Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Spacelabs Healthcare | 96280, Xhibit Telemetry Receiver (XTR) | 091-0303-08 Rev A | 12/20/2022

Question ID	Question		See note	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
DOC-1	Manufacturer Name	Spacelabs Healthcare	—			
DOC-2	Device Description	Spacelabs Healthcare Xhibit Telemetry Receiver (XTR) Ver. 1.4.2	—			
DOC-3	Device Model	96280, Xhibit Telemetry Receiver (XTR)	—			
DOC-4	Document ID	091-0303-08 Rev A	—			
DOC-5	Manufacturer Contact Information	Spacelabs Healthcare. 35301 S.E.Center Street. Snoqualmie, WA 98065	—			
DOC-6	Intended use of device in network-connected environment:	The 96280 Xhibit Telemetry Receiver (XTR) provides wireless reception for Spacelabs' patient-worn wireless telemetry transmitters. Capable of receiving and analyzing data from up to 16 patients, the telemetry receiver processes and communicates vital signs data for display on the central station. The XTR is a rack mounted device that uses the Microsoft Windows 10 IoT Enterprise Version 1809 operating system. These devices are traditionally housed in server racks that are physically locked from routine access. These devices connect to the RF antenna infrastructure, which receives data from as many as 16 Aria Tele devices for transmission via TCP/IP protocols to the central monitors or the Integration Software. The XTR has no user interface and a central monitor is used to assign a specific Aria Tele device to a specific patient so that data collected is properly associated to the patient.	—			
DOC-7	Document Release Date	Dec-22	—			
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	We publish bulletins for major vulnerabilities and threats as they emerge and we assess them. They are found on our website https://www.spacelabshealthcare.com/products/security/security-advisories-and-archives/			
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	No	—			
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	See Note 25			
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	—			
DOC-11.1	Does the SaMD contain an operating system?	N/A	—			
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	—			
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A				
DOC-11.4	Is the SaMD hosted by the customer?	N/A	—			
		Yes, No, N/A, or See Note	Note #			
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	—		AR-2	A.15.1.4
MPII-2	Does the device maintain personally identifiable information?	Yes	—		AR-2	A.15.1.4
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	—		AR-2	A.15.1.4
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	—			
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	—			
MPII-2.4	Does the device store personally identifiable information in a database?	No	—			
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	No	—		AR-2	A.15.1.4
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	—		AR-2	A.15.1.4
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	—		AR-2	A.15.1.4

MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	—			
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	Logs with PII are stored in secondary alternative drive partition		AR-2	A.15.1.4
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	—		AR-2	A.15.1.4
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	No	—		AR-2	A.15.1.4
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	No	—		AR-2	A.15.1.4
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	No	—		AR-2	A.15.1.4
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire,	No	—		AR-2	A.15.1.4
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	—		AR-2	A.15.1.4
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	No			AR-2	A.15.1.4
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	—		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?	Yes	—			
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	N/A	—		AR-2	A.15.1.4
Management of Private Data notes:					AR-2	A.15.1.4

	AUTOMATIC LOGOFF (ALOF)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.					
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	N/A	Note 1	Section 5.1, ALOF	AC-12	None
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	N/A	—	Section 5.1, ALOF	AC-11	A.11.2.8, A.11.2.9

	AUDIT CONTROLS (AUDT)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability to reliably audit activity on the device.					
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	—	Section 5.2, AUDT	AU-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AUDT-1.1	Does the audit log record a USER ID?	Yes	Note 32			
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	Note 2	Section 5.2, AUDT	AU-2	None
AUDT-2.1	Successful login/logout attempts?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.3	Modification of user privileges?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.4	Creation/modification/deletion of users?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.5	Presentation of clinical or PII data (e.g. display,	N/A	Note 1	Section 5.2, AUDT	AU-2	None
AUDT-2.6	Creation/modification/deletion of data?	Yes	—	Section 5.2, AUDT	AU-2	None

AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	N/A	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8.1	Remote or on-site support?	Yes	Note 3	Section 5.2, AUDT	AU-2	None
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-2.9	Emergency access?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-2.10	Other events (e.g., software updates)?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-2.11	Is the audit capability documented in more detail?	Yes	Note 4	Section 5.2, AUDT	AU-2	None
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-4.1	Does the audit log record date/time?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-4.1.1	Can date and time be synchronized by Network Time 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?	No	—			
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	—			
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	Yes	Note 5			
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	—	Section 5.2, AUDT	AU-2	None
AUDT-7.1	Are audit logs protected from access?	Yes				
AUDT-8	Can audit logs be analyzed by the device?	No	—	Section 5.2, AUDT	AU-2	None

	AUTHORIZATION (AUTH)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to determine the authorization of users.					
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	N/A	Note 1	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	N/A	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	N/A	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.3	Are any special groups, organizational units, or group policies required?	N/A	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	No	—	Section 5.3, AUTH	IA-2	A.9.2.1
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	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-4	Does the device authorize or control all API access requests?	No	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	No	—			

	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 device's security patches.					
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	Note 6			
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	Note 7			

CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	—
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	—
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	—
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—
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?	No	—
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—
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?	No	—
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	—
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	—
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	No	—
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	—
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	—
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	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?	N/A	—
CSUP-8	Does the device perform automatic installation of software updates?	N/A	—
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	N/A	—

CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	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	Note 26			
CSUP-11.2	Is there an update review cycle for the device?	Yes	Note 27			
	HEALTH DATA DE-IDENTIFICATION (DIDT)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to directly remove information that allows identification of a person.					
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	No	—	Section 5.6, DIDT	None	ISO 27038
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	No	—	Section 5.6, DIDT	None	ISO 27038
	DATA BACKUP AND DISASTER RECOVERY (DTBK)			**IEC TR 80001-2-2:2012**	**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.					
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?	No	—	Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-3	Does the device have an integral data backup capability to removable media?	No	—	Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-4	Does the device have an integral data backup capability to remote storage?	No	—			
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	No	—			
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	—	Section 5.7, DTBK	CP-9	A.12.3.1
	EMERGENCY ACCESS (EMRG)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.					
EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	No	—	Section 5.8, EMRG	SI-17	None
	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.					
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No	—	Section 5.9, IGAU	SC-28	A.18.1.3
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	—	Section 5.9, IGAU	SC-28	A.18.1.3
	MALWARE DETECTION/PROTECTION (MLDP)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to effectively prevent, detect and remove malicious software (malware).					
MLDP-1	Is the device capable of hosting executable software?	Yes	Note 8	Section 5.10, MLDP		

	Does the device support the use of anti-malware software (or other anti-malware mechanism)?					
MLDP-2	Provide details or reference in notes.	No	—	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-2.1	Does the device include anti-malware software by default?	N/A	—	Section 5.10, MLDP	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
MLDP-2.2	Does the device have anti-malware software available as an option?	N/A	—	Section 5.10, MLDP	AU-6	A.12.4.1, A.16.1.2, A.16.1.4
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	N/A	—	Section 5.10, MLDP	CP-10	A.17.1.2
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	N/A	—	Section 5.10, MLDP	AU-2	None
MLDP-2.5	Does notification of malware detection occur in the device user interface?	N/A	—			
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	N/A	—			
MLDP-2.7	Are malware notifications written to a log?	N/A	—			
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	N/A	—			
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	Note 9	Section 5.10, MLDP	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	Yes	—	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	No	Note 10	Section 5.10, MLDP	SI-4	None
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	No	—	Section 5.10, MLDP	CM-7	A.12.5.1
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	No	—	Section 5.10, MLDP		

	NODE AUTHENTICATION (NAUT)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to authenticate communication partners/nodes.					
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	No	—	Section 5.11, NAUT	SC-23	None
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	Yes	—	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	Is the firewall ruleset documented and available for review?	No				
NAUT-3	Does the device use certificate-based network connection authentication?	No	—			

