SUP-5.2 update require vendor or vendor-authorized yes see above note SUP-5.3 update require vendor or patches or software updates? Update from any third-party manufacturers (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 | C3UF=3 | | res | _ | | |
| Does the device require vendor or vendor-authorized service to install patches or software updates? SUP-5.3 Does the device have the capability to receive receive and sufficient of the capability to receive received and supposed from the thing party manufacturers (e.g., Microsoft) to be installed without approval from the supposed from supposed from supposed from the supposed from the supposed fr | | | | All the coftware components (OS OTS) are undated | | |
| SUP-5.2 service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device contain other software updates? Does the device contain other software components (e.g., seet management) five, please provide details or reference in notes and complete 6.16.4. No Does the device contain of patches or software updates? SUP-6.1 updates? Does the device notes and complete 6.16.4. No Does the device notes and complete 6.16.4. No Does the device contain of patches or software updates? SUP-6.2 service to install patches or software updates? Does the device note management of the soft was updates? Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updates? N/A Does the device note management of the soft was updated whom the provision of the soft was updated and the soft was updated and the soft was updat | CCLID E 1 | | | | | |
| SUP-5.2 service to install patcher or software updates? UPS-5.3 installation of patches or software updates? Does the device have the capability to receive remote visualization of patches or software updates? Does the medical device manufacturer allow security visualization of patches or software updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the software components of the software updates are approved details or reference in notes and complete 6.1-6. SUP-6.1 Does the device contain other software components or ware free freence in notes and complete 6.1-6. SUP-6.1 Updates? SUP-6.1 Updates? Does the device require vendor or vendor-authorized service to install patcher or roftware updates? Does the device require vendor or vendor-authorized service to install patcher or roftware updates? UPS-6.2 Updates are approved from the manufacturer allow security updates? UPS-6.3 Updates are approved from the manufacturer allow security updates? UPS-6.4 Updates are approved for installation? UPS-7 Updates are approved for installation? UPS-8 Software updates are approved for installation? UPS-8 Software updates are approved for installation? UPS-8 Software updates are approved first third- Version and the capability to receive remote the capabi | C3UF=3.1 | upuates: | res | at once | | |
| SUP-5.2 service to install patcher or software updates? UPS-5.3 installation of patches or software updates? Does the device have the capability to receive remote visualization of patches or software updates? Does the medical device manufacturer allow security visualization of patches or software updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the software components of the software updates are approved details or reference in notes and complete 6.1-6. SUP-6.1 Does the device contain other software components or ware free freence in notes and complete 6.1-6. SUP-6.1 Updates? SUP-6.1 Updates? Does the device require vendor or vendor-authorized service to install patcher or roftware updates? Does the device require vendor or vendor-authorized service to install patcher or roftware updates? UPS-6.2 Updates are approved from the manufacturer allow security updates? UPS-6.3 Updates are approved from the manufacturer allow security updates? UPS-6.4 Updates are approved for installation? UPS-7 Updates are approved for installation? UPS-8 Software updates are approved for installation? UPS-8 Software updates are approved for installation? UPS-8 Software updates are approved first third- Version and the capability to receive remote the capabi | | Door the device require yander or yander authorized | | | | |
| Does the device have the capability to receive remote USUP-5.3 initialization of patches or software updates? Does the medical device manufacturer allow security updates from any thirdy-arty manufacturers (e.g., Microsoft) to be installation of patches or software updates? Does the device contain other software components (e.g., asset management) strivane, Icense management; by the, please provide details or reference in notes and complete 6.1-6.4. No Does the device contentation provide instructions for owner/operator installation of patches or software updates? NA Does the device require vendor or vendor-authorized SUP-6.1 updates? Does the device have the capability to receive remote survey. NA Does the medical device manufacturer allow security updates from any thirdy-aptry manufacturers (e.g., Microsoft) to be installed without approval from the Microsoft to be installed and thout approval from the Microsoft to be installed without approval from the Microsoft to be installed wit | CCLID E 3 | | Vos | con above note | | |
| SUP-5.3 installation of patches or software updates? Use she medical device munifactures related security updates from any third-party manufacturer (e.g., sask management) stoftware updates? SUP-5.4 manufacturer? Does the device contain other software components (e.g., sask management) stoftware (e.g., sask management) stoftware, license management) stoftware, license management is oftware updates? SUP-6.1 updates? Does the device quaire vendor or vendor-authorized service to install patches or software updates? NA Does the device faquire vendor or vendor-authorized service to install patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to install seld on the patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative requires vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer of low security updates from multiplicative requires vendor or vendor-authorized service to installation of patches or software updates? NA Does the device preform authorized reductive requires vendor or vendor-authorized service or installation of patches or software updates? NA Does the device preform authorized reductive red | CSUP-5.2 | service to instail patches of software updates: | res | see above note | | |
| SUP-5.3 installation of patches or software updates? Use she medical device munifactures related security updates from any third-party manufacturer (e.g., sask management) stoftware updates? SUP-5.4 manufacturer? Does the device contain other software components (e.g., sask management) stoftware (e.g., sask management) stoftware, license management) stoftware, license management is oftware updates? SUP-6.1 updates? Does the device quaire vendor or vendor-authorized service to install patches or software updates? NA Does the device faquire vendor or vendor-authorized service to install patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to install seld on the patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative require vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer allow security updates from multiplicative requires vendor or vendor-authorized service to installation of patches or software updates? NA Does the medical device manufacturer of low security updates from multiplicative requires vendor or vendor-authorized service to installation of patches or software updates? NA Does the device preform authorized reductive requires vendor or vendor-authorized service or installation of patches or software updates? NA Does the device preform authorized reductive red | | | | | | |
| Does the emelical device manufacturer allow security updates from any thirdy party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer (e.g., asset manugaments offware, license manugament)? If yes, please provide details or reference in notes and complete 6.1-6.4 Does the device documentation provide instructions for owner/poperator installation of patches or software updates? Does the device require vendor or vendor-authorized service to install patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturer (e.g., Microsoft) to be installed unthout approval from the manufacturer notify the customer when the patches or software updates from any third-party manufacturers (e.g., Microsoft) to be installed unthout approval from the manufacturer motify the customer when the patches or software updates from any updates from any third-party manufacturers (e.g., Microsoft) to be installed unthout approval from the manufacturer notify the customer when the patches or software updates from any under the part of the software updates from any under the patches or software updates from any under the patches or software updates are applied upon administrator available at startup. Does the device perform automatic installation of patches or software updates? Does the device perform automatic installation of patches or software updates are applied upon administrator applied upon administrator applied upon administrator approval. Does the manufacturer have an approved list of third- | CC110 F 2 | | | | | |
| update from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the SUP-5.4 manufacturer? Does the device contain other software components (e.g., asset management) if we, please provide details or reference in notes and complete 5.16-4. Does the device documentation provide instructions for owner/poeration installation of patches or software updates? SUP-6.1 Updates? Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote updates? N/A Does the device have the capability to receive remote updates of most ward updates or software updates? SUP-6.3 Does the manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer rotify the customer when updates or software updates or softwa | CSUP-5.3 | | Yes | see above note | | |
