

Approved by ECO PR053240

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category Specialty Module	Manufacturer Spacelabs Healthcare	Document ID 091-0323-03, Rev. A	Document Release Date 30-Oct-2020
Device Model 91496	Software Revision 2.9.0	Software Release Date	30-Oct-2020
Manufacturer or Representative Contact Information:	Company Name Spacelabs Healthcare Representative Name/Position Michael Lanka, Information Security Officer	Manufacturer Contact Information Spacelabs Healthcare, 35301 S.E. Center Street, Snoqualmie, WA 98065	

<u>MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)</u>	Yes	No	N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?.....	Yes			#1
2. Types of ePHI data elements that can be maintained by the device:				
a. Demographic (e.g., name, address, location, unique identification number)?.....	Yes			#1
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?.....	No			
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?.....	No			
d. Open, unstructured text entered by device user/operator?.....	No			
3. Maintaining ePHI - Can the device				
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?.....	Yes			#2
b. Store ePHI persistently on local media?.....	No			
c. Import/export ePHI with other systems?.....	No			
4. Mechanisms used for the transmitting, importing/exporting of ePHI – Can the device				
a. Display ePHI (e.g., video display)?.....	No			#3
b. Generate hardcopy reports or images containing ePHI?.....	No			#3
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?.....	No			
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?.....	No			
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?.....	No			
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?.....	No			
g. Other?	N/A			

<u>ADMINISTRATIVE SAFEGUARDS</u>	Yes	No	N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?.....	No			
6. What underlying operating system(s) (including version number) are used by the device? VxWorks 5.3.....				

<u>PHYSICAL SAFEGUARDS</u>	Yes	No	N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e. cannot remove without tools)?	Yes			#4
8. Does the device have an integral data backup capability (i.e., backup onto removable media like tape, disk)?.....	No			
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No			

<u>TECHNICAL SAFEGUARDS</u>	Yes	No	N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?.....	No			
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	No			
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?.....	No			
b. Can the device provide an audit trail of remote-service activity?.....	No			
c. Can security patches or other software be installed remotely?.....	No			
12. Level of owner/operator service access to device operating system: Can the device owner/operator				
a. Apply device manufacturer-validated security patches?.....	No			
b. Install or update antivirus software?.....	No			
c. Update virus definitions on manufacturer-installed antivirus software?.....	No			
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?.....	No			
13. Does the device support user/operator specific username and password?.....	No			
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?.....	No			

This document contains Spacelabs Healthcare proprietary and confidential information.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Specialty Module	Spacelabs Healthcare	091-0323-03, Rev. A	30-Oct-2020
Device Model	Software Revision	Software Release Date	
91496	2.9.0	30-Oct-2020	
Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information	
	Spacelabs Healthcare	Spacelabs Healthcare, 35301 S.E. Center Street, Snoqualmie, WA 98065	
	Representative Name/Position Michael Lanka, Information Security Officer		
15. Events recorded in device audit trail (e.g., user, date/time, action taken): Can the audit trail record.....			
a. Login and logout by users/operators?.....			No #5
b. Viewing of ePHI?.....			No _____
c. Creation, modification or deletion of ePHI?.....			No _____
d. Import/export or transmittal/receipt of ePHI?.....			No _____
16. Does the device incorporate an emergency access ("break-glass") feature that is logged?.....			No
17. Can the device maintain ePHI during power service interruptions?.....			Yes #2
18. Controls when exchanging ePHI with other devices:.....			
a. Transmitted only via a point-to-point dedicated cable?.....			No _____
b. Encrypted prior to transmission via a network or removable media?.....			No _____
c. Restricted to a fixed list of network destinations.....			No _____
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?.....			Yes #6

Other Security Considerations

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Specialty Module	Spacelabs Healthcare	091-0323-03, Rev. A	30-Oct-2020
Device Model	Software Revision	Software Release Date	
91496	2.9.0	30-Oct-2020	
Manufacturer or Representative Contact Information:	Company Name Representative Name/Position	Manufacturer Contact Information	
	Spacelabs Healthcare Michael Lanka, Information Security Officer	Spacelabs Healthcare, 35301 S.E. Center Street, Snoqualmie, WA 98065	

SECTION 2

EXPLANATORY NOTES (from questions 1 - 19)

IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form

#1: ePHI is in the 91496 as part of a 12-lead report, specifically the patient name, ID, and age (which may be over 89). The 12-lead report complete with PHI is not available when the 91496 is inserted into a Spacelabs monitor and is only available after the report is sent to the Spacelabs ICS product and the ICS product is used to access the report.

#2 The 91496 can temporarily maintain PHI as a stand-alone device for a time period of ten minutes, after which the PHI is erased. This PHI is only available when the 91496 is inserted into a Spacelabs monitor.

#3. The 91496 product as a standalone product cannot maintain, transmit, or display ePHI. The 91496 product only works when integrated with Spacelabs monitoring products. When integrated with Spacelabs monitoring products the combination of the two products (module and monitor) can display PHI and generate hardcopy reports with PHI.

#4. ePHI is stored in volatile memory; the part is soldered onto the board and is not removable.

#5. There is no audit log in the 91496.

#6. A checksum is used to determine the integrity of the stored ePHI. Refer to note #2 for the 'lifetime' of the PHI after power is removed from the 91496.

This document contains Spacelabs Healthcare proprietary and confidential information.

© Copyright 2008 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.