Manufacturer Disclosure Statement for Medical Device Security -- MDS2

| 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 | Lifescreen PRO Ambulatory ECG | _ | | | |
| | | Version 1.1.2 | | | | |
| | | | | | | |
| DOC-3 | Device Model | 98800 | | | | |
| DOC-4 | Document ID | 091-0441-00 Rev A | _ | | | |
| DOC-5 | Manufacturer Contact Information | Spacelabs Healtcare, | <u> </u> | | | |
| 1000 3 | ividinal declarer contact information | 35301 SE Center Street, | | | | |
| | | Snoqualmie, WA 98065 | | | | |
| DOC-6 | Intended use of device in network-connected | The Lifescreen PRO Ambulatory ECG | | | | |
| | environment: | Analyser is a software product. The | | | | |
| | | application runs as a single process | | | | |
| | | on client PCs in Sentinel network | | | | |
| | | topologies. The intended use is to | | | | |
| | | analyse recorded ECG stored in | | | | |
| | | Sentinel to produce a report for a | | | | |
| | | clinician. the output report can be | | | | |
| | | stored in Sentinel or sent to a | | | | |
| | | printer. | | | | |
| | | Lifescreen PRO can be used as a | | | | |
| | | triage tool for assessment of | | | | |
| | | ambulatory ECG from supported | | | | |
| | | devices; supporting selection and | | | | |
| | | export of ECG segments for more | | | | |
| | | detailed analysis in the Spacelabs | | | | |
| | | Pathfinder SL Analyser product. | | | | |
| | | , , , , , , , , , , , , , , , , , , , | | | | |
| DOC-7 | Document Release Date | TBC-24 | | | | |
| DOC-8 | Coordinated Vulnerability Disclosure: Does the | Yes | _ | | | |
| | manufacturer have a vulnerability disclosure program | | | | | |
| | for this device? | | | | | |
| DOC-9 | ISAO: Is the manufacturer part of an Information | No | _ | | | |
| | Sharing and Analysis Organization? | | | | | |
| | | | | | | |
| DOC-10 | Diagram: Is a network or data flow diagram available | Yes | We have network diagrams of our DC suite with | | | |
| | that indicates connections to other system | | Lifescreen PRO as part of those models. This is not | | | |
| | components or expected external resources? | | published and can be made available on request. | | | |
| | | | | | | |
| DOC-11 | SaMD: Is the device Software as a Medical Device (i.e. | Yes | _ | | | |
| DOC-11.1 | software-only, no hardware)? Does the SaMD contain an operating system? | No | | | | |
| DOC-11.1 | Does the SaMD rely on an owner/operator provided | Yes | | | | |
| DOC-11.2 | operating system? | res | _ | | | |
| DOC 44.3 | | NI | | | | |
| DOC-11.3 | Is the SaMD hosted by the manufacturer? | No | | | | |
| DOC 11 4 | lethe CaMD heated by the costones? | V | | | | |
| DOC-11.4 | Is the SaMD hosted by the customer? | Yes | _ | | | |
| | | Voc No | | | | |
| | | Yes, No, | | | | |
| | | N/A, or See Note | Note # | | | |
| | MANAGEMENT OF PERSONALLY IDENTIFIABLE | See NOTE | NOTE # | | | |
| | INFORMATION | | | IEC TD 90001 2 2:2012 | NICT CD OOD E2 Dog 4 | ISO 27002:2013 |
| F | INFORIVIATION | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | 130 2/002:2013 |
| | Con this device discuss the result of the control of | | | | | |
| | Can this device display, transmit, store, or modify | | | | | |
| MDII 1 | personally identifiable information (e.g. electronic | Vos | | | AD 2 | A 1 F 1 A |
| MPII-1 | Protected Health Information (ePHI))? | Yes | _ | 1 | AR-2 | A.15.1.4 |

Spacelabs Healthcare 98800 091-0441-00 Rev A Oct-24

| | Does the device maintain personally identifiable | | |
|-------------|---|-----|---|
| MPII-2 | information? | Yes | |
| | | | Lifescreen PRO stores temporary information within |
| | Does the device maintain personally identifiable | | the volatile memory of the supporting PC. If power is |
| | information temporarily in volatile memory (i.e., until | | lost, newly entered data |
| MPII-2.1 | cleared by power-off or reset)? | Yes | MAY be lost. |
| | Does the device store personally identifiable | | |
| MPII-2.2 | information persistently on internal media? | No | |
| 1411 11 2.2 | information persistently on internal internal. | 110 | - |
| | Is personally identifiable information preserved in the | | |
| MPII-2.3 | device's non-volatile memory until explicitly erased? | No | |
| IVIF II-2.3 | Does the device store personally identifiable | NO | _ |
| MPII-2.4 | information in a database? | No | |
| IVIPII-2.4 | information in a database? | No | _ |
| | December devices allow as offer matical to extensive like | | |
| | Does the device allow configuration to automatically | | |
| | delete local personally identifiable information after it | | |
| MPII-2.5 | is stored to a long term solution? | N/A | _ |
| | | | |
| | Does the device import/export personally identifiable | | |
| | information with other systems (e.g., a wearable | | |
| | monitoring device might export personally | | |
| MPII-2.6 | identifiable information to a server)? | Yes | _ |
| | Does the device maintain personally identifiable | | |
| | information when powered off, or during power | | |
| MPII-2.7 | service interruptions? | No | _ |
| | Does the device allow the internal media to be | | |
| | removed by a service technician (e.g., for separate | | |
| MPII-2.8 | destruction or customer retention)? | N/A | |
| | 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 | | |
| MPII-2.9 | storage location)? | No | |
| | Does the device have mechanisms used for the | | |
| MPII-3 | | Yes | |
| | transmitting, importing/exporting of personally | | |
| | identifiable information? | | |
| NADU 2 4 | Does the device display personally identifiable | V | |
| MPII-3.1 | information (e.g., video display, etc.)? | Yes | - |
| | | | |
| | Does the device generate hardcopy reports or images | | |
| MPII-3.2 | containing personally identifiable information? | Yes | _ |
| | | | |
| | 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 | | |
| MPII-3.3 | card, memory stick, etc.)? | No | _ |
| | Does the device transmit/receive or import/export | | |
| | personally identifiable information via dedicated | | |
| | cable connection (e.g., RS-232, RS-423, USB, FireWire, | | |
| MPII-3.4 | etc.)? | No | |
| | Does the device transmit/receive personally | | _ |
| | identifiable information via a wired network | | Only when sending a report to a local/networked |
| MPII-3.5 | connection (e.g., RJ45, fiber optic, etc.)? | Yes | printer. |
| IVIFII-3.3 | Does the device transmit/receive personally | les | printer. |
| | identifiable information via a wireless network | | |
| | | | |
| A ADU C. C | connection (e.g., WiFi, Bluetooth, NFC, infrared, | | |
| MPII-3.6 | cellular, etc.)? | No | _ |
| | Does the device transmit/receive personally | | |
| | identifiable information over an external network | | |
| MPII-3.7 | (e.g., Internet)? | No | _ |
| | | | |
| | Does the device import personally identifiable information via scanning a document? | | |

A.15.1.4

AR-2

| Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 | | | |
|------------------------|---|-------------------|---|-------------------------------------|-----------------------|------------------------------|
| MPII-3.9 | Does the device transmit/receive personally identifiable information via a proprietary protocol? Does the device use any other mechanism to transmit, import or export personally identifiable | No | | | | |
| MPII-3.10 | | No | | | AR-2 | A.15.1.4 |
| Management of Private | Data notes: | | | | AR-2 | A.15.1.4 |
| | 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)? | No | | Section 5.1, ALOF | AC-12 | None |
| 7.001 1 | Is the length of inactivity time before auto- | | | 323.01.3.1,7.123. | 7.6 12 | e |
| ALOF-2 | 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. | | | | | |
| | | | All Audit logging is performed by Sentinel. Lifescreen PRO CAN ONLY be installed on either a Sentinel Client or a Sentinel Workstation. Lifescreen PRO has no audit logging, but Sentinel will audit the | | | |
| | Can the medical device create additional audit logs or | | use of Lifescreen PRO for each recording that is | Couling E.S. AUDT | A11.4 | A.5.1.1, A.5.1.2, A.6.1.1, |
| AUDT-1 AUDT-1.1 | reports beyond standard operating system logs? Does the audit log record a USER ID? | No No | analysed. | Section 5.2, AUDT | AU-1 | A.12.1.1, A.18.1.1, A.18.2.2 |
| 7.007 1.1 | Does other personally identifiable information exist in | | _ | | | |
| AUDT-1.2 | the audit trail? Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-2 | audit log: | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.1 | Successful login/logout attempts? | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.2 | Unsuccessful login/logout attempts? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.3 | Modification of user privileges? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.4 | Creation/modification/deletion of users? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.5 | Presentation of clinical or PII data (e.g. display, print)? | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.6 | Creation/modification/deletion of data? | No | _ | 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)? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.8 | Receipt/transmission of data or commands over a network or point-to-point connection? | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.8 AUDT-2.8.1 | Remote or on-site support? | No | _ | Section 5.2, AUDT Section 5.2, AUDT | AU-2 AU-2 | None |
| 7.001 2.0.1 | Application Programming Interface (API) and similar | | | 3.2,71001 | 7.0 2 | Hone |
| AUDT-2.8.2 | 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 | · | No | | Section 5.2, AUDT | AU-2 | None |
| ALIDT. 2 | Can the owner/operator define or select which | No | | Section 5.2 AUDT | ALL 2 | None |
| AUDT-3 | events are recorded in the audit log? Is a list of data attributes that are captured in the | No | | Section 5.2, AUDT | AU-2 | None |
| AUDT-4 | audit log for an event available? | No | | Section 5.2, AUDT | AU-2 | None |
| | Does the audit log record date/time? | No | | Section 5.2, AUDT | AU-2 | None |

| Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 | | | |
|----------------------|---|-------------------|---|-----------------------|-----------------------|----------------|
| | Can date and time be synchronized by Network Time | | | | | |
| AUDT-4.1.1 | Protocol (NTP) or equivalent time source? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-5 | Can audit log content be exported? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-5.1 | Via physical media? | No | _ | | | |
| | Via IHE Audit Trail and Node Authentication (ATNA) | | | | | |
| AUDT-5.2 | profile to SIEM? | No | _ | | | |
| AUDT 5 2 | Via Other communications (e.g., external service | | | | | |
| AUDT-5.3 | device, mobile applications)? Are audit logs encrypted in transit or on storage | No | _ | | | |
| AUDT-5.4 | media? | No | | | | |
| 7.001 311 | Can audit logs be monitored/reviewed by | | _ | | | |
| AUDT-6 | owner/operator? | No | _ | | | |
| AUDT-7 | Are audit logs protected from modification? | No | _ | Section 5.2, AUDT | AU-2 | None |
| AUDT-7.1 | Are audit logs protected from access? | No | | | | |
| 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. | | | | | |
| | | | | | | |
| | Does the device prevent access to unauthorized users | | Lifescreen PRO does not directly prevent access. The | | | |
| ALITH 1 | through user login requirements or other mechanism? | No | authorization to use Lifescreen PRO is granted by | Section F.2 AllTII | IA-2 | A.9.2.1 |
| AUTH-1 | Can the device be configured to use federated | No | permission held within the Sentinel system | Section 5.3, AUTH | IA-Z | A.9.2.1 |
| | credentials management of users for authorization | | | | | |
| AUTH-1.1 | (e.g., LDAP, OAuth)? | No | | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| 7.0111 1.12 | Can the customer push group policies to the device | | _ | | <u>-</u> | , . |
| AUTH-1.2 | (e.g., Active Directory)? | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | Are any special groups, organizational units, or group | | | | | |
| AUTH-1.3 | policies required? | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | Can users be assigned different privilege levels based | | | | | |
| | on 'role' (e.g., user, administrator, and/or service, | | | | | |
| AUTH-2 | etc.)? | No | _ | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | Con the device and a second second second the second second | | | | | |
| | Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access | | | | | |
| | operating system or application via local root or | | | | | |
| AUTH-3 | administrator account)? | No | | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| 701113 | Does the device authorize or control all API access | | _ | 3666011 3.3, 710 111 | 7.7.2 | 7.13.2.1 |
| AUTH-4 | requests? | No | | Section 5.3, AUTH | IA-2 | A.9.2.1 |
| | | | _ | , | | |
| | Does the device run in a restricted access mode, or | | Lifescreen PRO runs as a single process on clients in | | | |
| AUTH-5 | 'kiosk mode', by default? | Yes | Sentinel network topologies | | | |
| | | | | | | |
| | 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. | | | | | |
| | 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 | | | | | |
| CCLID 4 | software/firmware? If no, answer "N/A" to questions | | | | | |
| CSUP-1 | in this section. | Yes | Lifection DDO is a coffware and dust this the | | | |
| | Does the device contain an Operating System? If yes, | | Lifescreen PRO is a software product. It is the customers responsibility to provide the physical PC | | | |
| CSUP-2 | | No | on which it runs. | | | |
| CJU1 -Z | COMPLETE 2.1-2.4. | 140 | on willout it ruits. | | | |

| | Does the device documentation provide instructions | | |] | |
|-----------|---|------|--|--------------|--|
| | for owner/operator installation of patches or | | | | |
| CSUP-2.1 | software updates? | Vac | | | |
| C30F-2.1 | software updates: | Yes | _ | | |
| | Door the device were incomeded on an angle of the sire of | | | | |
| 00110 0 0 | Does the device require vendor or vendor-authorized | | | | |
| CSUP-2.2 | service to install patches or software updates? | No | _ | | |
| | | | | | |
| | Does the device have the capability to receive remote | | | | |
| CSUP-2.3 | installation of patches or software updates? | No | _ | | |
| | Does the medical device manufacturer allow security | | | | |
| | updates from any third-party manufacturers (e.g., | | | | |
| | Microsoft) to be installed without approval from the | | | | |
| CSUP-2.4 | manufacturer? | Yes | _ | | |
| | Does the device contain Drivers and Firmware? If yes, | | | | |
| CSUP-3 | complete 3.1-3.4. | No | _ | | |
| | Does the device documentation provide instructions | | | | |
| | for owner/operator installation of patches or | | | | |
| CSUP-3.1 | software updates? | No | | | |
| | · | | | | |
| | Does the device require vendor or vendor-authorized | | | | |
| CSUP-3.2 | service to install patches or software updates? | No | | | |
| 3301 3.2 | service to instan pateries of software apartes. | | | | |
| | Does the device have the capability to receive remote | | | | |
| CSUP-3.3 | installation of patches or software updates? | No | | | |
| C30F-3.3 | Does the medical device manufacturer allow security | | _ | | |
| | updates from any third-party manufacturers (e.g., | | | | |
| | | | | | |
| CCLID 2.4 | Microsoft) to be installed without approval from the | NI - | | | |
| CSUP-3.4 | manufacturer? | No | _ | | |
| | Does the device contain Anti-Malware Software? If | | | | |
| CSUP-4 | yes, complete 4.1-4.4. | No | _ | | |
| | Does the device documentation provide instructions | | | | |
| | for owner/operator installation of patches or | | | | |
| CSUP-4.1 | software updates? | Yes | _ | | |
| | | | | | |
| | Does the device require vendor or vendor-authorized | | | | |
| CSUP-4.2 | service to install patches or software updates? | Yes | _ | | |
| | | | | | |
| | Does the device have the capability to receive remote | | | | |
| CSUP-4.3 | installation of patches or software updates? | No | | | |
| | Does the medical device manufacturer allow security | | | | |
| | updates from any third-party manufacturers (e.g., | | | | |
| | Microsoft) to be installed without approval from the | | | | |
| CSUP-4.4 | manufacturer? | No | _ | | |
| | Does the device contain Non-Operating System | | | | |
| | commercial off-the-shelf components? If yes, | | | | |
| CSUP-5 | complete 5.1-5.4. | Yes | | | |
| | Does the device documentation provide instructions | | The COTS components are built in to the Lifescreen | | |
| | for owner/operator installation of patches or | | PRO system, patches or updates will require a new | | |
| CSUP-5.1 | software updates? | No | version of Lifescreen PRO. | | |
| 333. 3.1 | | - | 333.33 | | |
| | Does the device require vendor or vendor-authorized | | | | |
| CSUP-5.2 | service to install patches or software updates? | No | | | |
| C30F-3.2 | service to instan patches or software upuates: | | | | |
| | Does the device have the canability to receive remate | | | | |
| CCUD 5 3 | Does the device have the capability to receive remote | | | | |
| CSUP-5.3 | installation of patches or software updates? | No | | - | |
| | Does the medical device manufacturer allow security | | | | |
| | updates from any third-party manufacturers (e.g., | | | | |
| | Microsoft) to be installed without approval from the | | | | |
| CSUP-5.4 | manufacturer? | No | | | |
| | | | | | |

