Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

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	Sentinel Cardiology Information Management System. Version 11.6	__			
DOC-3	Device Model	98201	__			
DOC-4	Document ID	091-0440-00 Rev A	__			
DOC-5	Manufacturer Contact Information	Spacelabs Healtcare, 35301 SE Center Street, Snoqualmie, WA 98065	__			
DOC-6	Intended use of device in network-connected environment:	Sentinel is a software product. The application runs on client PCs in network topologies. The intended use sentinel stores the data from the spacelabs diagnostic cardiology products such as patient-worn Spacelabs ABP, ECG and Holter monitors, Spacelabs analysis software such as Pathfinder SL and Lifescreen PRO.	__			
DOC-7	Document Release Date	Jul-24	__			
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	__			
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	We have network diagrams of our DC suite with Sentinel as part of those models. This is not published and can be made available on request.			
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	Yes	__			
DOC-11.1	Does the SaMD contain an operating system?	No	This is a Windows application requiring a Windows Operating System to function.			
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	Yes	Supported Operating Systems include Microsoft Windows 10 and 11 and Server 2019 and Windows Server 2022			
DOC-11.3	Is the SaMD hosted by the manufacturer?	No	__			
DOC-11.4	Is the SaMD hosted by the customer?	Yes	__			

		Yes, No, N/A, or See Note	Note #	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION					
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	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?	No	__			
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	No	__			

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

MPII-2.4	Does the device store personally identifiable information in a database?	Yes	__	AR-2	A.15.1.4
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)?	N/A	__		
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	Yes	__	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?	Yes	__	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.)?	Yes	Sentinel has ability to store files to file system folders (potentially on removable media) is restricted by security role permissions.	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, etc.)?	Yes	Sentinel can be configured to send PII to Ambulatory ECG and ABP devices but it does not need to and Spacelabs recommends that this not be done.	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	Sentinel does not require Internet to function. However, the customer has the option to implement Sentinel's Remote Data Transfer (RDT) feature where an internet connection may be required.	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	If the customer is using RDT that would receive PII in SNTL files transferred over HTTPS. SNTL is a Spacelabs file format. SNTL files are encrypted.	AR-2	A.15.1.4
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	__	AR-2	A.15.1.4

Management of Private Data notes:

Spacelabs Healthcare | 98201 | 091-0440-00 Rev A | Oct-24

	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.*			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
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	__	Section 5.1, ALOF	AC-12	None
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	__	Section 5.1, ALOF	AC-11	A.11.2.8, A.11.2.9

	AUDIT CONTROLS (AUDT) *The ability to reliably audit activity on the device.*			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	Sentinel generates audit records containing information which establishes what type of event occurred, when the event occurred, the identity of individuals or subjects associated with the event.	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	__	Section 5.2, AUDT	AU-2	None
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	The description field in the audit trail indicates the patient name.	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	__	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	Any auditing of the staff records is audited.	Section 5.2, AUDT	AU-2	None
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	If a user reviews clinical data that's audited. If they begin editing records but do not complete the edit (and hence see the data e.g. patient data) that's audited. Print from the review web page is not audited because that is done via Adobe Acrobat not Sentinel.	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)?	Yes	__	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?	No	__	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?	See Notes	Sentinel does not provide emergency access	Section 5.2, AUDT	AU-2	None
AUDT-2.10	Other events (e.g., software updates)?	N/A	__	Section 5.2, AUDT	AU-2	None
AUDT-2.11	Is the audit capability documented in more detail?	N/A	Sentinel generates audit records containing information which establishes what type of event occurred, when the event occurred, the identity of individuals or subjects associated with the event.	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

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

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?	Yes	Administrators can view the audit trail in the Sentinel user interface.			
AUDT-7	Are audit logs protected from modification?	Yes	System administrators can delete the whole audit trail but no user can modify any audit entries.	Section 5.2, AUDT	AU-2	None
AUDT-7.1	Are audit logs protected from access?	Yes	Stored in the database with all protection at rest and in transit that implies.			
AUDT-8	Can audit logs be analyzed by the device?	No	__	Section 5.2, AUDT	AU-2	None

	AUTHORIZATION (AUTH) *The ability of the device to determine the authorization of users.*			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	__	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)?	Yes	__	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)?	Yes	__	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.3	Are any special groups, organizational units, or group policies required?	Yes	__	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.)?	Yes	Sentinel has security roles which can be defined by the customer to indicate which kinds of users have permission to perform which Sentinel functions. It also have mandatory filters in these roles which define which records these kinds of users are permitted to access (e.g. only patients in the ward where the user works).	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)?	Yes	Only if the operator has operating system permissions to do so	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-4	Does the device authorize or control all API access requests?	No	HL7 and DICOM does not support authentication.	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?	N/A	__			