| Microsoft) to be installed without approval from the manufacturer allow security updates are applied without approval from the software updates? SUP-6.4 Microsoft) to be installed without approval from the software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.5 Updates are approved for installation of partners or software updates? SUP-6.6 Updates are approved for installation of partners or software updates? SUP-6.7 Updates are approved for installation of partners or software updates? SUP-8 Updates are approved for installation of partners or software updates? SUP-8 Updates are approved for installation of software updates? SUP-8 Updates are approved for installation of software updates? SUP-8 Updates are applied upon administrator applied upon administrator applied upon administrator approval. SUP-8 Updates are applied upon administrator applied upon administrator approval. SUP-8 Updates are applied upon administrator approval installation of software updates? SUP-8 Updates are applied upon administrator approval installation of software updates? SUP-8 Updates are applied upon administrator applied upon administrator approval. SUP-8 Updates are applied upon administrator applied upon administrator approval. SUP-8 Updates are applied upon administrator applied upon administrator approval. SUP-8 Updates are applied upon administrator approval installation of third-support approval. | | | | | | |
| SUP-5.4 manufacturer? Does the device contain other software components (e.g., asset management) flyes, please provide details or reference in notes and complete 6.1-6.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? SUP-6.1 updates? Does the device require vendor or vendor-authorised service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? SUP-6.2 installation of patches or software updates? Does the manufacturer of the updates are approved for installation? SUP-6.4 manufacturer? Does the manufacturer of the updates are approved for installation? SUP-8 software updates? Does the manufacturer allow security updates are approved for installation? SUP-8 Software updates? Does the manufacturer allow security updates are approved for installation of software updates are applied upon administrator approval. Does the manufacturer have an approved list of third- | | | | | | |
| Does the device contain other software components (e.g., assert managements of tware, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? N/A Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of software updates? Does the manufacturer and we capability to receive remote installation? Does the manufacturer notify the customer when updates are approved for installation? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | | | |
| (e.g., asset management software, license management) fly ess, please provide details or reference in notes and complete 6.1-6.4. No | CSUP-5.4 | | NO . | _ | | |
| management)? If yes, please provide details or reference in notes and complete 6.1-6.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? SUP-6.1 Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the MAN Device can be configured to verify if new update are updates are approved for installation? SUP-6.4 Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of No briter party software updates are applied upon administrator software updates? No Obes the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | | | | | | |
| SUP-6.1 poes the device vecumentation provide instructions for owner/operator installation of patches or software updates? SUP-6.1 poes the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when support of installation? Does the device perform automatic installation of software updates? Does the device perform automatic installation of software updates? Does the device perform automatic installation of software updates? N/A Device can be configured to verify if new update are available at startup. SUP-8 Does the manufacturer notify the customer when software updates? Yes available at startup. Does the manufacturer phave an approved list of third- No third party software can be installed on the | | | | | | |
| Does the device documentation provide instructions for owner/operator installation of patches or software updates? N/A Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when updates are approved for installation? Does the manufacturer notify the customer when updates are approved for installation of Does the device perform automatic installation of Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | | | | | | |
| for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when updates are approved for installation? Does the manufacturer mutical installation of software updates? Does the manufacturer and without approval from the manufacturer notify the customer when supparts and the provided for installation of software updates? Does the manufacturer and without approval from automatic installation of software updates are approved for installation of software updates? Does the manufacturer have an approved list of third- No third party software can be installed on the | CSUP-6 | | No | _ | | |
| Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when updates are approved for installation? Does the manufacturer outly the customer when superior of software updates? Does the device perform automatic installation? Does the device perform automatic installation of software updates? No Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | | | | | | |
| Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when SUP-7 updates are approved for installation? Does the manufacturer notify the customer when SUP-8 software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | | | |
| SUP-6.2 service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the SUP-6.4 manufacturer? Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of SUP-8 software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | CSUP-6.1 | updates? | N/A | _ | | |
| SUP-6.2 service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the SUP-6.4 manufacturer? Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of SUP-8 software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | | | | | | |
| Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when the possible of the possible of the customer when the possible of the pos | | | | | | |
| SUP-6.3 installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when SUP-7 updates are approved for installation? Does the manufacturer match installation of Software updates? No boes the device perform automatic installation of Software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | CSUP-6.2 | service to install patches or software updates? | N/A | _ | | |
| SUP-6.3 installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when SUP-7 updates are approved for installation? Does the manufacturer match installation of Software updates? No boes the device perform automatic installation of Software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- | | | | | | |
| Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer notify the customer when Device can be configured to verify if new update are available at startup. SUP-6.4 manufacturer notify the customer when Updates are approved for installation? SUP-7 updates are approved for installation? Does the device perform automatic installation of Software updates are applied upon administrator approval. No Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | | | |
| updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the SUP-6.4 manufacturer? N/A Device can be configured to verify if new update are updates are approved for installation? Very available at startury. Does the device perform automatic installation of SUP-8 software updates? No approved is of third- | CSUP-6.3 | | N/A | _ | | |
| Microsoft) to be installed without approval from the manufacturer notify the customer when Device can be configured to verify if new update are supplied upon administrator approved for installation? Does the device perform automatic installation of SUP-8 Software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | | | |
| SUP-6.4 manufacturer? Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of Software updates? Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | | updates from any third-party manufacturers (e.g., | | | | |
| Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of SUP-8 software updates? Does the device perform automatic installation of Software updates? No Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | | Microsoft) to be installed without approval from the | | | | |
| Does the manufacturer notify the customer when updates are approved for installation? Does the device perform automatic installation of SUP-8 software updates? Does the device perform automatic installation of Software updates? No Does the manufacturer have an approved list of third- Does the manufacturer have an approved list of third- No third party software can be installed on the | CSUP-6.4 | manufacturer? | N/A | _ | | |
| SUP-7 updates are approved for installation? Does the device perform automatic installation of software updates? No approval. Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | Device can be configured to verify if new update are | | |
| Does the device perform automatic installation of software updates? No Software updates are applied upon administrator approval. Does the manufacturer have an approved list of third- No third party software can be installed on the | CSUP-7 | | Yes | | | |
| SUP-8 software updates? No approval. Does the manufacturer have an approved list of third- No third party software can be installed on the | | | | | | |
| Does the manufacturer have an approved list of third- No third party software can be installed on the | CSUP-8 | | No | | | |
| | ··· • | | | | | |
| | | Does the manufacturer have an approved list of third- | | No third party software can be installed on the | | |
| | CSUP-9 | | | | | |
| | | ,, | | | | |

| iuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | |
|--------------------|--|-----------|------------------------|--|
| | Can the owner/operator install manufacturer- | | | |
| | approved third-party software on the device | | | |
| CSUP-10 | themselves? | No | _ | |
| | Does the system have mechanism in place to prevent | | | |
| CSUP-10.1 | installation of unapproved software? | Yes | _ | |
| | Does the manufacturer have a process in place to | | | |
| CSUP-11 | assess device vulnerabilities and updates? | Yes | _ | |
| | Does the manufacturer provide customers with | | | |
| CSUP-11.1 | review and approval status of updates? | No | _ | |
| CSUP-11.2 | Is there an update review cycle for the device? | Yes | At most every 2 months | |

| | HEALTH DATA DE-IDENTIFICATION (DIDT) The ability of the device to directly remove information that allows identification of a person. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
|-----------------------------|---|---------------|---|--|-----------------------|------------------------|
| DIDT-1 DIDT-1.1 | Does the device provide an integral capability to de- identify personally identifiable information? Does the device support de-identification profiles that comply with the DICOM standard for de- identification? | Yes | For Logs: Clear logs in system configer on on DICOM export on USB/CD/DVD:Jpeg export of US images are anonymised (as soon so perator does not entre PHI in annotation)screenshot of patient folder are not anonymised patient name, DoB, Patient ID, accession# may be visible)report are not anonymised (patient name, DoB, Patient ID, accession# may be visible) | Section 5.6, DIDT Section 5.6, DIDT | None None | ISO 27038 ISO 27038 |
| | | | | | | |
| | DATA BACKUP AND DISASTER RECOVERY (DTBK) The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| DTBK-1 | The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to | No . | - | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| DTBK-1 DTBK-2 | The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? | | - | IEC TR 80001-2-2:2012 Section 5.7, DTBK | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? | No _ | - - - | | | |
| DTBK-2 DTBK-3 | The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a hackup capability for system configuration information, patch restoration, and software restoration? | No Yes Yes No | | Section 5.7, DTBK | CP-9 | A.12.3.1 |
| DTBK-2 DTBK-3 DTBK-4 | The obility to recover ofter damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? | No Yes Yes No | System configuration can be backed up | Section 5.7, DTBK | CP-9 | A.12.3.1 |
| DTBK-2 DTBK-3 DTBK-4 DTBK-5 | The ability to recover ofter damage or destruction of device data, hardware, software, or site configuration information. Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the | Yes | System configuration can be backed up | Section 5.7, DTBK Section 5.7, DTBK | CP-9 CP-9 | A.12.3.1 A.12.3.1 |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|----------------------|---|------------|--|-----------------------|-----------------------|---|
| | HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) How the device ensures that the stored data on the | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | device has not been altered or destroyed in a non- authorized manner and is from the originator. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital | | | | | |
| IGAU-1 | signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., | Yes | The mechanisms are provided by the OS | Section 5.9, IGAU | SC-28 | A.18.1.3 |
| IGAU-2 | RAID-5)? | Yes | The mechanisms are provided by the OS | Section 5.9, IGAU | SC-28 | A.18.1.3 |
| | MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware). | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| MLDP-1 | Is the device capable of hosting executable software? | No | User has no access to underlying OS, MAC prevent installation of software and partitions are mounted in noewe: Malicious code protection mechanisms by: - Use of secure Open-source operating system - Pervasive configuration management and comprehensive software integrity controls are used | Section 5.10, MLDP | | |
| | Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide | | to prevent execution of unauthorized code - secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than | | | |
| MLDP-2 | details or reference in notes. Does the device include anti-malware software by | Yes | the functions intended | Section 5.10, MLDP | SI-3 | A.12.2.1 A.9.2.3, A.9.4.5, A.12.1.2, |
| MLDP-2.1 | default? Does the device have anti-malware software available | | _ | Section 5.10, MLDP | CM-5 | A.12.1.4, A.12.5.1 |
| MLDP-2.2 | as an option? Does the device documentation allow the | No | _ | Section 5.10, MLDP | AU-6 | A.12.4.1, A.16.1.2, A.16.1.4 |
| MLDP-2.3 | owner/operator to install or update anti-malware software? Can the device owner/operator independently (re- | No | _ | Section 5.10, MLDP | CP-10 | A.17.1.2 |
| MLDP-2.4 |)configure anti-malware settings? Does notification of malware detection occur in the | No | - | Section 5.10, MLDP | AU-2 | None |
| MLDP-2.5 | device user interface? Can only manufacturer-authorized persons repair | N/A | | | | |
| MLDP-2.6 MLDP-2.7 | systems when malware has been detected? Are malware notifications written to a log? | Yes N/A | | | | |
| MLDP-2.8 | Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? | Yes | | | | |
| | | | Device has been designed to not execute any data imported on the system. only Signed software components can be installed on system. SuperSonic Imagine recommends the following cyber | | | |
| | | | Hygiene practices: Ensure that your equipment is in a physically protected and actively monitored area; | | | |
| | | | Ensure that only secure/sanitized USB storage devices are utilized; Ensure that your equipment is protected against network access by unsupervised systems | | | |
| | If the answer to MLDP-2 is NO, and anti-malware | | (typically provided by mechanisms such as firewalls and VPNs); and | | | |
| MLDP-3 | cannot be installed on the device, are other compensating controls in place or available? Does the device employ application whitelisting that | Yes | Ensure your data has been backed up and stored according to your institution policy. | Section 5.10, MLDP | SI-2 | A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3 |