091-0441-00 Rev A

98800

Oct-24

Spacelabs Healthcare

| | Does the device contain other software components | | | | | |
|-----------|---|-----|----------|-----------------------|-----------------------|------------------|
| | (e.g., asset management software, license | | | | | |
| | management)? If yes, please provide details or | | | | | |
| CSUP-6 | refernce in notes and complete 6.1-6.4. | No | | | | |
| | Does the device documentation provide instructions | | | | | |
| | for owner/operator installation of patches or | | | | | |
| CSUP-6.1 | software updates? | Yes | | | | |
| | | | | | | |
| | Does the device require vendor or vendor-authorized | | | | | |
| CSUP-6.2 | service to install patches or software updates? | No | _ | | | |
| | | | | | | |
| | Does the device have the capability to receive remote | | | | | |
| CSUP-6.3 | installation of patches or software updates? | Yes | _ | | | |
| | Does the medical device manufacturer allow security | | | | | |
| | updates from any third-party manufacturers (e.g., | | | | | |
| | Microsoft) to be installed without approval from the | | | | | |
| CSUP-6.4 | | No | | | | |
| | | | _ | | | |
| CCLID 7 | Does the manufacturer notify the customer when | Vas | | | | |
| CSUP-7 | | Yes | _ | | | |
| CCLID 0 | Does the device perform automatic installation of | N | | | | |
| CSUP-8 | software updates? | No | <u> </u> | | | |
| | | | | | | |
| | Does the manufacturer have an approved list of third- | | | | | |
| CSUP-9 | | No | | | | |
| | Can the owner/operator install manufacturer- | | | | | |
| | approved third-party software on the device | | | | | |
| CSUP-10 | | No | _ | | | |
| | Does the system have mechanism in place to prevent | | | | | |
| CSUP-10.1 | • • | Yes | _ | | | |
| | Does the manufacturer have a process in place to | | | | | |
| CSUP-11 | | Yes | _ | | | |
| | Does the manufacturer provide customers with | | | | | |
| CSUP-11.1 | review and approval status of updates? | No | _ | | | |
| CSUP-11.2 | Is there an update review cycle for the device? | No | _ | | | |
| | | | | | | |
| | | | | | | |
| | 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. | | | _ | | |
| | | | | | | |
| | Does the device provide an integral capability to de- | | | | | |
| DIDT-1 | identify personally identifiable information? | No | _ | Section 5.6, DIDT | None | ISO 27038 |
| | Does the device support de-identification profiles | | | | | |
| | that comply with the DICOM standard for de- | | | | | |
| DIDT-1.1 | 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. | | | | | |
| | Does the device maintain long term primary storage | | | 1 | | |
| | of personally identifiable information / patient | | | | | |
| DTBK-1 | | No | | | | |
| D.D.C.I | Does the device have a "factory reset" function to | | _ | 1 | | |
| | restore the original device settings as provided by the | | | | | |
| DTBK-2 | manufacturer? | No | | Section 5.7, DTBK | CP-9 | A.12.3.1 |
| DI DIK-Z | Does the device have an integral data backup | 110 | _ | Section 5.7, DTBR | CI -3 | U.17'3'I |
| DTBK-3 | - | No | | Section 5.7, DTBK | CP-9 | A.12.3.1 |
| II)IKK-≺ | | | | 3000001 J./, DIDN | C1 J | / \. ± ∠ . J . ± |

| Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 | 4 | | |
|----------------------|--|-------------------|--|------------------------|-----------------------|---|
| | Does the device have an integral data backup | | | | | |
| DTBK-4 | capability to remote storage? Does the device have a backup capability for system | No | | - | | |
| | configuration information, patch restoration, and | | | | | |
| DTBK-5 | software restoration? | No | | | | |
| | | | | | | |
| DTDV 6 | Does the device provide the capability to check the | No | | Section 5.7 DTDV | CP-9 | A.12.3.1 |
| DTBK-6 | 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. | | 1 | _ | | |
| FMDC 1 | Does the device incorporate an emergency access | No | | Continu F 9 FMBC | SI-17 | None |
| EMRG-1 | (i.e. "break-glass") feature? | No | _ | Section 5.8, EMRG | 51-17 | 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. | | | | | |
| | Does the device provide data integrity checking | | | | | |
| | mechanisms of stored health data (e.g., hash or | | | | | |
| IGAU-1 | digital signature)? Does the device provide error/failure protection and | No | _ | Section 5.9, IGAU | SC-28 | A.18.1.3 |
| | recovery mechanisms for stored health data (e.g., | | | | | |
| IGAU-2 | 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 |
| | , | | | 120 111 00002 2 212022 | | 100 1700111010 |
| | The ability of the device to effectively prevent, detect | | | | | |
| | and remove malicious software (malware). | | | 7 | | |
| MLDP-1 | Is the device capable of hosting executable software? | No | | Section 5.10, MLDP | | |
| | | | | | | |
| | Does the device support the use of anti-malware | | | | | |
| | software (or other anti-malware mechanism)? | ., | Please refer exclusions from real time antivirus | | 21.2 | |
| MLDP-2 | Provide details or reference in notes. Does the device include anti-malware software by | Yes | scanning document :077-0255-00 Rev G | Section 5.10, MLDP | SI-3 | A.12.2.1 A.9.2.3, A.9.4.5, A.12.1.2, |
| MLDP-2.1 | default? | No | | Section 5.10, MLDP | CM-5 | A.3.2.3, A.9.4.3, A.12.1.2, A.12.1.4, A.12.5.1 |
| | Does the device have anti-malware software available | | | | | |
| MLDP-2.2 | as an option? | No | | Section 5.10, MLDP | AU-6 | A.12.4.1, A.16.1.2, A.16.1.4 |
| | Does the device documentation allow the | | | | | |
| MLDP-2.3 | owner/operator to install or update anti-malware software? | Yes | | Section 5.10, MLDP | CP-10 | A.17.1.2 |
| | Can the device owner/operator independently (re- | | | 333.32.20,22. | J. 20 | / 1412 |
| MLDP-2.4 |)configure anti-malware settings? | Yes | _ | Section 5.10, MLDP | AU-2 | None |
| | Does notification of malware detection occur in the | | | | | |
| MLDP-2.5 | device user interface? | N/A | | - | | |
| | Can only manufacturer-authorized persons repair | | | | | |
| MLDP-2.6 | systems when malware has been detected? | N/A | | | | |
| MLDP-2.7 | Are malware notifications written to a log? | N/A | | | | |
| | · · · · · · · · · · · · · · · · · · · | | | _ | | |

| Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 | | | |
|------------------------|--|-------------------|--|-----------------------|-----------------------|-------------------------------|
| MLDP-2.8 | Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? | N/A | | | | |
| | If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other | | | 6 5.40.44.00 | | A.12.6.1, A.14.2.2, A.14.2.3, |
| MLDP-3 | compensating controls in place or available? | N/A | | Section 5.10, MLDP | SI-2 | A.16.1.3 |
| | Does the device employ application whitelisting that restricts the software and services that are permitted | | | | | |
| MLDP-4 | to be run on the device? Does the device employ a host-based intrusion | N/A | | Section 5.10, MLDP | SI-3 | A.12.2.1 |
| MLDP-5 | 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) | | | 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. | 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. | | Node Authentication occurs between clients and the | | | |
| NAUT-1 | Web APIs, SMTP, SNMP)? | No | Sentinel side. | Section 5.11, NAUT | SC-23 | None |
| | Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use | | | | | A.13.1.1, A.13.1.3, |
| NAUT-2 | a network connection white list)? Is the firewall ruleset documented and available for | N/A | | Section 5.11, NAUT | SC-7 | A.13.2.1,A.14.1.3 |
| NAUT-2.1 | review? Does the device use certificate-based network | No | | | | |
| NAUT-3 | connection authentication? | No | | | | |
| | CONNECTIVITY CAPABILITIES (CONN) All network and removable media connections must be considered in determining appropriate security | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| | controls. This section lists connectivity capabilities that may be present on the device. | | | | | |
| CONN-1 | Does the device have hardware connectivity capabilities? | N/A | Lifescreen PRO is a software product | | | |
| CONN-1.1 | Does the device support wireless connections? | N/A | | | | |
| CONN-1.1.1 | | N/A | | | | |
| 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 | | | | |
| COMM-1.1.5 | Does the device support other wireless connections | INO | | | | |
| CONN-1.1.4 CONN-1.2 | (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? | No N/A | _ | | | |
| COIMIN-T.Z | boes the device support physical conflections: | IV/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? Does the device require, use, or support removable | No | | | | |
| CONN-1.2.3 | memory devices? | No | | | | |

Spacelabs Healthcare 98800 091-0441-00 Rev A Oct-24

| CONN-1.2.4 | Does the device support other physical connectivity? | No | |
|------------|--|-----|--|
| | Does the manufacturer provide a list of network ports | | Lifescreen PRO does not communicate over a |
| | and protocols that are used or may be used on the | | network. Network comms is a Sentinel function. |
| CONN-2 | device? | N/A | |
| | Can the device communicate with other systems | | Lifescreen PRO is a software product that will be |
| CONN-3 | within the customer environment? | N/A | hosted on customer hardware. |
| | Can the device communicate with other systems | | |
| | external to the customer environment (e.g., a service | | |
| CONN-4 | host)? | N/A | |
| CONN-5 | Does the device make or receive API calls? | N/A | |
| | Does the device require an internet connection for its | | |
| CONN-6 | intended use? | Yes | |
| | Does the device support Transport Layer Security | | |
| CONN-7 | (TLS)? | Yes | _ |
| | | | This is a software application. TLS configurations are |
| CONN-7.1 | Is TLS configurable? | No | applied at the OS layer. |
| | Does the device provide operator control | | |
| | functionality from a separate device (e.g., | | |
| CONN-8 | telemedicine)? | No | |

