

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category Intesys® Clinical Suite (ICS) Smart Disclosure	Manufacturer Spacelabs Healthcare	Document ID 091-0354-06 Rev B	Document Release Date 28-Oct-20
Device Model 92810, 92880, 92876	Software Revision 5.5.0	Software Release Date 28-Oct-20	
Manufacturer or Representative Contact Information: Michael Lanka, Information Security Officer	Company Name Spacelabs Healthcare Representative Name/Position	Manufacturer Contact Information Spacelabs Healthcare, 35301 S.E. Center Street, Snoqualmie, WA 98065	

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	Yes	No	N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?.....	Yes			
2. Types of ePHI data elements that can be maintained by the device:				
a. Demographic (e.g., name, address, location, unique identification number)?.....	Yes			
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?.....	Yes			
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?.....	Yes			
d. Open, unstructured text entered by device user/operator?.....	Yes			
3. Maintaining ePHI - Can the device				
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?.....	Yes			
b. Store ePHI persistently on local media?.....	Yes			#1
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)?.....	Yes			
b. Generate hardcopy reports or images containing ePHI?.....	Yes			
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)?.....	Yes			
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?.....	No			
g. Other?	N/A			

ADMINISTRATIVE SAFEGUARDS	Yes	No	N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?.....	Yes			
6. What underlying operating system(s) (including version number) are used by the device?.....				#2

PHYSICAL SAFEGUARDS	Yes	No	N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e. cannot remove without tools)?.....			N/A	#3
8. Does the device have an integral data backup capability (i.e., backup onto removable media like tape, disk)?.....			N/A	
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?.....		No		

TECHNICAL SAFEGUARDS	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?.....			N/A	#3
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?.....	Yes			#4
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?.....	Yes			#3
b. Can the device provide an audit trail of remote-service activity?.....		No		#3
c. Can security patches or other software be installed remotely?.....			N/A	#5
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?.....		Yes		
c. Update virus definitions on manufacturer-installed antivirus software?.....			N/A	
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?.....		No		#3
13. Does the device support user/operator specific username and password?.....	Yes			
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?.....		No		#3

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

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category Intesys® Clinical Suite (ICS) Smart Disclosure	Manufacturer Spacelabs Healthcare	Document ID 091-0354-06 Rev B	Document Release Date 28-Oct-20
Device Model 92810, 92880, 92876	Software Revision 5.5.0	Software Release Date	28-Oct-20
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	

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?..... Yes
 - b. Viewing of ePHI?..... Yes
 - c. Creation, modification or deletion of ePHI?..... Yes
 - d. Import/export or transmittal/receipt of ePHI?..... Yes
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?..... No
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..... Yes
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?..... Yes

Other Security Considerations

This is a software product that is hosted by the Health Delivery Organization on their network and infrastructure. A significant part of the product security is reliant on how the HDO implements, controls, and administers their network and host infrastructure.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Intesys® Clinical Suite (ICS) Smart Disclosure	Spacelabs Healthcare	091-0354-06 Rev B	28-Oct-20
Device Model	Software Revision	Software Release Date	
92810, 92880, 92876	5.5.0	28-Oct-20	
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		

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: This product is part of a suite of integrated software solutions. The Client software operates as an optional extension of the central ICS Client Access solution (92810), which includes a database. The database is where data is stored to disk. This service connects to the ICS database to gain access to data, but it does not store the data. If it is interrupted, it will resume operations after reconnecting with the database.

#2: The server and database software can be hosted on Windows Server 2012 R2 or Windows Server 2016. The client software can be loaded onto Windows 10 or Windows 7.

#3: This is a software product hosted by the customer Healthcare Delivery Organization (HDO). Physical security of the host server(s) and access to the server(s) and network(s) is controlled by the customer's IT infrastructure and policies. As part of administration, the HDO is responsible for data system backup, and is provided user instructions for how to perform this.

#4: The product does not enable remote access or service, but the customer could enable it on the host platform.

#5: This product is sold as software that is implemented on the Healthcare organizations infrastructure. Administration, patch and upgrade protocols are controlled by the hosting Healthcare organization.