

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06985	Document Release Date	18-Nov-11
Device Model	Vitreax® and Vitrea fX®	Software Revision	6.2	Software Release Date			28-Nov-11
Manufacturer or Representative Contact Information:	Company Name	Vital Images, Inc.		Manufacturer Contact Information			
	Representative Name/Position	Ottar Schmitz Product Manager		5850 Opus Parkway Suite #300, Minnetonka MN 55343 952-487-9500			

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			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			___
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			___
c. Import/export ePHI with other systems?	Yes			___
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)?	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)?	Yes			___
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			2
6. What underlying operating system(s) (including version number) are used by the device? Microsoft Windows XP Professional x64 Edition, Windows 7 x64 Editions, Windows 2008 Server, and Windows 2003 Server Editions				___

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	3
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?			N/A	3

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)?			N/A	3
b. Can the device provide an audit trail of remote-service activity?			N/A	3
c. Can security patches or other software be installed remotely?			N/A	3
12. Level of owner/operator service access to device operating system: Can the device owner/operator				
a. Apply device manufacturer-validated security patches?			N/A	5
b. Install or update antivirus software?	Yes			3
c. Update virus definitions on manufacturer-installed antivirus software?	Yes			5
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?	Yes			3
13. Does the device support user/operator specific username and password?	Yes			3
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?			N/A	3

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06985	Document Release Date	18-Nov-11
Device Model	Vitreax® and Vitrea fX®	Software Revision	6.2	Software Release Date			28-Nov-11
Manufacturer or Representative Contact Information:	Company Name	Vital Images, Inc.		Manufacturer Contact Information			
	Representative Name/Position	Ottar Schmitz Product Manager		5850 Opus Parkway Suite #300, Minnetonka MN 55343 952-487-9500			

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	3
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?.....	Yes	3
18. Controls when exchanging ePHI with other devices:.....		
a. Transmitted only via a point-to-point dedicated cable?.....	N/A	3
b. Encrypted prior to transmission via a network or removable media?.....	N/A	3
c. Restricted to a fixed list of network destinations.....	N/A	3
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?.....	No	

Other Security Considerations

No additional security concerns identified.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06985	Document Release Date	18-Nov-11
Device Model	Vitreax® and Vitrea fX®	Software Revision	6.2	Software Release Date			28-Nov-11
Manufacturer or Representative Contact Information:	Company Name	Vital Images, Inc.		Manufacturer Contact Information			
	Representative Name/Position	Ottar Schmitz Product Manager		5850 Opus Parkway Suite #300, Minnetonka MN 55343 952-487-9500			

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. The term "device" herein refers to the Vitrea Enterprise Suite® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components.
2. The Vitrea® software can create audit logs that list user actions to ePHI data.
3. Vital Images, Inc. does not manufacture hardware or operating system software and /or components which may extend these functions.
4. Vital Images, Inc. Technical Support can use WebEx or VPN for remote application (Vitrea®) support
5. Vital Images, Inc. does not provide customers with Anti-Virus Definition Files, Operating System Security or Service Packs. Customer is responsible for managing hardware security and software update policies.