

## Manufacturer Disclosure Statement for Medical Device Security - MDS<sup>2</sup>

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
<b>Question ID</b>	<b>Question</b>	<b>Answer</b>	<b>See note</b>
DOC-1	Manufacturer Name	Hologic SuperSonic imagine	—
DOC-2	Device Description	Ultrasound imaging modality	—
DOC-3	Device Model	SuperSonic MACH 20/30/40 V3.0	—
DOC-4	Document ID	RD.REC.115	—
DOC-5	Manufacturer Contact Information	Cybersecurity questions shall be asked to cybersecurity@supersonicimagine.com For other inquiries please contact your local representative.	—
DOC-6	Intended use of device in network-connected environment:	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 - 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-7	Document Release Date	11/15/2020	—
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	Vulnerabilities information available at: <a href="https://www.supersonicimagine.Com/security">https://www.supersonicimagine.Com/security</a>
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?	N/A	—
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	—
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	—
DOC-11.4	Is the SaMD hosted by the customer?	N/A	—
		Yes, No, N/A, or See Note	Note #
	<b>MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION</b>		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	This device download, display, transmit and store the following PII: • Patient Name • Patient ID • Patient Age • Date of birth
MPII-2	Does the device maintain personally identifiable information?	Yes	

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
MP11-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	---
MP11-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	---
MP11-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	---
MP11-2.4	Does the device store personally identifiable information in a database?	Yes	---
MP11-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	By default, the exams must be manually deleted. However the device can be configured to delete : <ul style="list-style-type: none"> <li>• all the exams after a configurable period of time</li> <li>• all the archived exams after a configurable period of time</li> <li>• all the exams archived and committed after a configurable period of time</li> <li>• the oldest exams when disk is full after a configurable period of time</li> </ul>
MP11-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	The device will query PII from the modality worklist server, and transmit PHI on PACS and on removable media (CD/DVD/USB)
MP11-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	The PHI are stored on a crypted partition
MP11-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	
MP11-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	Yes	The PHI are stored on a dedicated crypted partition separated from the device's Operating System.
MP11-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	e-PHI can be transmitted over DICOM Storage service, exportation on removable device and backup restore
MP11-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	e-PHI are displayed on main screen
MP11-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	Yes	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
MP11-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)?	Yes	The device can record PII to USB removable HDD, USB Memory, DVD-R/RW, CD-R/RW. The device can also import and display PHI from the above-mentioned device (but it is a purchasable option)
MP11-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	---
MP11-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	The device can connect to Ethernet networks
MP11-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., Wi-Fi, Bluetooth, NFC, infrared, cellular, etc.)?	Yes	The device can connect to Wi-Fi (this is a purchasable option)
MP11-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	The device can be remote-serviced (this is a purchasable option). During such connection an operator may access to PII.
MP11-3.8	Does the device import personally identifiable information via scanning a document?	No	
MP11-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
MP11-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	Yes	Device's information (that may or may not include PII) can be backed up and restored. Both actions require USB access and admin role.
Management of Private Data notes:			
	<b>AUTOMATIC LOGOFF (ALOF)</b>		
	<i>The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.</i>		
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	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.
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	Configurable to the following values 10 min (default), 20 min, 30min or never
	<b>AUDIT CONTROLS (AUDT)</b>		
	<i>The ability to reliably audit activity on the device.</i>		
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
AUDT-1.1	Does the audit log record a USER ID?	Yes	___
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No	Audit logs are compliant to DICOM Specific Audit Messages
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	Actor-start-stop, Begin-storing-instances, Instances-deleted PHI-export, PHI-import, Study Deleted, Study used, User Authentication Login and User Authentication Logout
AUDT-2.1	Successful login/logout attempts?	Yes	___
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	___
AUDT-2.3	Modification of user privileges?	N/A	___
AUDT-2.4	Creation/modification/deletion of users?	N/A	___
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	___
AUDT-2.6	Creation/modification/deletion of data?	Yes	___
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	___
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	___
AUDT-2.8.1	Remote or on-site support?	No	___
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	___
AUDT-2.9	Emergency access?	Yes	___
AUDT-2.10	Other events (e.g., software updates)?	No	___
AUDT-2.11	Is the audit capability documented in more detail?	No	___
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	___
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	No	___
AUDT-4.1	Does the audit log record date/time?	Yes	___
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	___
AUDT-5	Can audit log content be exported?	Yes	___
AUDT-5.1	Via physical media?	Yes	___
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	___
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No	___
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	No	___
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	No	___
AUDT-7	Are audit logs protected from modification?	Yes	___
AUDT-7.1	Are audit logs protected from access?	Yes	___
AUDT-8	Can audit logs be analyzed by the device?	No	___
	<b>AUTHORIZATION (AUTH)</b>		