	CYBER SECURITY PRODUCT UPGRADES (CSUP) *The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.*			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
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	__			

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	No	Sentinel is a software product. It is the customers responsibility to provide the physical PC or server on which it runs.
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	—
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	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.	No	—
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	—
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	It is the responsibility of the customer to run anti-malware software on their servers and clients
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?	No	—
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	It is the responsibility of the customer to install operating system and SQL Server updates on their servers and clients
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	—
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	—

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	__			
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	Yes	Sentinel does manage the software licences for Sentinel, Pathfinder SL and Lifescreen PRO.			
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__			
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	__			
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	No	__			
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?	Yes	It is the responsibility of the customer to install update on their servers and clients			
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	__			
CSUP-8	Does the device perform automatic installation of software updates?	No	__			
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	__			
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	No	Sentinel is a software product installed in a customer's PC/VM and It is the customer's responsibility to install or not third-party software in PC/VM.			
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	No	Sentinel is a software product installed in a customer's PC/VM and It is the customer's responsibility to install or not third-party software in PC/VM.			
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	__			
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	__			
CSUP-11.2	Is there an update review cycle for the device?	No	__			

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	HEALTH DATA DE-IDENTIFICATION (DIDT) *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?	Yes	The customer has the ability to edit patient and staff records and remove PII	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

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	DATA BACKUP AND DISASTER RECOVERY (DTBK) *The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.*					

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	Yes	__			
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?	Yes	__	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?	Yes	__			
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)

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.

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
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)

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.

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
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)?	Yes	The customer could set up RAID disks if they wish. That would be transparent to the Sentinel software.	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		Section 5.10, MLDP		
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	Please refer exclusions from real time antivirus scanning document :077-0255-00 Rev G	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-2.1	Does the device include anti-malware software by default?	No	__	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?	No	__	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?	Yes	__	Section 5.10, MLDP	CP-10	A.17.1.2
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	Yes	__	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?	N/A	—	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?	N/A	—	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	N/A	—	Section 5.10, MLDP	SI-4	None
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	—	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?	N/A	—	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**
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)?	No	Sentinel is just software that resides in the customer's network. It doesn't provide whitelisting etc of itself. The operating system, IIS, and the customer network do that.	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?	Yes	Sentinel supports HTTPS			

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	Sentinel have capabilites of connecting with hardware device like Eclispe Pro, Eclipse Mini, Ontrak and more.			
CONN-1.1	Does the device support wireless connections?	Yes	While Sentinel does not explicitly have wireless capabilities. Customers can use it in a wireless network . Sentinel sits in the customer's network.			

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

CONN-1.1.1	Does the device support Wi-Fi?	Yes	While Sentinel does not explicitly have wireless capabilities. Customers can use it in a wireless network . Sentinel sits in the customer's network.
CONN-1.1.2	Does the device support Bluetooth?	N/A	__
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?	N/A	__
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	N/A	__
CONN-1.2.2	Does the device have available USB ports?	Yes	Depends if the PC on which Sentinel is installed has USB ports.
CONN-1.2.3	Does the device require, use, or support removable memory devices?	No	__
CONN-1.2.4	Does the device support other physical connectivity?	Yes	__
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	N/A	Sentinel is a software product that will be hosted on customer hardware. Spacelabs can provide the necessary ports and protocols for customers to configure.
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	EMRs through HL7, PACS though DICOM, other systems through file drops and HTTP/HTTPS
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?	N/A	__
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	__
CONN-7.1	Is TLS configurable?	No	This is a software application. TLS configurations are applied at the OS layer.
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	__

	PERSON AUTHENTICATION (PAUT) *The ability to configure the device to authenticate users.*			**IEC TR 80001-2-2:2012**	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	__	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)?	Yes	__	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.)?	Yes	__	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?	Yes	__	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?	Yes	__	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?	Yes	__	Section 5.12, PAUT		

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-7	Does the device support account passwords that expire periodically?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-8	Does the device support multi-factor authentication?	Yes	Multifactor authentication can configurable through active directory as well as directly in the product	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-9	Does the device support single sign-on (SSO)?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-11	Does the device support biometric controls?	Yes	Using Active Directory and single sign on customers can use all biometric and other controls supported by Active Directory.	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-12	Does the device support physical tokens (e.g. badge access)?	N/A	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-14	Does the application or device store or manage authentication credentials?	Yes	Only for non-Active Directory users. For Active Directory the authentication credentials are stored in Active Directory.	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-14.1	Are credentials stored using a secure method?	Yes	Non-Active Directory users credentials are stored in the database and even then are further encrypted.	Section 5.12, PAUT	IA-2	A.9.2.1