	CONNECTIVITY CAPABILITIES (CONN)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.					
CONN-1	Does the device have hardware connectivity capabilities?	Yes	—			
CONN-1.1	Does the device support wireless connections?	Yes	—			
CONN-1.1.1	Does the device support Wi-Fi?	No	—			
CONN-1.1.2	Does the device support Bluetooth?	No	—			
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	—			
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	Yes	Note 12			
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	Note 13			
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?	No	—			
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	Note 14			
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	—			
CONN-5	Does the device make or receive API calls?	No	—			
CONN-6	Does the device require an internet connection for its intended use?	No	—			
CONN-7	Does the device support Transport Layer Security (TLS)?	No	—			
CONN-7.1	Is TLS configurable?	N/A	—			
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	—			
	PERSON AUTHENTICATION (PAUT)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability to configure the device to authenticate users.					
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	No	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	N/A	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS 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?	N/A	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	N/A	Note 28	Section 5.12, PAUT	SA-4(5)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
PAUT-5	Can all passwords be changed?	N/A	—	Section 5.12, PAUT		
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	N/A	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-7	Does the device support account passwords that expire periodically?	N/A	—			
PAUT-8	Does the device support multi-factor authentication?	No	—			
PAUT-9	Does the device support single sign-on (SSO)?	N/A	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-10	Can user accounts be disabled/locked on the device?	No	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-11	Does the device support biometric controls?	No	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	—			
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	—			
PAUT-14	Does the application or device store or manage authentication credentials?	No	—			
PAUT-14.1	Are credentials stored using a secure method?	N/A	—			
	PHYSICAL LOCKS (PLOK)			**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.	No	—	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes	—	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No		Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3

PLOK-4	Does the device have an option for the customer to 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)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	Manufacturer's plans for security support of third-party components within the device's life cycle.					
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	Note 15	Section 5.14, RDMP	CM-2	None
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	—	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	No	—	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?	Yes	Note 16	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
	SOFTWARE BILL OF MATERIALS (SBoM)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.					
SBOM-1	Is the SBoM for this product available?	Yes	Appendix 1			
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	Note 17			
SBOM-2.1	Are the software components identified?	Yes	—			
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	—			
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	—			
SBOM-2.4	Are any additional descriptive elements identified?	No	—			
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No	Note 30			
SBOM-4	Is there an update process for the SBoM?	Yes	Note 18			
	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 malware.					
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	Note 19	Section 5.15, SAHD	CM-7 AC-17(2)/IA-3	A.12.5.1* A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/None
SAHD-2	Has the device received any cybersecurity certifications?	No		Section 5.15, SAHD	SA-12(10)	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	Note 8			
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?	No	—			
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?	No	—	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	—	Section 5.15, SAHD	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-5.1	Does the device provide role-based access controls?	N/A	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes	Note 20	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No	—	Section 5.15, SAHD	CM-7	A.12.5.1*

SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	N/A	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	Note 13	Section 5.15, SAHD	SA-18	None
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	Note 33	Section 5.15, SAHD	CM-6	None
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	Note 34	Section 5.15, SAHD	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
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	Note 21			
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	—			
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No				
SAHD-14	Can the device be hardened beyond the default provided state?	No	—			
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A	—			
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes	Note22			
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	No	—			

	SECURITY GUIDANCE (SGUD)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.					
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	Note 23	Section 5.16, SGUD	AT-2/PL-2	A.7.2.2, A.12.2.1/A.14.1.1
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes	Note 31	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?	N/A	—	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	Can the owner/operator manage password control for all accounts?	No	—			
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	Note 29			

	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.					
STCF-1	Can the device encrypt data at rest?	No	—	Section 5.17, STCF	SC-28	A.8.2.3
STCF-1.1	Is all data encrypted or otherwise protected?	N/A	—			
STCF-1.2	Is the data encryption capability configured by default?	N/A	—			
STCF-1.3	Are instructions available to the customer to configure encryption?	N/A	—			
STCF-2	Can the encryption keys be changed or configured?	N/A	—	Section 5.17, STCF	SC-28	A.8.2.3
STCF-3	Is the data stored in a database located on the device?	No	—			
STCF-4	Is the data stored in a database external to the device?	N/A	—			

	TRANSMISSION CONFIDENTIALITY (TXCF)	**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**

	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.					
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	No	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	N/A	—			
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	No	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-4	Are connections limited to authenticated systems?	No	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	No	—			

	TRANSMISSION INTEGRITY (TXIG)			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	The ability of the device to ensure the integrity of transmitted data.					
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	No	—	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
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	—			

	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	Note 24		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?	No	—			
RMOT-1.2	Is there an indicator for an enabled and active remote session?	No	—			
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes	—		AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No	—			
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote	No	—			