| MLDP-4 | restricts the software and services that are permitted to be run on the device? Does the device employ a host-based intrusion | No | - | Section 5.10, MLDP | SI-3 | A.12.2.1 |
| MLDP-5 | detection/prevention system? Can the host-based intrusion detection/prevention | No | - | Section 5.10, MLDP | SI-4 | None |
| MLDP-5.1 | system be configured by the customer? Can a host-based intrusion detection/prevention | N/A | - | Section 5.10, MLDP | CM-7 | A.12.5.1 |
| MLDP-5.2 | system be installed by the customer? | No | _ | Section 5.10, MLDP | | |
| | NODE AUTHENTICATION (NAUT) The ability of the device to authenticate communication partners/nodes. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|--------------------------|---|-----------|---|-----------------------|-----------------------|--|
| | 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 | | | | | |
| NAUT-1 | authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)? Are network access control mechanisms supported | Yes | DICOM TLS | Section 5.11, NAUT | SC-23 | None |
| NAUT-2 | (E.g., does the device have an internal firewall, or use a network connection white list)? Is the firewall ruleset documented and available for | No | reduced number of services available | Section 5.11, NAUT | SC-7 | A.13.1.1, A.13.1.3, A.13.2.1,A.14.1.3 |
| NAUT-2.1 | review? Does the device use certificate-based network | N/A | - | | | |
| NAUT-3 | connection authentication? | Yes | DICOM TLS | | | |
| | 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. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| CONN-1 | Does the device have hardware connectivity capabilities? | Yes | | | | |
| CONN-1.1 | Does the device support wireless connections? | Yes | _ | | | |
| CONN-1.1.1 CONN-1.1.2 | Does the device support Wi-Fi? Does the device support Bluetooth? | Yes No | _ | | | |
| CONN-1.1.3 | Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? | No | | | | |
| | Does the device support other wireless connections | | _ | | | |
| CONN-1.1.4 CONN-1.2 | (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? | No 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. | | | | |
| | | | The supported network protocols are: DICOM, DHCP, NTP. | | | |
| | Does the manufacturer provide a list of network ports and protocols that are used or may be used on the | | HTTPS protocol may be enabled for remote | | | |
| CONN-2 | device? Can the device communicate with other systems | Yes | maintenance. | | | |
| CONN-3 | within the customer environment? | Yes | The device may be connected to a PACS, to a Modality Worklist, to a printer. | | | |
| | Can the device communicate with other systems external to the customer environment (e.g., a service | | | | | |
| CONN-4 | host)? | Yes | The device may be remotely serviceable | | | |
| CONN-5 | Does the device make or receive API calls? Does the device require an internet connection for its | No | _ | | | |
| CONN-6 | intended use? | No | _ | | | |
| CONN-7 | Does the device support Transport Layer Security (TLS)? | Yes | for DICOM connection | | | |
| CONN-7.1 | Is TLS configurable? | Yes | see DICOM Conformance statement and User Guide | | | |
| | Does the device provide operator control functionality | · | | | | |
| CONN-8 | from a separate device (e.g., telemedicine)? | No No | _ | | | |
| | PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | Does the device support and enforce unique IDs and passwords for all users and roles (including service | | 4 accounts exists: emergency access, sonographer, | | | |
| PAUT-1 | accounts)? | Yes | admin and service | Section 5.12, PAUT | IA-2 | A.9.2.1 |
| | Does the device enforce authentication of unique IDs and passwords for all users and roles (including | | | | | |
| PAUT-1.1 | service accounts)? | No | _ | Section 5.12, PAUT | IA-2 | A.9.2.1 |
| | Is the device configurable to authenticate users through an external authentication service (e.g., MS | | | | | |
| PAUT-2 | Active Directory, NDS, LDAP, OAuth, etc.)? | No | _ | Section 5.12, PAUT | IA-5 | A.9.2.1 |
| PAUT-3 | Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? | No | _ | Section 5.12, PAUT | IA-2 | A.9.2.1 |
| | Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the | | | | | A.14.1.1, A.14.2.7, A.14.2.9, |
| PAUT-4 | documentation? | Yes | - | Section 5.12, PAUT | SA-4(5) | A.15.1.2 |
| PAUT-5 | Can all passwords be changed? | Yes | _ | Section 5.12, PAUT | | |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|----------------------|--|-----------|--|---------------------------------------|-----------------------|------------------------------|
| PAUT-6 | Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules? Does the device support account passwords that expire periodically? | No No | - | Section 5.12, PAUT | IA-2 | A.9.2.1 |
| PAUT-8 PAUT-9 | Does the device support multi-factor authentication? Does the device support single sign-on (SSO)? | | _ | Section 5.12, PAUT | IA-2 | A.9.2.1 |
| PAUT-10 PAUT-11 | Can user accounts be disabled/locked on the device? Does the device support biometric controls? | | _ | Section 5.12, PAUT Section 5.12, PAUT | IA-2 IA-2 | A.9.2.1 A.9.2.1 |
| PAUT-12 | Does the device support physical tokens (e.g. badge access)? Does the device support group authentication (e.g. | No | _ | | | |
| PAUT-14 | hospital teams)? Does the application or device store or manage authentication credentials? | No Yes | - | | | |
| PAUT-14.1 | Are credentials stored using a secure method? | Yes | Person authentication is achieved through the Linux Pluggable Authentication Module (PAM) is a mechanism | | | |