PERSON AUTHENTICATION (PAUT)

The ability to configure the device to authenticate

| | Does the device support and enforce unique IDs and | | |
|------------|--|------|---|
| | passwords for all users and roles (including service | | Sentinel manages user accounts on behalf of the |
| PAUT-1 | accounts)? | No | Lifescreen PRO |
| | Does the device enforce authentication of unique IDs | | |
| | and passwords for all users and roles (including | | |
| PAUT-1.1 | service accounts)? | No | _ |
| | | | |
| | Is the device configurable to authenticate users | | |
| | through an external authentication service (e.g., MS | | |
| PAUT-2 | Active Directory, NDS, LDAP, OAuth, etc.)? | No | |
| | | | _ |
| | Is the device configurable to lock out a user after a | | |
| PAUT-3 | certain number of unsuccessful logon attempts? | No | |
| | Are all default accounts (e.g., technician service | | |
| | accounts, administrator accounts) listed in the | | |
| PAUT-4 | documentation? | No | |
| PAUT-5 | Can all passwords be changed? | No | |
| | | | _ |
| | Is the device configurable to enforce creation of user | | |
| | account passwords that meet established | | |
| PAUT-6 | (organization specific) complexity rules? | No | |
| 17.01 0 | Does the device support account passwords that | | _ |
| PAUT-7 | expire periodically? | No | |
| 7,017 | expire periodically. | | - |
| PAUT-8 | Does the device support multi-factor authentication? | No | |
| PAUT-9 | Does the device support single sign-on (SSO)? | No | <u></u> |
| TAOTS | boes the device support single sign on (550). | | |
| PAUT-10 | Can user accounts be disabled/locked on the device? | No | |
| PAUT-11 | Does the device support biometric controls? | No | - |
| 17.01 11 | Does the device support physical tokens (e.g. badge | | - |
| PAUT-12 | access)? | No | |
| 7.01 12 | Does the device support group authentication (e.g. | | _ |
| PAUT-13 | hospital teams)? | No | |
| 7.01 10 | Does the application or device store or manage | | _ |
| PAUT-14 | authentication credentials? | No | |
| PAUT-14.1 | Are credentials stored using a secure method? | No | _ |
| 17.01 17.1 | The creatitians stored asing a secure method: | 1140 | <u> </u> |

| IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
|--|-----------------------|---|
| | | |
| Section 5.12, PAUT | IA-2 | A.9.2.1 |
| Section 5.12, PAUT | IA-2 | A.9.2.1 |
| Section 5.12, PAUT | IA-5 | A.9.2.1 |
| Section 5.12, PAUT | IA-2 | A.9.2.1 |
| Section 5.12, PAUT Section 5.12, PAUT | SA-4(5) | A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2 |
| Section 5.12, PAUT | IA-2 | A.9.2.1 |
| Section 5.12, PAUT | IA-2 | A.9.2.1 |
| Section 5.12, PAUT Section 5.12, PAUT | IA-2 IA-2 | A.9.2.1 A.9.2.1 |
| | | |
| | | |

SBOM-2.4

Are any additional descriptive elements identified?

| | 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 | | | IEC 1R 80001-2-2:2012 | NIST SP 800-55 Rev. 4 | 130 27002:2013 |
| | physical access to the device from compromising the | | | | | |
| | integrity and confidentiality of personally identifiable | | | | | |
| | information stored on the device or on removable | | | | | |
| | media | | | | | |
| | Is the device software only? If yes, answer "N/A" to | | | | | |
| PLOK-1 | | Yes | | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| | Are all device components maintaining personally | | | | | |
| | identifiable information (other than removable | | | | | |
| | media) physically secure (i.e., cannot remove without | | | | | |
| PLOK-2 | | N/A | _ | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| | Are all device components maintaining personally | | | | | |
| | identifiable information (other than removable | | | | | |
| | media) physically secured behind an individually | | | 6 11 5 42 51 61 | 25.2(4) | |
| PLOK-3 | · · · · · · · · · · · · · · · · · · · | N/A | _ | Section 5.13, PLOK | PE- 3(4) | A.11.1.1, A.11.1.2, A.11.1.3 |
| | Does the device have an option for the customer to | | | | | |
| DLOK 4 | attach a physical lock to restrict access to removable | N/A | | Section E 12 DLOV | DE 2/4) | A 11 1 1 A 11 1 2 A 11 1 2 |
| PLOK-4 | 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) | | | 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. | | | | | |
| | Was a secure software development process, such as | | | | | |
| | ISO/IEC 27034 or IEC 62304, followed during product | | | | | |
| RDMP-1 | development? | Yes | | Section 5.14, RDMP | CM-2 | None |
| | | | | | | |
| | Does the manufacturer evaluate third-party | | | | | |
| 20040 | applications and software components included in | V. | | Carlina F 44 BBMB | CN4.0 | |
| RDMP-2 | | Yes | _ | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| | Does the manufacturer maintain a web page or other source of information on software support dates and | | | | | |
| RDMP-3 | | Yes | | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| KUIVIF-3 | Does the manufacturer have a plan for managing | 163 | The list of third-party software is defined in the | Section 5.14, Noivir | CIVI-0 | A.8.1.1, A.8.1.2 |
| RDMP-4 | | Yes | products' software development plan. | Section 5.14, RDMP | CM-8 | A.8.1.1, A.8.1.2 |
| ROWN 4 | ama party component and or me. | 100 | products software development plan. | 30000113.11, 1131111 | CIVI C | ,, , |
| | | | | | | |
| | 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 | | | | |
| | Does the SBoM follow a standard or common method | | _ | | | |
| SBOM-2 | | Yes | _ | | | |
| SBOM-2.1 | <u> </u> | Yes | | | | |
| | Are the developers/manufacturers of the software | | | | | |
| SBOM-2.2 | · | Yes | | | | |
| CDOM 2.2 | Are the major version numbers of the software | Voc | | | | |
| SBOM-2.3 | components identified? | Yes | | | | |

| | Does the device include a command or process | | |
|--------|---|-----|---|
| | method available to generate a list of software | | |
| SBOM-3 | components installed on the device? | Yes | |
| SBOM-4 | Is there an update process for the SBoM? | Yes | _ |

