

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

### SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06981	Document Release Date	31-Oct-11
Device Model	Vitreia Enterprise Suite	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			
6. What underlying operating system(s) (including version number) are used by the device? Microsoft Windows XP Professional x32/x64 Edition, Windows Vista – x64/x32 Business Edition, Windows 7 x32/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			
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 – MDS<sup>2</sup>

### SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06981	Document Release Date	31-Oct-11
Device Model	Vitreia Enterprise Suite	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			5850 Opus Parkway Suite #300, Minnetonka MN 55343			
		Ottar Schmitz   Product Manager		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	2
b. Viewing of ePHI?.....	Yes	2
c. Creation, modification or deletion of ePHI?.....	Yes	2
d. Import/export or transmittal/receipt of ePHI?.....	Yes	2
16. Does the device incorporate an emergency access ("break-glass") feature that is logged?.....	No	3
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?.....	Yes	3
c. Restricted to a fixed list of network destinations.....	Yes	3
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?.....	No	3

### Other Security Considerations

No additional security concerns identified.

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

### SECTION 1

Device Category	Class II	Manufacturer	Vital Images, Inc.	Document ID	VLC-06981	Document Release Date	31-Oct-11
Device Model	Vitrea Enterprise Suite	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			5850 Opus Parkway Suite #300, Minnetonka MN 55343			
		Ottar Schmitz   Product Manager		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 Enterprise Suite® software can create audit logs that list user actions to ePHI data.ePHI information available to users in VES is in the form of DICOM data and Reports. Any time a user loads a dataset, creates snapshots or batches, exports, reports on, prints, burns to media or deletes it from VES, action is logged in an audit log file
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.