| 7707 2412 | PHYSICAL LOCKS (PLOK) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | 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. Are all device components maintaining personally identifiable information (other than removable | No | - | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-2 | media) physically secure (i.e., cannot remove without tools)? Are all device components maintaining personally identifiable information (other than removable | Yes | - | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-3 | media) physically secured behind an individually keyed locking device? Does the device have an option for the customer to | No | disks maintaining e-PHI are crypted | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-4 | attach a physical lock to restrict access to removable media? | No | | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| | 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. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| RDMP-1 | Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development? Does the manufacturer evaluate third-party | Yes | IEC 62304 | Section 5.14, RDMP | CM-2 | None |
| RDMP-2 | applications and software components included in the device for secure development practices? Does the manufacturer maintain a web page or other | Yes | _ | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| RDMP-3 | source of information on software support dates and updates? | No | If remote service is enabled user can be notified when an update is available At most every 2 months a service pack will be released incorporating security patch when necessary, and every year a major release with an | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| RDMP-4 | Does the manufacturer have a plan for managing third party component end-of-life? | d. Yes | updated version of the OS and 3rd party components will be released. | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| | 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. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| SBOM-1 SBOM-2 | Is the SBoM for this product available? Does the SBoM follow a standard or common method in describing software components? | Yes No | - | | | |
| SBOM-2.1 SBOM-2.2 | Are the software components identified? Are the developers/manufacturers of the software components identified? | Yes | Ξ- | | | |
| | | | _ | | | |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|--------------------|--|-----------|--|-----------------------|------------------------|---|
| | Are the major version numbers of the software | | | | | |
| SBOM-2.3 | components identified? | Yes | _ | | | |
| SBOM-2.4 | Are any additional descriptive elements identified? | No | _ | | | |
| | Does the device include a command or process | | | | | |
| | method available to generate a list of software | | | | | |
| SBOM-3 | components installed on the device? | No | _ | | | |
| SBOM-4 | Is there an update process for the SBoM? | No | _ | | | |
| | | | | | | |
| | SYSTEM AND APPLICATION HARDENING (SAHD) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | The device's inherent resistance to cyber attacks and | | | EC 11 00001 2 2.2012 | 14151 51 000 55 Nev. 4 | 130 27002.2013 |
| | malware. | | | | CM-7 | A.12.5.1* |
| | | | | | | |
| | | | The following compensation are implemented to | | | |
| | | | harden system | | | |
| | | | - Single-function system: US | | | |
| | | | Address space layout randomization (ASLR) Protected database link (only local access enabled, | | | |
| | | | password protection)Unused services disabled | | | |
| | | | - Remote loging service disabled | | | |
| | | | - Use of Mandatory Access Control (MAC) | | | |
| | | | mecanism | | | |
| | Is the device hardened in accordance with any | | - Least privilege principle | | | A.6.2.1, A.6.2.2, A.13.1.1, |
| SAHD-1 | industry standards? | Yes | - Least functionality principle | Section 5.15, SAHD | AC-17(2)/IA-3 | A.13.2.1, A.14.1.2/None |
| CALLE O | Has the device received any cybersecurity | | | | 64 42(42) | A.14.2.7, A.15.1.1, A.15.1.2, |
| SAHD-2 | certifications? Does the device employ any mechanisms for software | No | _ | Section 5.15, SAHD | SA-12(10) | A.15.1.3 |
| SAHD-3 | integrity checking | No | | | | |
| JAIID-J | integrity checking | NO | All the software included in the medical device are | | | |
| | | | provided by a trusted source provider (GNU/Linux | | | |
| | | | Debian). The Debian packages that are included on | | | |
| | Does the device employ any mechanism (e.g., release- | | the medical devices are digitally signed by | | | |
| | specific hash key, checksums, digital signature, etc.) to | | SuperSonic Imagine. | | | |
| | ensure the installed software is manufacturer- | | Debian package is a tamper-evident packaging | | | |
| SAHD-3.1 | authorized? | Yes | format. All the software included in the medical device are | | | |
| | | | provided by a trusted source provider (GNU/Linux | | | |
| | | | Debian). The Debian packages that are included on | | | |
| | Does the device employ any mechanism (e.g., release- | | the medical devices are digitally signed by | | | |
| | specific hash key, checksums, digital signature, etc.) to | | SuperSonic Imagine. | | | |
| | ensure the software updates are the manufacturer- | | Debian package is a tamper-evident packaging | | | |
| SAHD-3.2 | authorized updates? | Yes | format. | Section 5.15, SAHD | CM-8 | A.8.1.1, A.8.1.2 |
| | Can the owner/operator perform software integrity checks (i.e., verify that the system has not been | | | | | A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, |
| SAHD-4 | modified or tampered with)? | No | | Section 5.15, SAHD | AC-3 | A.14.1.2, A.14.1.3, A.18.1.3 |
| 3/11/2 4 | Is the system configurable to allow the | | _ | | | ,, |
| | implementation of file-level, patient level, or other | | | | | |
| SAHD-5 | types of access controls? | No | _ | Section 5.15, SAHD | CM-7 | A.12.5.1* |
| | | | Emergency access can only acquire images | | | |
| | | | Sonographer role can acquire images, manage | | | |
| | | | exams, export exams, and change non-security settings | | | |
| | | | admin roles can do all the above plus change | | | |
| SAHD-5.1 | Does the device provide role-based access controls? | Yes | security settings. | Section 5.15, SAHD | CM-7 | A.12.5.1* |
| | Are any system or user accounts restricted or disabled | | , | | ****** * | |
| SAHD-6 | by the manufacturer at system delivery? | No | _ | Section 5.15, SAHD | CM-8 | A.8.1.1, A.8.1.2 |
| | Are any system or user accounts configurable by the | | | | | |
| SAHD-6.1 | end user after initial configuration? | No | Only password can be changed | Section 5.15, SAHD | CM-7 | A.12.5.1* |