| The device's interview restrained to approve and enter constant of control state of the contr | | SYSTEM AND APPLICATION HARDENING (SAHD) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
|--|-----------|--|------|---|-----------------------|-----------------------|-------------------------------|
| Ultracever NO A dependent on the control of any system feedbelling of the collection of the collecti | | • | | | | CM-7 | ۸ 12 5 1* |
| Section 215, 54/10 A A A A A A A A A | | maware. | | Lifescreen PRO is dependent on the controls and | | CIVI-7 | A.12.J.1 |
| Math | | Is the device hardened in accordance with any | | · | | | A.6.2.1, A.6.2.2, A.13.1.1, |
| SAFD 2 | SAHD-1 | industry standards? | N/A | operating system. | Section 5.15, SAHD | AC-17(2)/IA-3 | A.13.2.1, A.14.1.2/None |
| Does the device employ any mechanisms for enthusing the processing of the content of the conte | | Has the device received any cybersecurity | | | | | A.14.2.7, A.15.1.1, A.15.1.2, |
| SAND 5. Ober 15th Section Fig. 2, entering the symmetric interior (section of the section path) and the symmetric interior (section of the section of the se | SAHD-2 | certifications? | No | _ | Section 5.15, SAHD | SA-12(10) | A.15.1.3 |
| Does the device employ are rectangled accessoration? SMD-3.1 Assistance with the street employ are rectangled accessoration to commend the installed solvine rectangle rectangle rectangled accessoration to commend the installed solvine rectangled accessoration to commend the installed solvine rectangle rectangle rectangle rectangle rectangled accessoration to commend the installed solvine rectangle rectangled accessoration to commend the installed solvine rectangle rectangle rectangled accessoration rectan | | Does the device employ any mechanisms for software | | | | | |
| specific hash key, checksum, digital signature, etc.) to essure the installation of these is maintenance or consumer to installation of these is maintenance or consumer to installation of the decker protection. No. SAND 5. SAND 6. SAND 7. SAND 8. SAND 9. SAND 9. | SAHD-3 | integrity checking | No | _ | | | |
| to ensure the installed software is manufactured by althorized by althor | | Does the device employ any mechanism (e.g., release- | - | | | | |
| SAMD 3.1 authorized? See the device employ any mechanism is as, released secretic froath key, checksums, digital ginature, etc.) to ensure the souther exposite as the manufacturer of the souther souther and souther southe | | specific hash key, checksums, digital signature, etc.) | | | | | |
| Once the device employ any mechanism (e.g., refease specific hash beyond predators expectly nath signature, etc.) Demoure the software update are the manufacturer outhorized updates? AS22,0312,73512, AS412, AS412 AS44,AS43,AS433, SABD4 monified or tampered with? SABD4 monified or tampered with? SABD4 monified or tampered with? SABD5 monified or tampered with a monified monified monified or tampered with a monified monified with a monified monified monified with a monified monified with a monified monified with a monified monified with a moni | | to ensure the installed software is manufacturer- | | | | | |
| specific hash key, checksums, digital signature, etc.) to creasure the characteristic memory to the manufacture of subjects of the memory of t | SAHD-3.1 | authorized? | No | _ | | | |
| SAID-3.2 authorized updates? No Section 5.15, 5AHD CM-8 A.5.12, A.5.12 | | Does the device employ any mechanism (e.g., release- | - | | | | |
| SAND-3.7 Section 5.15, SAND CM-8 A.8.1.1, A.8.1.2 | | | | | | | |
| Cart the conter/operator perform software integrity checks (i.e., verify that the system has not been modified or the interested with part of the device provider role (i.e., software) (i.e., were first than the system configuration of the levels, positive to disolved the interested with part of the device provider role based access controls? SAND-S.1 Does the device provide role based access controls? No Does the device provide role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? SAND-S.1 Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device provider role based access controls? No Does the device role required role role access controls? No Does the device role required role role access role acc | | to ensure the software updates are the manufacturer- | - | | | | |
| checks (i.e., verify that the system has not been modified or transpered with!)? SAHD-5 Indication of file-level, patient level, or other implementation of file-level, patient level, or other implementations, or level implementation of file-level, patient level, or other implementations, or level implementation of file-level, patient level, or other implementations, to level implementation of file-level, patient level, or other implementations, to level implementation of file-level, patient level, or other implementations, to level implementation, to level implem | SAHD-3.2 | authorized updates? | No | _ | Section 5.15, SAHD | CM-8 | A.8.1.1, A.8.1.2 |
| checks (i.e., verify that the system has not been modified or transpered with!)? SAHD-5 Indication of file-level, patient level, or other implementation of file-level, patient level, or other implementations, or level implementation of file-level, patient level, or other implementations, or level implementation of file-level, patient level, or other implementations, to level implementation of file-level, patient level, or other implementations, to level implementation of file-level, patient level, or other implementations, to level implementation, to level implem | | | | | | | |
| SAHD-4 modified or tampered with? Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls? SAHD-5 Does the device provide role-based access controls? Are any system or user accounts restricted or disabled by the manufacturer at system delivery? SAHD-6 disabled by the manufacturer at system delivery? SAHD-6 Does this include restricting certain system or user accounts configurable by the odd user after intuits configurable by the not required for the intended use of the device most required for the intended use of the device most required for the intended use of the device provide for the intended use of the device of the device of the intended use of the device of the device of the intended use of the device of | | Can the owner/operator perform software integrity | | | | | A.6.2.2, A.9.1.2, A.9.4.1, |
| Is the system configurable to allow the implementation of file-level, paintif level, or other implementation of file-level, paintif level, and the second of the state | | | | | | | A.9.4.4, A.9.4.5, A.13.1.1, |
| implementation of file-level, patient level, or other types of access controls? SAHD-5.1 Does the device provide role-based access controls? Are any system or user accounts restricted or disabled by the manufacturer at system deliven? Are any system or user accounts configurable by the end user after initial configuration? Are any system or user accounts configurable by the end user after initial configuration? Are any system or user accounts configurable by the end user after initial configuration? Are any system or user accounts configurable by the end user after initial configuration? Are any system or user accounts configurable by the end user after initial configuration? Are all stord configuration? Are all stord configuration? Are all stord configuration or user and protocols that are not required for the intended use of the device disabled? Are all stord configuration or the device of the device of disabled? Are all stord configuration or the intended use of the device of disabled? Are all stord configurations (as a service technical configuration or the configuration or the configuration of the intended use of the device of the device of disabled? Are all stord configurations (as a service technical configuration or the configuration of the intended use of the device of the device of disabled? Are all stord configurations (as a service technical configuration or the configuration of the intended use of the device of the devi | SAHD-4 | | Yes | _ | Section 5.15, SAHD | AC-3 | A.14.1.2, A.14.1.3, A.18.1.3 |
| SAHD-5 types of access controls? No | | | | | | | |
| SAHD-5.1 Does the device provide role-based access controls? No Section 5.15, SAHD CM-7 A.12.5.1* 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 Are any system or user accounts configurable by the end user after initial configuration? N/A Section 5.15, SAHD CM-7 A.12.5.1* Does this include restricting certain system or user accounts, such as service technicians, to least provide the chindrians, to least on trequired for the intended use of the device disabled? N/A Section 5.15, SAHD CM-7 A.12.5.1* Are all anther resources (e.g., file shares) which are not required for the intended use of the device deleted/disabled? Yes customers to configure. SAHD-8 Are all services (e.g., telent, file transfer protocol [FIP], internet information server [IIS], etc., which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD CM-7 Section 5.15, SAHD Section 5.15, SAHD Section 5.15, SAHD CM-7 A.12.5.1* Are all applications (COTS applications as well as OS-included applications, e.g., Misternet Explore, e.g., which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD Section 5.15, SAHD SHAB Section 5.15, SAHD SHAB Section 5.15, SAHD SHAB N/A Section 5.15, SAHD SHAB Section 5.15, SAHD SHAB N/A SAHD SHAB N/A SAHD SHAB N/A SA | | | | | | | |
| Are any system or user accounts restricted or disabled by the manufacturer at system delivery? Are any system or user accounts configurable by the manufacturer at system delivery? Are any system or user accounts configurable by the medium and a system delivery? Are any system or user accounts restricting certain system or user accounts, such as service technicians, to least provide technicians, to least provide technicians, to least provide the intended use of the device disabled? Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of deleted/disabled? Are all applications server (IS), e.c.), which are not required for the intended use of the device of deleted/disabled? Are all applications (COTS applications as well as 05-c included applications; (RM) from the controlled or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of | SAHD-5 | types of access controls? | No | _ | Section 5.15, SAHD | CM-7 | A.12.5.1* |
| Are any system or user accounts restricted or disabled by the manufacturer at system delivery? Are any system or user accounts configurable by the manufacturer at system delivery? Are any system or user accounts configurable by the medium and a system delivery? Are any system or user accounts restricting certain system or user accounts, such as service technicians, to least provide technicians, to least provide technicians, to least provide the intended use of the device disabled? Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of the device of disabled? Are all services (e.g., file shares) which are not required for the intended use of the device of deleted/disabled? Are all applications server (IS), e.c.), which are not required for the intended use of the device of deleted/disabled? Are all applications (COTS applications as well as 05-c included applications; (RM) from the controlled or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of the device of the device or removable media (i.e., as our ce other than an internal for the intended use of the device or removable media (i.e., as our ce other than an internal for the intended use of | | | | | 5 .: 545 6415 | o | . 42 5 4* |
| SAHD-6 disabled by the manufacturer at system delivery? Are any system or user accounts configurable by the end user after initial configuration? Does this include restricting certain system or user accounts, such as service technicians, to least accounts, such as services technicians, to least accounts accou | SAHD-5.1 | Does the device provide role-based access controls? | NO | - | Section 5.15, SAHD | CIVI-7 | A.12.5.1* |
| SAHD-6 disabled by the manufacturer at system delivery? Are any system or user accounts configurable by the end user after initial configuration? Does this include restricting certain system or user accounts, such as service technicians, to least accounts, such as services technicians, to least accounts accou | | And any systems any coordinate machine and an | | | | | |
| Are any system or user accounts configuration? And Does this include restricting certain system or user accounts, such as service technicians, to least privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device deteed/disabled? Are all applications (CDT applications as well as OS-include applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device device deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device device deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device device deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device device deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device of the device device deleted/disabled? And the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal or the device prohibit boot from uncontrolled or removable media (i.e.) as source other than an internal or the device prohibit boot from uncontrolled o | CALID | | 01/0 | | Costion F 1F CAUD | CNA O | A O 1 1 A O 1 2 |
| SAHD-6.1 end user after initial configuration? Does this include restricting certain system or user accounts, such as service technicians, to least privileged access? SAHD-6.2 privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device disabled? 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 of deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.), which are not required for the intended use of the device of the thin an internal of the device | SAND-0 | | IN/A | _ | Section 5.15, SARD | CIVI-8 | A.6.1.1, A.6.1.2 |
| Does this include restricting certain system or user accounts, such as service technicians, to least privileged access? SAHD-6.2 Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? No | SAUD 6 1 | | N/A | | Section 5 15 SAHD | CM-7 | ۸ 12 5 1* |
| accounts, such as service technicians, to least privileged access? Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device disabled? 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 SAHD-9 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 detected/disabled? N/A Section 5.15, SAHD CM-7 A.12.5.1* Section 5.15, SAHD CM-6 None 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 detected/disabled? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | 3AHD-0.1 | | N/A | _ | Section 5.15, SAITE | CIVI-7 | A.12.3.1 |
| SAHD-6.2 privileged access? N/A Section 5.15, SAHD CM-7 A.12.5.1* Are all shared resources (e.g., file shares) which are not required for the intended use of the device deleted/disabled? No Section 5.15, SAHD CM-7 A.12.5.1* A.12.6.1, A.14.2.2, A.14.2.3, | | | | | | | |
| Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal resources). Are all shared resources (e.g., file shares) which are not required for the intended use of the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal resources). Are all shared resources (e.g., file shares) which are not required for the intended use of the device of the device deleted/disabled? No Lifescreen PRO is a software product. Spacelabs can provide the necessary ports and protocols for customers to configure. Section 5.15, SAHD Section 5.15, SAHD Section 5.15, SAHD CM-7 A.12.5.1* A.12.5.1.4 A.12.5.1 A.12.5.1.4 A.12.5.1 A.12.5.1.4 A.12.5.1 A.12.5.1.4 A.12.5.1 A.12.5.1.4 A.12.5.1 | SAHD-6 2 | | N/A | | Section 5.15 SAHD | CM-7 | Δ 12 5 1* |
| not required for the intended use of the device disabled? Are all communication ports and protocols that are not required for the intended use of the device (EFTP), internet information server [IIS], etc.), which are not required for the intended use of the device (EAHD-9) deleted/disabled? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device (EAHD-10) device deleted/disabled? 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 minute of the intended use of the device deleted/disabled? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | SATID-0.2 | | N/A | _ | Section 3.13, 3And | CIVI 7 | A.12.3.1 |
| SAHD-7 disabled? Are all communication ports and protocols that are not required for the intended use of the device SAHD-8 disabled? 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 SAHD-9 deleted/disabled? 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 device deleted/disabled? N/A Section 5.15, SAHD CM-7 A.12.5.1* A.12.5.1* Section 5.15, SAHD Soction 5.15, SAHD Soction 5.15, SAHD Soction 5.15, SAHD CM-6 None A.12.6.1, A.14.2.2, A.14.2.3, A.12.6.1, A.14.2.3, A.12.6.1, A.14.2.3, A.12. | | | | | | | |
| Are all communication ports and protocols that are not required for the intended use of the device disabled? SAHD-8 disabled? Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD SA-18 None Are all applications ever [IIS], etc.), which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD CM-6 None Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD SI-2 A.16.1.3 Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | SAHD-7 | • | No | | Section 5.15, SAHD | CM-7 | A 12.5.1* |
| not required for the intended use of the device disabled? 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? Are all applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the which are not required for the intended use of the Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | 574115 7 | | | Lifescreen PRO is a software product. Spacelabs can | 500.0.1 5.15, 5, 11.5 | c <i>,</i> | 7.112.13.12 |
| SAHD-8 disabled? Yes customers to configure. Section 5.15, SAHD SA-18 None Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD CM-6 None Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD SI-2 A.16.1.3 Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | | | | · · · · · · · · · · · · · · · · · · · | | | |
| Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? N/A Are all applications (COTS applications as well as OSincluded applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD CM-6 None A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD Sincluded applications of the device deleted/disabled? A.12.6.1, A.14.2.2, A.14.2.3, Section 5.15, SAHD A.12.6 | SAHD-8 | · | Yes | 1. | Section 5.15, SAHD | SA-18 | None |
| [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? N/A | 0 | | | G | | | |
| are not required for the intended use of the device SAHD-9 deleted/disabled? 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 SAHD-10 device deleted/disabled? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | | | | | | | |
| SAHD-9 deleted/disabled? N/A Section 5.15, SAHD CM-6 None Are all applications (COTS applications as well as OS- included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? N/A Section 5.15, SAHD SI-2 A.16.1.3 Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | | | | | | | |
| 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? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | SAHD-9 | | N/A | | Section 5.15, SAHD | CM-6 | None |
| included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the A.12.6.1, A.14.2.2, A.14.2.3, Adevice deleted/disabled? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | | · | | | , | | |
| which are not required for the intended use of the device deleted/disabled? Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal removable media (i.e., a source other than an int | | | | | | | |
| SAHD-10 device deleted/disabled? N/A | | | | | | | A.12.6.1, A.14.2.2, A.14.2.3. |
| Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal | SAHD-10 | · · · · · · · · · · · · · · · · · · · | N/A | | Section 5.15, SAHD | SI-2 | |
| removable media (i.e., a source other than an internal | | | | | | | |
| removable media (i.e., a source other than an internal | | Can the device prohibit boot from uncontrolled or | | | | | |
| | | · | | | | | |
| | SAHD-11 | | | | | | |