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
	<i>The ability of the device to determine the authorization of users.</i>		
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	---
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	No	---
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	---
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	---
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	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.
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	No	---
AUTH-4	Does the device authorize or control all API access requests?	Yes	---
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	Yes	The user has no access to the underlying operating system
	<b>CYBER SECURITY PRODUCT UPGRADES (CSUP)</b>		
	<i>The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.</i>		
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	---
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	---
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	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	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	Configurable option
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	The Operating System is maintained by Hologic SuperSonic Imagine
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	—
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	Firmware and drivers are installed during software updates or software re-installation
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	—
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	No	—
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	—
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	—
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	All the software components (OS, OTS) are updated at once
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	see above note

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	see above note
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	---
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	---
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	---
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	---
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	---
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	---
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	Device can be configured to verify if new update are available at startup.
CSUP-8	Does the device perform automatic installation of software updates?	No	Software updates are applied upon administrator approval.
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	No third party software can be installed on the device
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	No	---
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	---
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	---
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	---
CSUP-11.2	Is there an update review cycle for the device?	Yes	At most every 2 months
	<b>HEALTH DATA DE-IDENTIFICATION (DIDT)</b>		

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
	<i>The ability of the device to directly remove information that allows identification of a person.</i>		
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	Yes	<p>For Logs: Clear logs in system config</p> <p>For non DICOM export on USB/CD/DVD:</p> <ul style="list-style-type: none"> <li>-Jpeg export of US images are anonymised (as soon as operator does not entre PHI in annotation)</li> <li>- screenshot of patient folder are not anonymised (patient name, DoB, Patient ID, accession# may be visible)</li> <li>- report are not anonymised (patient name, DoB, Patient ID, accession# may be visible)</li> </ul> <p>For printed images: no anonymisation (patient name, DoB, Patient ID, accession# are visible)</p> <p>For DICOM :</p> <p>Basic Profile, for US images being exported on DICOM Store and DICOM Media</p> <p>no anonymisation for</p> <ul style="list-style-type: none"> <li>- DICOM Print (patient name, DoB, Patient ID, accession# will be visible)</li> <li>- screenshot of patient folder are not anonymised (patient name, DoB, Patient ID, accession# may be visible)</li> <li>- report are not anonymised (patient name, DoB, Patient ID, accession# may be visible)</li> </ul>
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes	Device implement the DICOM version 2019a Basic Profile for de-identification.
	<b>DATA BACKUP AND DISASTER RECOVERY (DTBK)</b>		
	<i>The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.</i>		
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	No	—
DTBK-2	Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?	Yes	—
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	—
DTBK-4	Does the device have an integral data backup capability to remote storage?	No	—



Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes	System configuration can be backed up
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	—
<b>EMERGENCY ACCESS (EMRG)</b>			
<i>The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.</i>			
EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	Yes	—
<b>HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)</b>			
<i>How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.</i>			
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes	The mechanisms are provided by the OS
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes	The mechanisms are provided by the OS
<b>MALWARE DETECTION/PROTECTION (MLDP)</b>			
<i>The ability of the device to effectively prevent, detect and remove malicious software (malware).</i>			
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 noexec
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	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