	OTHER SECURITY CONSIDERATIONS (OTHR)	**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
	NONE			

Notes:

Note 1	The XTR has no user interface. A Central Monitor is used to assign a specific Aria Tele device to a specific patient so that data collected is properly associated to the patient.
Note 2	The XTR device logs all requests made by the monitoring client software. Such request include patient admit, patient discharge, modification of patient data, and patient transfer.
Note 3	The XTR maintains on-site support
Note 4	Audit, code and windows event logs can be configured to make available. LogStash configuration document 070-2946-00 contains the details.
Note 5	The audit logs can be downloaded via using Service tool
Note 6	Outstanding patches are incorporated in product software updates. These updates are applied by Spacelabs approved Field Service Engineers for customers with service contracts.
Note 7	Windows 10 IoT Enterprise Version 1809

Note 8	Windows AppLocker is configured to control executable files and scripts (whitelisting)
Note 9	XTR uses Unified Write Filter and AppLocker as a compensating controls instead of anti-malware software
Note 10	Windows Event Viewer is used for analysis of event logs.
Note 12	RF controls is used for wireless connections
Note 13	There is a device firewall that closes all but essential communication ports. Auto Launch has been disabled for USB devices, and the USB ports are covered by a plate. Network discovery and file/printer sharing is disabled.
Note 14	The system is intended to provide the SpaceLabs Healthcare monitoring system with adult, pediatric and neonatal patient data
Note 15	The software development process is performed according to IEC 62304. It is documented in 808-0120-05 Software Development Plan 96280 Xhibit Telemetry Receiver (XTR) 1.4.0, Rev A
Note 16	List of third-party components and configuration management rules are defined in 808-0120-05 Software Development Plan 96280 Xhibit Telemetry Receiver (XTR) 1.4.0, Rev A
Note 17	Software components are defined and described in 806-0103-00 XTR Software Architecture, Rev D
Note 18	This is tracked in the software development plan document.
Note 19	The system only includes essential Windows components that are required for operation. There is a device firewall that closes all but essential communication ports. Auto Launch has been disabled for USB devices, and the USB ports are covered by a plate. Network discovery and file/printer sharing is disabled.
Note 20	We have administrator account only used during system installation. Password is generated randomly and does not kept anywhere
Note 21	After using tools to gain access to the USB port, product updates are performed by authorized service staff. Service staff receive product updates from a trusted source and only use authenticated updates they have received through official channels. The device is configured to disable AutoPlay on all inserted USB media.
Note 22	BIOS password is used to prevent from booting alternative operating systems on removable devices or prevent from installation another operating system over current operating system
Note 23	The information is provided in Service Manual (96280) 070-2409-03 and Operator Manual (96280) 070-2114-06; Product Service Notice (96280); Security Operations Guide 070-2926-00
Note 24	Authorized Spacelabs service staff can use a remote tool to configure elements of the product.
Note 25	We have network diagrams of our PMC suite with XTR as part of those models. This is not published and can be made available on request.
Note 26	XTR is a closed appliance product, and any updates to it are managed via Spacelabs product release process
Note 27	For products using off-the-shelf Windows operating system like Windows Server 2016, patch testing is performed monthly. For other products such as XTR, reviews are part of the product update development process.
Note 28	The default admin account is documented in the product Security Operations Guide 070-2926-00
Note 29	Refer to the product Security Operations Guide 070-2926-00

Note 30	The device is configurable using the ET Service Tool, explained in the product Service Manual p/n 070-2409-03
Note 31	The Service Manual p/n 070-2409-03 has instructions on how to use the ET Service Tool that has a Reset Receiver Menu and explanation on how to permanently reset data. For Software reimaging the instructions are included in the PSN.
Note 32	XTRs ID are reflected in audit logs, so user's ID may be defined using the information
Note 33	Note 33 - Most of common services, not required by XTR, are disabled using Windows Features. Other services that are not needed were set to disabled but some services were left as is as they are needed by other Microsoft components and can impact system health if they are disabled.
Note 34	Other Windows features except Unbranded boot, UWF and PowerShell 2.0 are disabled. Applications such as calc.exe, notepad.exe, SnippingTools.exe are added to AppLocker blocking rules.