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

| Availability of security guidance for operator and administrator plue device and manufacturer sales and service. Does the device include security documentation for the work-operator? SGUD-1 the owner/operator? SGUD-2 Device the device three the capability, and provide instructions, for the permanent deletion of data from the device or media? SGUD-3 Are all access accounts documented? NA SGUD-3 Device the product include documentation on recommended compensating controls for the device? NA Does the product include documentation on recommended compensating controls for the device? NA HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the device to ensure unauthorized access stoes not compromise the indeptity and confidentiality of personally identifiable informations stared on the device or remove the indeptity and confidentiality of personally identifiable information stared on the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the device or remove integrity on the start of the start of the device or remove integrity of the start of the device or remove integrity of the start of the continuence of the start of the device or remove integrity of the start of the device or remove integrity of the start of the device or remove integrity of the start of the s | Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 | | | |
|--|----------------------|--|-------------------|--------|---|------------------------|----------------------------|
| SAND 13 ox periodical documentation include information on south periodical documentation included information or provinced sales of the periodical documentation or provinced sales of the periodical documentation or provinced sales or provin | | | | | | | |
| SAND 33 on operational network executing by pasts? SAND 34 can the device a manifest obeyond the default of control devices of the device of default of the pasts prepared access to MEO or other or No. SAND 34 can return from a southlike from vendor for increased of A. S. SAND 35 can be southliked as during (both). SAND 35 can be expected access to MEO or other No. SAND 35 can be expected as southliked from vendor for increased of A. S. SAND 35 can be southliked as during (both). Ask we additional hardening methods not included in No. SAND 35 can be expected as a southliked of the southliked of the southliked of the device of method. SECURITY GUIDANCE (SSUD) Ask additional hardening methods not included in No. SECURITY GUIDANCE (SSUD) Ask addition of pasts of pasts of pasts of the device of monitority of the device of monitority. SOUD-1 both owner/operation of the form of the form of the form owner/operation of the form of the form of the owner/operation of the form of the form of the owner/operation of the device of the owner/operation of the owner/operati | SAHD-12 | on the device without the use of physical tools? | N/A | | | | |
| Section 5.18, SOUD Section 5.18, SOUD MP-6 South 5.24 counter description of the defeat of product from vendor for increased MA | | Does the product documentation include information | | | | | |
| Seeb 13 proceeded state? NA Existatic Colors available from vendor for increased NA Seeb 13 And instance (Colors available from vendor for increased NA Seeb 13 And instance (Colors available from vendor for increased NA Seeb 13 Se | SAHD-13 | | | _ | | | |
| An instructions available from vendor for increased N/A N/A N/A SMD-15 Can the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system prevent access to 90% or other own and the system of t | | | | | | | |
| SAID-14.1 Indicating? SIAD-15 Carn the explane prevent access to 8005 or other boundaries during boot? Availability of Exempts of the device of conscious for control of the control of | SAHD-14 | - L' | N/A | _ | | | |
| SARD-15 Can the system greenel access to BIGS or other by MA SARD-15 Institutions or unique to that of the state of the s | CAUD 14 1 | | NI/A | | | | |
| SABLD 15 Bustulaters during bool 7 M/A Have additional hardwait prefronts not included in N/A Have additional hardwait dedicated N/A | JAIID-14.1 | <u> </u> | IN/A | | 1 | | |
| SECURITY GUIDANCE (SGUD) Availability of security guidance for operator and administrator of the device and monity-truer sales and service. SCILD-1 the convergiograph of the device and monity-truer sales and service. SCILD-1 the convergiograph of the device and monity-truer sales and service. SCILD-2 the convergiograph of the convergiograph of the service include security documentation for the convergiograph of the service include security documentation for the convergiograph of the service includes security documentation for the permanent celection of data from the device or monitorial instructions, for the permanent celection of data from the device or monitorial instructions, for the permanent celection of data from the device or monitorial instructions, for the permanent celection of data from the device or monitorial instructions, for the permanent celection of data from the device or monitorial instructions, for the permanent celection of data from the device or monitorial instructions and the service of the device or ensure unauthorized access dates not comparable the integrity and accombination or stord on the device or ensure unauthorized access dates not comparable the integrity of a confidential instruction in the device or remonitor media. STCF-1 Can the device contributed by N/A Are integrity of the device or composite media. N/A STCF-1 Section 5.17, STCT Section 5.17, STCT Section 5.17, STCT Section 5.17, STCF Section 5.17, S | SHAD-15 | | N/A | | | | |
| SECURITY GUIDANCE (SGUD) Availability of security guidance for operator and odministration of the device and manufacturer spiles and service. SCIUD-1 the owner/operator? SCIUD-1 the owner/operator? SCIUD-2 the remainst elektron of data from the device of monitorities of manufacturer spiles and service. SCIUD-3 was all access accounted documentation for the owner/operator? NA SCIUD-3 the objects of the device and manufacturer spiles and service. SCIUD-1 the objects or metale? NA SCIUD-3 to the permainst elektron of data from the objects or metale? NA SCIUD-3 to all accounts? SCIUD-3 to all accounts? NA SCIUD-3 to all accounts? HEALTH DATA STORAGE CONFIDENTIALITY STORAGE STORAGE CONFIDENTIALITY STORAGE CONFI | | | | | | | |
| SECURITY GUIDANCE (SGUD) Availability of security guidance for operator and administrator of the device and manufacturer sales and service. SOUD-1 Obes the device include security documentation for the converte generator and provide instructions, for the permanent deletion of data from SCUD-2 Obes the device have the capability, and provide Instructions, for the permanent deletion of data from SCUD-3 Are all access secrement deletion of data from SCUD-3 Obes the device or media? SOUD-3 Are all access secrements documented? Obes the product include documentation on greatment of accounted a secrement of accounted and secrement of accounted accounted accounted and secrement of accounted accounted accounted and secrement of accounted accounted accounted accounted accounted and secrement of accounted acco | | _ | | | | | |
| Availability of security quidance for operator and administrator of the device and manyloctures asles and service. Does the device include security documentalism for the owner/operator? SCUD-1 the owner/operator? Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? SCUD-2 Are all access accounts documented? N/A SCUD-3 Are all access accounts documented? SCUD-3 Are all access accounts documented? N/A SCUD-4 Product include documentation on recommended compensating controls for the device? N/A SCUD-4 PRODUCT (STCF) HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the device to ensure unauthorized access does not componing the integrity and confidentiality of personally identificable impromation stored on the device or removed media. STCF-1 Can the device accepted and strengthy and confidentiality of personally identificable impromation stored on the device or removed protected? N/A STCF-1 Scut the device accepted as at rest? N/A STCF-1 Scut the device accepted on the device of the strengthy of default? N/A STCF-1 Scut the device accepted on the very potential of the strengthy of default? N/A STCF-1 Scut the device accepted on the strengthy of default? N/A STCF-2 Can the device accepted on the device on the device of the device on th | SAHD-16 | 2.3.19 been used to harden the device? | N/A | _ | J | | |
| Admibitive of security guidance for operator and administrator of the device of manufacturer sales and service. Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? N/A Section 5.16, SSUD AT-2/PL-2 | | | | | | | |
| administrator of the device and manufacturer sales and service. Does the device include security documentation for No Section 5.16, SGUD AT-7/PI-7 | | SECURITY GUIDANCE (SGUD) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| and service. Does the device include security documentation for the wave/operator? No Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? SGUD-2 Are all access accounts documented? NA SGUD-3 Are all access accounts documented? NA Does the product include documentation on recommended compensating controls for the device? NA Does the product include documentation on recommended compensating controls for the device? NA HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of proposability of the device or ensure unauthorized access does not compromise the integrity and confidentiality of proposability of the device or ensure unauthorized access does not compromise the integrity and confidentiality of proposability configured by default? STCF-1 Can the device arrenged or configured? NA Are instructions available to the customer to onlique encryption? N/A STCF-1 Can the encryption available to the customer to onlique encryption? N/A STCF-1 Can the encryption has be changed or configured? N/A STCF-1 STCF-1 Can the encryption keys be changed or configured? N/A STCF-1 STCF-1 Str deduction available to the customer to onlique encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 Str deduction available to the customer to device or many the device or many t | | Availability of security guidance for operator and | | | | | |
| Does the device include security documentation for the owner/operator? Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? N/A SGUD-2 the device or media? N/A Are all access accounts documented? N/A SGUD-3.1 for all accounts? Does the product include documentation on recommended compensating controls for the device? N/A HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally information stored on the device or removed media. SICE-1 Can the device encryption data at its SY STCF-1 Is all data encryption capability configured by default? Are instructions available to the customer to configured? N/A STCF-1 Can the device or encryption Reys be changed or configured? N/A STCF-1 Can the device or encryption Reys be changed or configured? N/A STCF-1 Can the device or encryption Reys be changed or configured? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-3 is the data stored in a database external to the device? N/A STCF-4 is the data stored in a database external to the device? N/A STCF-4 is the data stored in a database external to the device? N/A STCF-4 is the data stored in a database external to the device? N/A STCF-5 is the data stored in a database external to the device? N/A STCF-6 is the data stored in a database external to the device? N/A STCF-7 is the data stored in a database external to the device? N/A STCF-7 is the data stored in a database external to the device? N/A STCF-7 is the data stored in a database external to | | | | | | | |