Does this include restricting certain system or user accounts, such as service technicians, to least

Are all shared resources (e.g., file shares) which are not required for the intended use of the device

Are all communication ports and protocols that are not required for the intended use of the device

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

Are all applications (COTS applications as well as OSincluded applications, e.g., MS Internet Explorer, etc.)

which are not required for the intended use of the

privileged access?

deleted/disabled?

device deleted/disabled?

disabled?

disabled?

SAHD-6.2

SAHD-7

SAHD-8

SAHD-9

SAHD-10

A minimal version of the OS is installed on the device. No remote logging, no web browser or mail

user agent are installed

CM-7

CM-7

SA-18

CM-6

SI-2

Section 5.15, SAHD

A.12.5.1*

A.12.5.1*

None

None

A.12.6.1, A.14.2.2, A.14.2.3,

A.16.1.3

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | 15-Nov-2020 | | | |
|--|--|---------------------------------|--|---|---|--|
| 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 | Disabled in the BIOS | | | |
| 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? Can the device be hardened beyond the default | | _ | | | |
| SAHD-14 SAHD-14.1 | provided state? Are instructions available from vendor for increased hardening? | Yes | — see User Guide | | | |
| SHAD-15 | Can the system prevent access to BIOS or other bootloaders during boot? | No | see oser outse | | | |
| SAHD-16 | Have additional hardening methods not included in 2.3.19 been used to harden the device? | No | _ | | | |
| | SECURITY GUIDANCE (SGUD) Availability of security guidance for operator and administrator of the device and manufacturer sales and service. | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| SGUD-1 | Does the device include security documentation for the owner/operator? Does the device have the capability, and provide | Yes | Security information are included in the User Guide | Section 5.16, SGUD | AT-2/PL-2 | A.7.2.2, A.12.2.1/A.14.1.1 |
| SGUD-2 | instructions, for the permanent deletion of data from the device or media? | No | Permanent deletion of data require storage device destruction. | Section 5.16, SGUD | MP-6 | A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 |
| SGUD-3 | Are all access accounts documented? Can the owner/operator manage password control for | Yes | — each user can change his own password, but admin | Section 5.16, SGUD | AC-6,IA-2 | A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5/A.9.2.1 |
| SGUD-3.1 | all accounts? Does the product include documentation on | Yes | can change all passwords | | | |
| SGUD-4 | recommended compensating controls for the device? | Yes | _ | | | |
| | | | | | | |
| | HEALTH DATA STORAGE CONFIDENTIALITY (STCF) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | (STCF) The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| Tree 4 | (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. | | e-PHI contained in database, DICOM objects, native archives and logs are stored on an encrypted | | | |
| STCF-1 STCF-1.1 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by | Yes Yes | archives and logs are stored on an encrypted partition using TPM1.2 | IEC TR 80001-2-2:2012 Section 5.17, STCF | NIST SP 800-53 Rev. 4 SC-28 | ISO 27002:2013 |
| | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to | | archives and logs are stored on an encrypted | | | |
| STCF-1.1 STCF-1.2 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? | Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled | | | |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 STCF-3 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the | Yes No No Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF | SC-28 | A.8.2.3 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? | Yes No No | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF | SC-28 | A.8.2.3 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the device? | Yes No No Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF | SC-28 | A.8.2.3 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? TRANSMISSION CONFIDENTIALITY (TXCF) The ability of the device to ensure the confidentiality of transmitted personally identifiable information. | Yes No No Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF Section 5.17, STCF | SC-28 SC-28 | A.8.2.3 A.8.2.3 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 STCF-3 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the device? TRANSMISSION CONFIDENTIALITY (TXCF) | Yes No No Yes No | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF Section 5.17, STCF | SC-28 SC-28 | A.8.2.3 A.8.2.3 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 STCF-3 STCF-4 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the device? TRANSMISSION CONFIDENTIALITY (TXCF) The ability of the device to ensure the confidentiality of transmitted personally identifiable information be transmitted only via a point-to-point dedicated cable? Is personally identifiable information encrypted prior to transmission via a network or removable media? | Yes No No No Yes No | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during | Section 5.17, STCF Section 5.17, STCF IEC TR 80001-2-2:2012 | SC-28 SC-28 NIST SP 800-53 Rev. 4 | A.8.2.3 A.8.2.3 ISO 27002:2013 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 STCF-3 STCF-4 TXCF-1 TXCF-1 TXCF-2 TXCF-2.1 | (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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the device? TRANSMISSION CONFIDENTIALITY (TXCF) The ability of the device to ensure the confidentiality of transmitted personally identifiable information. Can personally identifiable information be transmitted only via a point-to-point dedicated cable? Is personally identifiable information encrypted prior to transmission via a network or removable media? If data is not encrypted by default, can the customer configure encryption options? | Yes Yes No No No Yes No Yes Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during installation. There is no way to change them — No encryption on removable media. Data transmited over the network are crypted | Section 5.17, STCF Section 5.17, STCF IEC TR 80001-2-2:2012 Section 5.18, TXCF Section 5.18, TXCF | SC-28 SC-28 NIST SP 800-53 Rev. 4 CM-7 CM-7 | A.8.2.3 A.8.2.3 ISO 27002:2013 A.12.5.1 A.12.5.1 |
| STCF-1.1 STCF-1.2 STCF-1.3 STCF-2 STCF-3 STCF-4 TXCF-1 | 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. Can the device encrypt data at rest? Is all data encrypted or otherwise protected? Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured? Is the data stored in a database located on the device? Is the data stored in a database external to the device? ITRANSMISSION CONFIDENTIALITY (TXCF) The ability of the device to ensure the confidentiality of transmitted only via a point-to-point dedicated cable? Is personally identifiable information be transmitted only via a point-to-point dedicated cable? Is personally identifiable information encrypted prior to transmission via a network or removable media? If data is not encrypted by default, can the customer configure encryption options? Is personally identifiable information transmission restricted to a fixed list of network destinations? | Yes Yes No No Yes No Yes | archives and logs are stored on an encrypted partition using TPM1.2 Encryption can't be disabled Encryption can't be disabled or configured The encryption keys are generated during installation. There is no way to change them | Section 5.17, STCF Section 5.17, STCF IEC TR 80001-2-2:2012 Section 5.18, TXCF | SC-28 SC-28 NIST SP 800-53 Rev. 4 | A.8.2.3 A.8.2.3 ISO 27002:2013 |