PHYSICAL LOCKS (PLOK)

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

				IEC TR 80001-2-2:2012	**NIST SP 800-53 Rev. 4**	**ISO 27002:2013**
PLOK-1	Is the device software only? If yes, answer “N/A” to remaining questions in this section.	Yes	—	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)?	N/A	—	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?	N/A	—	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?	N/A	—	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?	Yes	—	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

Spacelabs Healthcare | 98201 | 091-0440-00 Rev A | Oct-24

RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	__	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	The list of third-party software is defined in the products "Software Bill of Materials".	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	Is the SBoM for this product available?	Yes	__			
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	__			
SBOM-2.1	Are the software components identified?	Yes	__			
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	__			
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	__			
SBOM-2.4	Are any additional descriptive elements identified?	N/A	__			
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	Yes	__			
SBOM-4	Is there an update process for the SBoM?	Yes	__			

SYSTEM AND APPLICATION HARDENING (SAHD)

The device's inherent resistance to cyber attacks and malware.

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
SAHD-1	Is the device hardened in accordance with any industry standards?	N/A	Sentinel is dependent on the controls and system hardening of the underlying Windows operating system.		CM-7	A.12.5.1*
SAHD-2	Has the device received any cybersecurity certifications?	No	__	Section 5.15, SAHD	AC-17(2)/IA-3	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/None
SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	__	Section 5.15, SAHD	SA-12(10)	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	Yes	__			
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	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?	Yes	Mandatory filters ensure that users only see the patient and test records they are authorized to see (e.g. only the patients in the ward where a nurse works). These controls are customer administrator configurable.	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-5.1	Does the device provide role-based access controls?	Yes	Sentinel has security roles. All users must belong to one or more of these roles. They restrict what product functions a user can perform and what records a user can access.	Section 5.15, SAHD	CM-7	A.12.5.1*

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	N/A	—	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?	Yes	The system administrator account (username: admin) is the only account shipped at system delivery. All other user accounts are configured by the customer thereafter (or automatically configured by Active Directory)	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?	Yes	There are no service technician accounts. Only the system admin account is delivered.	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?	No	Customer can disable these shared resources on the host.	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	Sentinel is a software product. Spacelabs can provide the necessary ports and protocols for customers to configure.	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?	No	The installer does not disable or delete services or ports on the PC/VM on which it is installed.	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?	No	The installer does not delete any applications from the PC/VM on which it is installed.	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)?	No	—			
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	N/A	—			
SAHD-13	Does the product documentation include information on operational network security scanning by users?	N/A	—			
SAHD-14	Can the device be hardened beyond the default provided state?	N/A	—			
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A	—			
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	N/A	—			
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	N/A	—			

	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?	Yes	The administrator manual provides the owner/operator with security documentation.	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	The operator manual provides the user how to delete patient, test and case records. The admin manual provides the administrator how to delete other records.	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?	No	The operating system accounts are the responsibility of the customer. On installation the only softeware login account is the system admin account. Customers are recommended to create additional software login accounts for clinical and administration use.	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

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	__			
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	No	__			

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
STCF-1	Can the device encrypt data at rest?	Yes	Sentinel uses Microsoft Transparent Data Encryption to protect database data at rest	Section 5.17, STCF	SC-28	A.8.2.3
STCF-1.1	Is all data encrypted or otherwise protected?	Yes	__			
STCF-1.2	Is the data encryption capability configured by default?	Yes	__			
STCF-1.3	Are instructions available to the customer to configure encryption?	No	Spacelabs can provide assistance to configure encryption.			
STCF-2	Can the encryption keys be changed or configured?	Yes	__	Section 5.17, STCF	SC-28	A.8.2.3
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?	Yes	__			

TRANSMISSION CONFIDENTIALITY (TXCF)

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

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	Yes	__	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?	Yes	__	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?	Yes	In v11.6 only HTTPS if HTTPS option ticked in the installer.			
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	See Notes	Sentinel is a software product. It is recommended that customers follow the Spacelabs networking deployment guide.	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-4	Are connections limited to authenticated systems?	See Notes	Sentinel is a software product. It is recommended that customers follow the Spacelabs networking deployment guide.			
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	No	__	Section 5.18, TXCF	CM-7	A.12.5.1

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?	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?	N/A	__			

Spacelabs Healthcare 98201 091-0440-00 Rev A Oct-24

	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?	No	Host server and customer controls can facilitate remote access.		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?	N/A	__			
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	If the customer were to allow remote control of the PC and it were logged into Sentinel.		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 training)?	N/A	__			