| SGUD-1 the owner/operator? No Section 5.16, SSUD AT-2/PL.2 Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? SGUD-2 Are all access accounts documented? NA Section 5.16, SGUD MP-6 SGUD-3.1 Can the owner/operator manage password control for all accounts? Does the product include documentation on recommended compensating controls for the device? N/A HEALTH DATA STORAGE CONFIDENTIALITY (STCF) IEC TR 80001-2-2:2012 NIST SP 800-53 Re The ability of the device to ensure unauthorized occess does not compromise the integrity and confidentiality of personally indentifiable information stored on the device or removable media. STCF-1 Can the device encrypt data at rest? N/A STCF-1.2 default? Are instructions available to the customer to default? Are instructions available to the customer to configure encryption? Are instructions available to the customer to device? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 Is the data stored in a database located on the device? N/A STCF-3 Is the data stored in a database external to the device? N/A STCF-3 Is the data stored in a database external to the device? N/A STCF-4 Is the data stored in a database external to the device? N/A STCF-1 Can the encryption keys be changed or configured? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to the device? N/A STCF-1 Is the data stored in a database external to th | Г | | | | 1 | | |
| Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? SGUD-3 Are all access accounts documented? N/A SGUD-3.1 Can the owner/operator manage password control for all accounts? N/A Does the product include documentation on recommended compensating controls for the device? N/A HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the device to ensure unauthorized occess does not compromise the integrity and confidentially destination of stored on the device or removable media. STCF-1 (and the device encrypt data at rest? N/A STCF-1.1 (is all data encryptor operator) Are instructions available to the customer to N/A Are instructions available to the customer to STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database external to the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database located on the device? N/A STCF-1 (is the data stored in a database external to the device? N/A STCF-1 (is the data stored in a database external to the device? N/A STCF-1 (is the data stored in a database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N/A STCF-1 (is the database external to the device? N | SCUD 1 | | No | | Saction E 16 SCUD | AT 2/DL 2 | A.7.2.2, A.12.2.1/A.14.1.1 |
| instructions, for the permanent deletion of data from the device or media? N/A SGUD 3 Are all access accounts documented? N/A SGUD 3 Are all access accounts documented? N/A SGUD 3.1 For all access accounts documented? N/A SGUD 3.1 For all access accounts documented? N/A SGUD 3.1 For all access accounts documentation on some product include documentation on ecommended compensating controls for the device? N/A SGUD 4.2 For 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-1.1 Sail data encryption ability configured by STCF-1.2 default? Are instructions available to the customer to N/A STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-1.3 is the data stored in a database located on the STCF-1 Stc and the data stored in a database external to the STCF-1 Stc and the data stored in a database external to the STCF-1 Stc and the device? N/A Stc and the encryption keys be changed or configured? N/A STCF-2 Can the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encryption keys be changed or configured? N/A Stc and the encrypt | 3G0D-1 | | NO | | Section 3.10, 300D | A1-2/FL-2 | A.7.2.2, A.12.2.1/A.14.1.1 |
| SGUD-2 the device or media? N/A Section 5.16, SGUD MP-6 SGUD-3 Are all access accounts documented? N/A Section 5.16, SGUD AC-6,IA-2 SGUD-3.1 Can the owner/operator manage password control of or all access accounts documentation on recommended compensating controls for the device? N/A SGUD-4 REALTH 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. STCF-1 Can the device nor ensure unauthorized by STCF-1.2 Is all data encryptic or deployed by N/A STCF-1.3 configured by Are instructions available to the customer to Are instructions available to the customer to STCF-1.3 configure encryption? N/A STCF-1.3 configure encryption? N/A STCF-2 Can the encryption Reys be changed or configured? N/A STCF-2 Can the encryption Reys be changed or configured? N/A STCF-3 Is the data stored in a database located on the device? N/A STCF-4 St. St. be data stored in a database external to the STCF-3 device? St. St. be data stored in a database external to the STCF-3 device? St. St. be data stored in a database external to the STCF-4 device? | | | | | | | A.8.2.3, A.8.3.1, A.8.3.2, |
| Can the owner/poerator manage password control for all accounts? M/A Does the product include documentation on recommended compensating controls for the device? N/A HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The oblity 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? STCF-1.1 S all data encryption capability configured by default? Are instructions available to the customer to STCF-1.3 configure encryption? Are instructions available to the customer to STCF-1.3 configure encryption? STCF-2 Can the encryption device profigured? N/A STCF-3 device? N/A SECTION 5.17, STCF SC-28 SC-2 | SGUD-2 | | | _ | Section 5.16, SGUD | MP-6 | A.11.2.7 |
| Can the owner/poerator manage password control for all accounts? N/A Does the product include documentation on recommended compensating controls for the device? N/A HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The oblity 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? STCF-1.1 S all data encrypted or otherwise protected? N/A STCF-1.2 default? Are instructions available to the customer to configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 device? N/A StCF-4 StC-4 StC-5 StC-6 StC-6 StC-7 StC-8 Section 5.17, STCF SC-28 S | | | | | | | A.9.1.2, A.9.2.3, A.9.4.4, |
| SGUD-3.1 for all accounts? | SGUD-3 | | N/A | _ | Section 5.16, SGUD | AC-6,IA-2 | A.9.4.5/A.9.2.1 |
| Does the product include documentation on recommended compensating controls for the device? N/A | SCUD 2.1 | | NI/A | | | | |
| HEALTH DATA STORAGE CONFIDENTIALITY (STCF) HEC TR 80001-2-2:2012 NIST SP 800-53 Re | 3000-3.1 | ioi ali accounts: | IN/A | | - | | |
| 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. STCF-1 Can the device encrypt data at rest? N/A STCF-1.1 Is all date encrypted or otherwise protected? N/A Is the data encryption capability configured by default? Are instructions available to the customer to STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A STCF-3 Is the data stored in a database located on the device? N/A STCF-4 STCF-4 STCF-4 STCF-4 STCF-6 SC-28 SECTION 5.17, STCF SC-28 | | Does the product include documentation on | | | | | |
| (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. STCF-1 Can the device encrypt data at rest? N/A | SGUD-4 | recommended compensating controls for the device? | N/A | | | | |
| (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. STCF-1 Can the device encrypt data at rest? N/A | | | | | | | |
| (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. STCF-1 Can the device encrypt data at rest? N/A | | HEALTH DATA STORAGE CONFIDENTIALITY | | | | | |
| The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media. STCF-1 | | | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media. STCF-1 | | • | | | | | |
| confidentiality of personally identifiable information stored on the device or removable media. STCF-1 | | | | | | | |
| STCF-1 Can the device or removable media. STCF-1.1 Is all date encrypted or otherwise protected? N/A Is the data encryption capability configured by STCF-1.2 default? N/A Are instructions available to the customer to STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A Is the data stored in a database located on the device? N/A Is the data stored in a database external to the device? Yes | | | | | | | |
| STCF-1 | | | | | | | |
| STCF-1.1 Is all data encrypted or otherwise protected? N/A Is the data encryption capability configured by default? N/A Are instructions available to the customer to configure encryption? N/A STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A Is the data stored in a database located on the device? N/A STCF-3 ls the data stored in a database external to the device? Yes STCF-4 device? Yes | STCF-1 | | IN/A | | Section 5.17, STCF | SC-28 | A.8.2.3 |
| Is the data encryption capability configured by default? Are instructions available to the customer to configure encryption? STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? Is the data stored in a database located on the device? N/A STCF-3 ls the data stored in a database external to the device? Ves STCF-4 device? Yes SECTION 1.17, STCF SC-28 | | | | _ | 300000000000000000000000000000000000000 | 36 26 | 7.1012.13 |
| Are instructions available to the customer to configure encryption? STCF-1.3 STCF-2 Can the encryption keys be changed or configured? Is the data stored in a database located on the device? N/A Section 5.17, STCF SC-28 STCF-3 Is the data stored in a database external to the device? Yes STCF-4 Are instructions available to the customer to N/A Section 5.17, STCF SC-28 Section 5.17, STCF SC-28 Section 5.17, STCF SC-28 STCF-4 | | | | | 1 | | |
| STCF-1.3 configure encryption? N/A STCF-2 Can the encryption keys be changed or configured? N/A Is the data stored in a database located on the STCF-3 device? N/A Is the data stored in a database external to the STCF-4 device? Yes SC-28 | STCF-1.2 | | N/A | | | | |
| STCF-2 Can the encryption keys be changed or configured? N/A Section 5.17, STCF SC-28 Is the data stored in a database located on the device? N/A STCF-3 Is the data stored in a database external to the device? Yes STCF-4 | | | | | | | |
| Is the data stored in a database located on the device? Is the data stored in a database external to the device? Yes Yes | STCF-1.3 | configure encryption? | N/A | | - | | |
| Is the data stored in a database located on the device? Is the data stored in a database external to the device? Yes Yes | STCF-2 | Can the encryption keys be changed or configured? | N/A | | Section 5.17 STCF | SC-28 | A.8.2.3 |
| STCF-3 device? N/A | 5.5. 2 | | .,,, | | - | 55.25 | , |
| STCF-4 device? Yes | STCF-3 | device? | N/A | _ | | | |
| | | | | | | | |
| TRANSMISSION CONFIDENTIALITY (TXCF) | STCF-4 | device? | Yes | _ |] | | |
| TRANSMISSION CONFIDENTIALITY (TXCF) | | | | | | | |
| | | TRANSMISSION CONFIDENTIALITY (TYCE) | | | IFC TR 80001_2_2.2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
| 11. Th 60001-2-2.2012 NIST SP 600-35 RE | | TRANSPORT CONTIDENTIALITY (TACI) | | | ILC 11 00001-2-2.2012 | 14151 SF 000-33 NEV. 4 | 130 2/002.2013 |

