

# Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

Device Category † 15678 Computer, Nuclear Medicine	Manufacturer † GVI Medical Devices	Document ID	Document Release Date
Device Model OnePass	Software Revision B3x	Software Release Date 2005	
Manufacturer or Representative Contact Information:	Name	Title	Department
	Company Name GVI Medical Devices	Telephone # (330) 963-4083	e-mail support@gvimd.com

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) <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 (ePHI)</i> ? †	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: <i>Can the device</i>				
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			
c. Import/export ePHI with other systems?	Yes			
4. Mechanisms used for the transmitting, importing/exporting of ePHI: <i>Can the device</i>				
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)?	Yes			
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	Yes			
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			1
6. What underlying operating system(s) (including version number) are used by the device? <u>Linux Kernel 2.6.8 or greater</u>				

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)?	Yes			
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?	Yes			
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes			2

TECHNICAL SAFEGUARDS	Yes	No	N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device? .....	Yes			
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	Yes			3
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	Yes			
b. Can the device log provide an audit trail of remote-service activity?	Yes			
c. Can security patches or other software be installed remotely? .....	Yes			
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? .....	Yes			4
b. Install or update antivirus software? .....	Yes			5
c. Update virus definitions on manufacturer-installed antivirus software? .....	Yes			
d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? ..	Yes			
13. Does the device support user/operator specific ID <i>and</i> password? .....	Yes			
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)? .....	No			
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? .....	Yes			
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 logs each instance of use? .....	No			
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? .....	No			6
18. Controls when exchanging ePHI with other devices:				
a. Transmitted only via a physically secure connection (e.g., dedicated cable)? .....	No			
b. Encrypted prior to transmission via a network or removable media? .....	No			7
c. Restricted to a fixed list of network addresses (i.e., host-based access control list)? .....	Yes			8
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? ....	Yes			9

† Recommend use of ECRI's Universal Medical Device Nomenclature System (UMDNS).

Adapted from *Information Security for Biomedical Technology: A HIPAA Compliance Guide*, ACCE/ECRI, 2004.  
ACCE – the American College of Clinical Engineering; ECRI – formerly the Emergency Care Research Institute.

# Manufacturer Disclosure Statement for Medical Device Security – MDS<sup>2</sup>

## 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. User, installation, and service documentation have information about system security features and their use.
2. It is possible to boot from external CD media, but this feature may be password protected from unauthorized use.
3. Remote access is used only with a customer's agreement.
4. Users are instructed to only apply updates from media supplied and validated by the manufacturer.
5. Only manufacturer supplied and validated anti-virus software may be installed.
6. Systems are supplied with an external battery backup system (UPS) that will maintain power to the system for a defined minimum period during power service interruptions.
7. Network device sharing and data review operations utilize secure communication protocols. Data archived to removable media is not encrypted.
8. Restricted network access can be configured on customer request.
9. Network communication utilizes TCP/IP protocol which assures accurate transmission and reception of data.
- 10.
- 11.
- 12.
- 13.
- 14.
- 15.
- 16.
- 17.
- 18.
- 19.
- 20.