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
MLDP-2.1	Does the device include anti-malware software by default?	No	---
MLDP-2.2	Does the device have anti-malware software available as an option?	No	---
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	No	---
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	---
MLDP-2.5	Does notification of malware detection occur in the device user interface?	N/A	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	Yes	
MLDP-2.7	Are malware notifications written to a log?	N/A	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes	
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	Yes	<p>Device has been designed to not execute any data imported on the system. only Signed software components can be installed on system.</p> <p>Hologic SuperSonic Imagine recommends the following cyber Hygiene practices:</p> <ul style="list-style-type: none"> <li>Ensure that your equipment is in a physically protected and actively monitored area;</li> <li>Ensure that only secure/sanitized USB storage devices are utilized;</li> <li>Ensure that your equipment is protected against network access by unsupervised systems (typically provided by mechanisms such as firewalls and VPNs); and</li> <li>Ensure your data has been backed up and stored according to your institution policy.</li> </ul>
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	No	---
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	No	---
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	---
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	No	---
	<b>NODE AUTHENTICATION (NAUT)</b>		
	<i>The ability of the device to authenticate communication partners/nodes.</i>		

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	Yes	DICOM TLS
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	No	reduced number of services available
NAUT-2.1	Is the firewall ruleset documented and available for review?	N/A	---
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	DICOM TLS
<b>CONNECTIVITY CAPABILITIES (CONN)</b>			
<i>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.</i>			
CONN-1	Does the device have hardware connectivity capabilities?	Yes	---
CONN-1.1	Does the device support wireless connections?	Yes	---
CONN-1.1.1	Does the device support Wi-Fi?	Yes	---
CONN-1.1.2	Does the device support Bluetooth?	No	---
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	---
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	No	---
CONN-1.2	Does the device support physical connections?	Yes	---
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	---
CONN-1.2.2	Does the device have available USB ports?	Yes	---
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	---
CONN-1.2.4	Does the device support other physical connectivity?	No	---
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	The supported network protocols are: DICOM, DHCP, NTP. HTTPS protocol may be enabled for remote maintenance.
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	The device may be connected to a PACS, to a Modality Worklist, to a printer.
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes	The device may be remotely serviceable
CONN-5	Does the device make or receive API calls?	No	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
CONN-6	Does the device require an internet connection for its intended use?	No	---
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	for DICOM connection
CONN-7.1	Is TLS configurable?	Yes	see DICOM Conformance statement and User Guide
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	---
	<b>PERSON AUTHENTICATION (PAUT)</b>		
	<i>The ability to configure the device to authenticate users.</i>		
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	4 accounts exists: emergency access, sonographer, admin and service
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	No	---
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	---
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	---
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	---
PAUT-5	Can all passwords be changed?	Yes	---
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	No	---
PAUT-7	Does the device support account passwords that expire periodically?	No	---
PAUT-8	Does the device support multi-factor authentication?	No	---
PAUT-9	Does the device support single sign-on (SSO)?	No	---
PAUT-10	Can user accounts be disabled/locked on the device?	No	---
PAUT-11	Does the device support biometric controls?	No	---
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	---
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	---
PAUT-14	Does the application or device store or manage authentication credentials?	Yes	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
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
<b>PHYSICAL LOCKS (PLOK)</b>			
	<i>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</i>		
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	No	—
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes	—
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No	disks maintaining e-PHI are crypted
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No	
<b>ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)</b>			
	<i>Manufacturer's plans for security support of third-party components within the device's life cycle.</i>		
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	IEC 62304
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	—
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	No	If remote service is enabled user can be notified when an update is available
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	At most every 2 months a service pack will be released incorporating security patch when necessary, and every year a major release with an updated version of the OS and 3rd party components will be released.
<b>SOFTWARE BILL OF MATERIALS (SBoM)</b>			

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
	<i>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.</i>		
SBOM-1	Is the SBoM for this product available?	Yes	---
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	No	---
SBOM-2.1	Are the software components identified?	Yes	---
SBOM-2.2	Are the developers/manufacturers of the software components identified?	No	---
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	---
SBOM-2.4	Are any additional descriptive elements identified?	No	---
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No	---
SBOM-4	Is there an update process for the SBoM?	No	---
	<b>SYSTEM AND APPLICATION HARDENING (SAHD)</b>		
	<i>The device's inherent resistance to cyber attacks and malware.</i>		
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	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 logging service disabled - Use of Mandatory Access Control (MAC) mechanism - Least privilege principle - Least functionality principle
SAHD-2	Has the device received any cybersecurity certifications?	No	---
SAHD-3	Does the device employ any mechanisms for software integrity checking	No	---
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	Yes	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 Hologic SuperSonic Imagine. Debian package is a tamper-evident packaging format.