Page 12 of 13

| Spacelabs Healthcare | 98800 | 091-0441-00 Rev A | Oct-24 |
|----------------------|--|-------------------|--|
| 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? | No | |
| TXCF-2.1 | If data is not encrypted by default, can the customer configure encryption options? | No | |
| TXCF-3 | Is personally identifiable information transmission restricted to a fixed list of network destinations? | See Notes | Lifescreen PRO is a software product. It is recommended that customers follow the Spacelabs networking deployment guide. |
| TXCF-4 | Are connections limited to authenticated systems? | See Notes | Lifescreen PRO 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)? | N/A | |

| CM-7 | A.12.5.1 |
|------|----------|
| CM-7 | A.12.5.1 |
| | |
| CM-7 | A.12.5.1 |
| CM-7 | A.12.5.1 |
| | CM-7 |

NIST SP 800-53 Rev. 4

| | TRANSMISSION INTEGRITY (TXIG) | | |
|--------|--|-----|---|
| | The ability of the device to ensure the integrity of | | |
| | transmitted data. | | |
| | Does the device support any mechanism (e.g., digital | | |
| | signatures) intended to ensure data is not modified | | |
| TXIG-1 | during transmission? | No | _ |
| | Does the device include multiple sub-components | | |
| TXIG-2 | connected by external cables? | N/A | |

| | REMOTE SERVICE (RMOT) | | | IEC TR 80001-2-2:2012 | NIST SP 800-53 Rev. 4 | ISO 27002:2013 |
|-------|--|-----|---|-----------------------|-----------------------|------------------------------|
| | | | | | | |
| KIG-2 | connected by external cables? | N/A | | | | |
| | Does the device include multiple sub-components | | | | | |
| (IG-1 | during transmission? | No | _ | Section 5.19, TXIG | SC-8 | A.13.2.3, A.14.1.2, A.14.1.3 |
| | signatures) intended to ensure data is not modified | | | | | A.8.2.3, A.13.1.1, A.13.2.1, |
| | Does the device support any mechanism (e.g., digital | | | | | |

| | 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. | | | | | |
| | Does the device permit remote service connections | | Host server and customer controls can facilitate | | | A.6.2.1, A.6.2.2, A.13.1.1, |
| RMOT-1 | for device analysis or repair? | No | remote access. | | AC-17 | A.13.2.1, A.14.1.2 |
| | Does the device allow the owner/operator to | | | | | |
| | initiative remote service sessions for device analysis | | | | | |
| RMOT-1.1 | or repair? | N/A | _ | | | |
| | Is there an indicator for an enabled and active remote | | | | | |
| RMOT-1.2 | session? | N/A | _ | | | |
| | Can patient data be accessed or viewed from the | | | | | A.6.2.1, A.6.2.2, A.13.1.1, |
| RMOT-1.3 | device during the remote session? | N/A | _ | | AC-17 | A.13.2.1, A.14.1.2 |
| | Does the device permit or use remote service | | | | | |
| RMOT-2 | connections for predictive maintenance data? | N/A | _ | | | |
| | Does the device have any other remotely accessible | | | | | |
| | functionality (e.g. software updates, remote | | | | | |
| RMOT-3 | training)? | N/A | | | | |

OTHER SECURITY CONSIDERATIONS (OTHR)

NONE

Notes:

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

Note 1

IEC TR 80001-2-2:2012

IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

ISO 27002:2013

ISO 27002:2013