| SuperSonic imagine | Aixplorer MACH30 V3.X Aixplorer MACH20 V3.X | RD.DD.533 | | | | | | |
|--------------------|--|-----------|--------------------------|--|-----------------------|-----------------------|--|--|
| TXCF-5 | Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? | Yes | DICOM TLS is implemented | | | | | |
| | TRANSMISSION INTEGRITY (TXIG) The ability of the device to ensure the integrity of transmitted data. | | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 | |
| TXIG-1 | Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables? | Yes No | DICOM TLS | | Section 5.19, TXIG | SC-8 | A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 | |
| TAIG-2 | connected by external capies: | | _ | | | | | |
| | REMOTE SERVICE (RMOT) | | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 | |
| | 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 | _ | | | AC-17 | A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2 | |
| RMOT-1.1 | Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair? | Yes | _ | | | | | |
| | Is there an indicator for an enabled and active remote | | | | | | | |

The device can be configured to send daily reports.

Those report do not contain any e-PHI.

Software update

OTHER SECURITY CONSIDERATIONS (OTHR)

functionality (e.g. software updates, remote training)? Yes

Can patient data be accessed or viewed from the

Does the device permit or use remote service

connections for predictive maintenance data?

Does the device have any other remotely accessible

device during the remote session?

NONE

session?

RMOT-1.2

RMOT-1.3

RMOT-2

RMOT-3

Notes:

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

Note 1 information

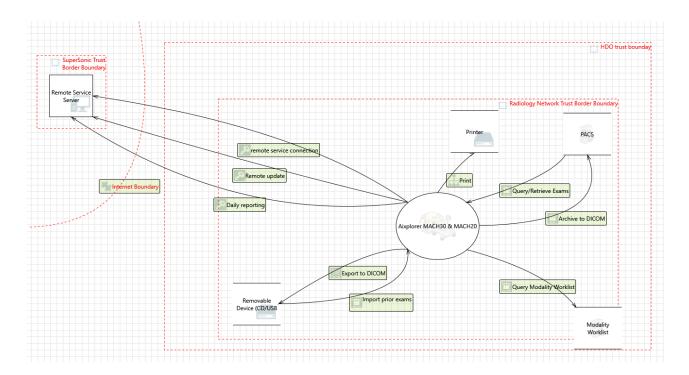
IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