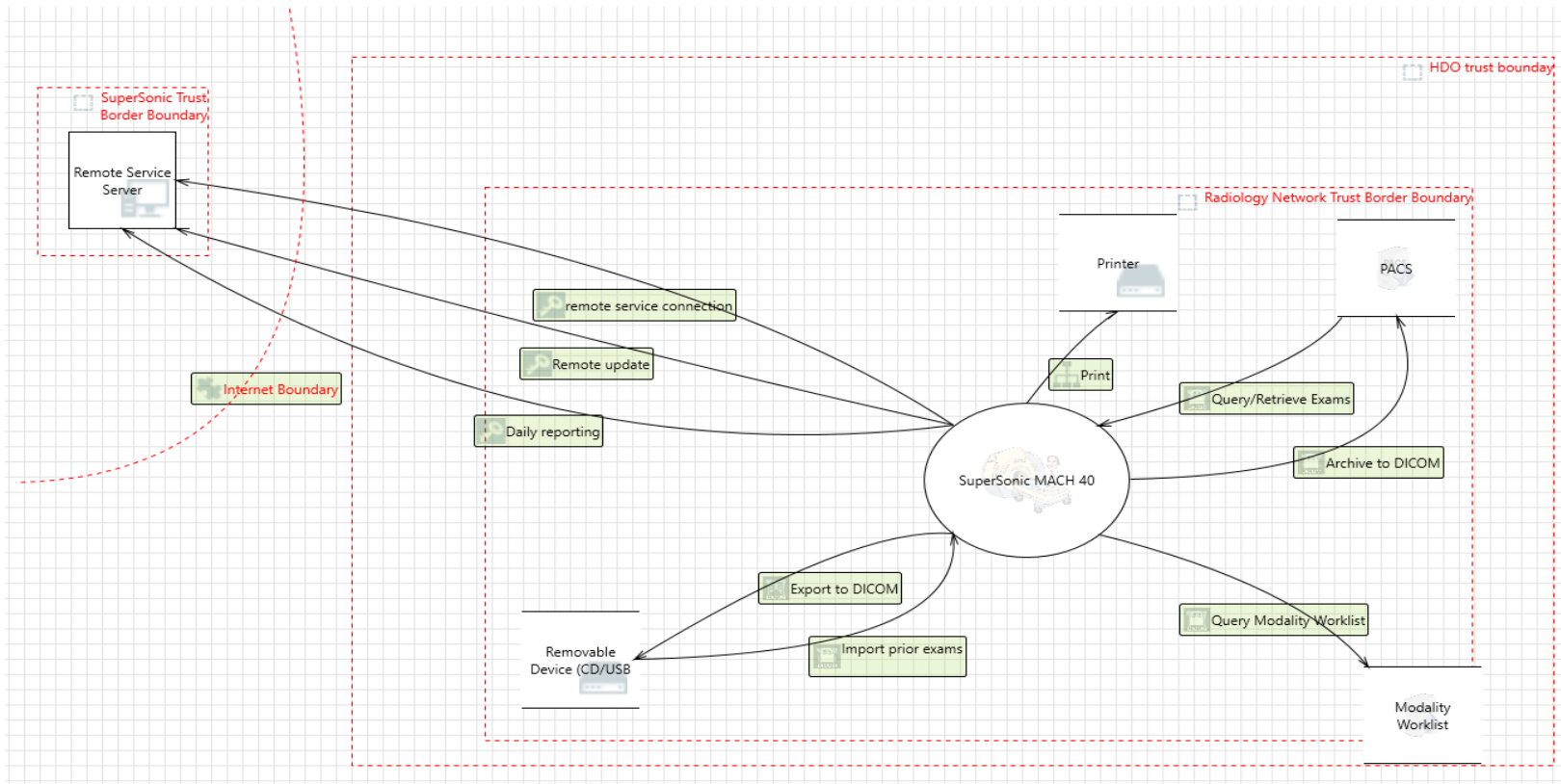
Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	All the software included in 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 Hologic SuperSonic Imagine. Debian package is a tamper-evident packaging format.
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	---
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	---
SAHD-5.1	Does the device provide role-based access controls?	Yes	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 security settings.
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	No	---
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No	Only password can be changed
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	---
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	---
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	---
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	Yes	---
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	Yes	A minimal version of the OS is installed on the device. No remote logging, no web browser or mail user agent are installed
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	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	---
SAHD-14	Can the device be hardened beyond the default provided state?	Yes	---
SAHD-14.1	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	---
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	No	---
	<b>SECURITY GUIDANCE (SGUD)</b>		
	<i>Availability of security guidance for operator and administrator of the device and manufacturer sales and service.</i>		
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	Security information are included in the User Guide
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	No	Permanent deletion of data require storage device destruction.
SGUD-3	Are all access accounts documented?	Yes	---
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	each user can change his own password, but admin can change all passwords
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	---
	<b>HEALTH DATA STORAGE CONFIDENTIALITY (STCF)</b>		
	<i>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.</i>		
STCF-1	Can the device encrypt data at rest?	Yes	e-PHI contained in database, DICOM objects, native archives and logs are stored on an encrypted partition using TPM1.2
STCF-1.1	Is all data encrypted or otherwise protected?	Yes	
STCF-1.2	Is the data encryption capability configured by default?	Yes	Encryption can't be disabled
STCF-1.3	Are instructions available to the customer to configure encryption?	No	Encryption can't be disabled or configured
STCF-2	Can the encryption keys be changed or configured?	No	The encryption keys are generated during installation. There is no way to change them



Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
STCF-3	Is the data stored in a database located on the device?	Yes	---
STCF-4	Is the data stored in a database external to the device?	No	---
<b>TRANSMISSION CONFIDENTIALITY (TXCF)</b>			
<i>The ability of the device to ensure the confidentiality of transmitted personally identifiable information.</i>			
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	---
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	No encryption on removable media. Data transmitted over the network are crypted
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	---
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	Only admin can configure network destination
TXCF-4	Are connections limited to authenticated systems?	Yes	Admin can configure the device to enforce authentication between systems
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	DICOM TLS is implemented
<b>TRANSMISSION INTEGRITY (TXIG)</b>			
<i>The ability of the device to ensure the integrity of transmitted data.</i>			
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes	DICOM TLS
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	---
<b>REMOTE SERVICE (RMOT)</b>			
<i>Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.</i>			
RMOT-1	Does the device permit remote service connections for device analysis or repair?	Yes	---
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes	---

Hologic SuperSonic imagine	SuperSonic MACH 20/30/40 V3.0	RD.REC.115	15-Nov-2020
RMOT-1.2	Is there an indicator for an enabled and active remote session?	Yes	---
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes	---
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	Yes	The device can be configured to send daily reports. Those report do not contain any e-PHI.
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes	Software update
	<b>OTHER SECURITY CONSIDERATIONS (OTHR)</b>		
	<i>NONE</i>		
	<b>Notes:</b>		
Note 1	Example note. Please keep individual notes to one cell. Please use separate notes for separate information		



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+cvcs20081104-13.2
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
TBB (libtbb2)	Intel (Open Source)	Intel® Threading Building Blocks (Intel® TBB) lets you easily write parallel C++ 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
libpam-pgsql	(Open Source)	PAM module to authenticate using a PostgreSQL database. 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
Maia	(Open Source)	Maia vectorial canvas	0.3.21-0gaussiane1
CUPS	(Open Source)	Common UNIX Printing System(tm)	2.2.1-8+ deb9u6
libopenjp2	(Open Source)	JPEG 2000 image compression/decompression library	2.1.2-1.1+deb9u5
charls	(Open Source)	Implementation of the JPEG-LS standard	1.1.0+dfsg-2
libsensors4	(Open Source)	library to read temperature/voltage/fan sensors	1:3.4.0-4
Thingworx-ssiclient	PTC	Thingworx client for SuperSonic Imagine's Aixplorers.	0.7.8-0gaussiane7 (for customer site environment) 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
pgm2d897	Sony	Sony pgm2d897 converter	0.0.3-0gaussian2
pnm2d23md	Sony	Sony pnm2d23md converter	0.0.2-0gaussian2
upd23md	Sony	Sony upd23md cups driver	1.0.10-0gaussian.2.1