

Manufacturer Disclosure Statement for Medical Device Security--MDS²

Device Category *		Manufacturer *		Document ID	Document Release Date
Device Model		Software Revision		Software Release Date	Other
Manufacturer or Representative Contact Information	Name		Title		Department
	Company Name		Telephone Number		E-mail

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (PHI) <i>As defined by HIPAA Security Rule, 45 CFR Part 164</i>	Yes	No	N/A	Note #
1. Can this device transmit or maintain <i>electronic Protected Health Information</i> (ePHI)?				
2. Types of ePHI data elements that can be maintained by the device:				
a. Demographic (e.g., name, address, location, unique identification number)?				
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?				
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiological data with identifying characteristics)?				
d. Open, unstructured text entered by device user/operator?				
3. Maintaining ePHI: <i>Can the device</i>				
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?				
b. Store ePHI persistently on local media?				
c. Import/export ePHI with other systems?				
4. Mechanisms used for the transmitting, importing/exporting of ePHI: <i>Can the device</i>				
a. Display ePHI (e.g., video display)?				
b. Generate hardcopy reports or images containing ePHI?				
c. Retrieve ePHI from or record EPHI to removable media (e.g., disk, DVD, CD_ROM, tape, CF/SD card, memory stick)?				
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?				
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?				
f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?				
g. Other _____				
ADMINISTRATIVE SAFEGUARDS				
5. Does manufacturer offer operator and technical support training or documentation on device security features?				
6. What underlying operating system(s) (including version number) are used by the device? _____				
PHYSICAL SAFEGUARDS				
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)?				
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?				
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?				
TECHNICAL SAFEGUARDS				
10. Can software or hardware not authorized by the device manufacturer be installed on the device?				
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?				
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?				
b. Can the device log provide an audit trail of remote-service activity?				
c. Can security patches or other software be installed remotely?				
12. Level of owner/operator service access to device operating system: <i>Can the device owner/operator?</i>				
a. Apply device manufacturer-validated security patches?				
b. Install or update antivirus software?				
c. Update virus definitions on manufacturer-installed antivirus software?				
d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)?				
13. Does the device support user/operator specific ID and password?				
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?				
15. Events recorded in device audit log (e.g., user, date/time, action taken): <i>Can the audit log record</i>				
a. Login and logout by users/operators?				
b. Viewing of ePHI?				
c. Creation, modification or deletion of ePHI?				
d. Import/export or transmittal/receipt of ePHI?				
16. Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use?				

17.	Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?		
18.	Controls when exchanging ePHI with other devices:		
a.	Transmitted only via a physically secure connection (e.g., dedicated cable)?		
b.	Encrypted prior to transmission via a network or removable media?		
c.	Restricted to a fixed list of network addresses (i.e., host-based access control list)?		
19.	Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?		

Manufacturer Disclosure Statement for Medical Device Security--MDS²

RECOMMENDED SECURITY PRACTICES

EXPLANATORY NOTES (from questions 1 – 19)

IMPORTANT: Refer to Instructions for the Manufacturers Disclosure Statement for medical Device Security for the proper interpretation of information provided in this form.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.