AC-17

ISO 27002:2013

A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2



| Component Name | Manufacturer | Description | Version |
|-----------------------|---|---|---|
| Debian 9 "Stretch" | Debian Community (Open Source) | Debian is an open source operating system (OS) | Debian 9 "Stretch" |
| Linux Kernel | (Open Source) | Linux image base package | 4.9.0-12 |
| Grub | (Open Source) | GRand Unified Bootloader, version 2 (PC/BIOS version) | 2.02~beta3-5 |
| Cairo | (Open Source) | Cairo 2D vector graphics library | 1.14.6-1gaussian1 |
| GNU/libc | (Open Source) | Embedded GNU C Library | 2.24-11+deb9u4 |
| Glib | (Open Source) | GLib library of C routines | 2.50.3-2+deb9u1 |
| libstdC++ | (Open Source) | GNU Standard C++ Library v3 | 6.3.0-18+deb9u1 |
| bash | (Open Source) | GNU Bourne Again SHell | 4.4-5 |
| python | (Open Source) | interactive high-level object-oriented language | 3.5.3-1 |
| Xorg | Free Desktop (Open Source) | X.Org X Window System | 1:7.7+19 |
| Redshift | Open Source | Adjusts the color temperature of your screen | 1.11-1 |
| Xfce | Xfce(Open Source) | Xfce desktop environment | 4.12.3 |
| xscreensaver | Open Source | Screensaver daemon and frontend for X11 | 5.36-1 |
| PostgreSQL | PostgreSQL (Open Source) | object-relational SQL database | 9.6+181+deb9u3 |
| Xerces | Apache Foundation (Open Source) | Xerces is a validating XML parser written in a portable subset of C++ | 3.1.4+debian-2+deb9u1 |
| Dcmtk | OFFIS (Oldenburg Research and Development Institute for Information Technology Tools and Systems) | DICOM toolkit | 3.6.5-11gaussian1 |
| dvd+rw-tools | Andy Polyakov (Open Source) | collection of open source DVD and Blu-ray Disc burning tools for Linux | 7.1-11.1 |
| Eject | (Open Source) | Eject is a utility that allows to eject CD-ROM. No documentation is provided to the end user. | 2.1.5+deb1+cvs20081104-13.2 |
| xorriso | (Open Source) | command line ISO-9660 and Rock Ridge manipulation tool | 1.4.6-1+b1 |
| Libusb-1.0.0 | (Open Source) | user space USB programming library | 2:1.0.21-1 |
| PulseAudio | (Open Source) | PulseAudio is a network-capable sound server program distributed via the freedesktop.org project | 10.0-1+deb9u1 |
| libcanberra0 | (Open Source) | simple abstract interface for playing event sounds with pulseAudio backend | 0.30-3 |
| CUDA | Nvidia | CUDA allows faster image processing and therefore it is very useful to an imaging system. Provided by the Aixplorer series graphics card manufacturer – Nvidia. | 430.50-1 |
| Cg | Nvidia | Nvidia Cg core runtime library | 3.1.0013-2+b1 |
| OpenCV | (Open Source) | computer vision Image Processing library | 2.4.13.7-0gaussiane2 |
| OpenMP | (Open Source) | OpenMP (Open Multi-Processing) is an application programming interface (API) that supports multi-platform shared memory multiprocessing programming in C, C++ | 6.3.0-18+deb9u1 |
| Intel MKL | Intel (Open Source) | Intel® Math Kernel Library (Intel® MKL) | 2019.1.144-3~bpo9+1 |
| IIICI IVIKE | mer (open source) | Intel® Threading Building Blocks (Intel® TBB) lets you easily write parallel C++ | |
| TBB (libtbb2) | Intel (Open Source) | programs that take full advantage of multicore performance, | 4.3~20150611-2 |
| libdbus-c++ | (Open Source) | C++ API for D-Bus (runtime package) | 0.9.0-9gaussian2 |
| opendds | OCI | OpenDDS is an Open Source, native C++ implementation of the OMG (Object Management Group) Data Distribution Service (DDS) for Real-Time Systems specification. | 3.14.1-0gaussiane0 |
| pam | (Open Source) | Pluggable Authentication Modules | 1.1.8-3.6 |
| F | (open source) | PAM module to authenticate using a PostgreSQL database. | |
| libpam-pgsql | (Open Source) | This module lets you authenticate users against a table in a PostgreSQL database. It also supports checking account information and updating authentication tokens (i.e., passwords). | 0.7.3.2-1 |
| gconf2 | (Open Source) | GNOME configuration database system (shared libraries) | 3.2.6-4gaussian1 |
| gtk2 & libgtkmm | (Open Source) | gtk2: Development environment for GTK toolkit for graphical user interfaces. libgtkmm: C++ wrappers for GTK+ (shared libraries) | gtk2: 2.24.31-1gaussian1 libgtkmm: 1:2.24.5-1gaussian1 |
| h 4-:- | (0, 6,) | | |
| Maia | (Open Source) | Maia vectorial canvas | 0.3.21-0gaussiane1 |
| CUPS | (Open Source) | Common UNIX Printing System(tm) | 2.2.1-8+ deb9u6 2.1.2-1.1+deb9u5 |
| libopenjp2 | (Open Source) (Open Source) | JPEG 2000 image compression/decompression library Implementation of the JPEG-LS standard | 2.1.2-1.1+deb9u5 1.1.0+dfsg-2 |
| charls libsensors4 | , | | 1:3.4.0-4 |
| Thingworx-ssiclient | (Open Source) PTC | library to read temperature/voltage/fan sensors Thingworx client for SuperSonic Imagine's Aixplorers. | 0.7.8-0gaussiane7 (for customer site environment) |
| v11vnc | (Onen Source) | | 0.3.10-0gaussiane1(for production environment |
| x11vnc | (Open Source) | VNC server to allow remote access to an existing X session | 0.9.13-2+deb9u1 |
| rastertosonyhs | Sony | Sony CUPS raster filter for UP-D897, UP-990AD, UP-970AD and UP-711MD | 1.4.1-0gaussian6 |
| rastertosony | Sony | Sony CUPS raster filter for Sony UP-DR80MD, UP-D25MD, UP-991AD, UP- 971AD, UP-D898MD, UP-X898MD | 1.4.0.2-0gaussiane2 |
| Inam 2d007 | Sony | Sony pgm2d897 converter | 0.0.3-0gaussian2 |
| pgm2d897 | | | |
| pnm2d23md upd23md | Sony Sony | Sony pnm2d23md converter Sony upd23md cups driver | 0.0.2-0gaussian2 1.0.10-0gaussian2.1 |