Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17

Device Model	Software Revision		Software Release Date
Vitrea Advanced Visualization	7.5		28-Apr-17

Manufacturer or Representative Contact Information	Company Name Vital Images, Inc.	Manufacturer Contact Information 5850 Opus Parkway Suite #300, Minnetonka MN 55343 952-487-9500
	Representative Name/Position Kelly Dupasquier, Program Manager	

Intended use of **device** in network-connected environment:

Vitrea is a medical diagnostic system that allows the processing, review, analysis, communication, and media interchange of multi-dimensional

digital images acquired from a variety of imaging devices. Vitrea is not meant for primary image interpretation in mammography

MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information [ePHI]**)?	Yes	1
B	Types of **private data** elements that can be maintained by the **device**:		
B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	__
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	Yes	__
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	__
B.4	Open, unstructured text entered by **device user/operator**?	Yes	__
B.5	**Biometric data**?	No	__
B.6	Personal financial information?	No	__
C	Maintaining **private data** - Can the **device**:		
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	1
C.2	Store **private data** persistently on local media?	Yes	1
C.3	Import/export **private data** with other systems?	Yes	1
C.4	Maintain **private data** during power service interruptions?	Yes	1
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
D.1	Display private data (e.g., video display, etc.)?	Yes	__
D.2	Generate hardcopy reports or images containing **private data**?	Yes	__
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	1
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	1
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	1
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	1
D.7	Import **private data** via scanning?	Yes	__
D.8	Other?	N/A	__

Management of Private Data notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components.

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17

Device Model	Software Revision		Software Release Date
Vitrea Advanced Visualization	7.5		28-Apr-17

SECURITY CAPABILITIES

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

		Yes, No, N/A, or See Note	Note #
1	**AUTOMATIC LOGOFF (ALOF)**		
	The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	1
	1-1.1 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	Yes	2
	1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	No	
ALOF notes:	1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions. 2. The length of inactivity time before auto-logoff has a default of four hours for a user session and 15 min for application inactivity.		
2	**AUDIT CONTROLS (AUDT)**		
	The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	No	1
2-2	Indicate which of the following events are recorded in the audit log:		
	2-2.1 Login/logout	No	1
	2-2.2 Display/presentation of data	No	1
	2-2.3 Creation/modification/deletion of data	No	1
	2-2.4 Import/export of data from **removable media**	No	1
	2-2.5 Receipt/transmission of data from/to external (e.g., network) connection	No	2
	2-2.5.1 **Remote service** activity	No	2
	2-2.6 Other events? (describe in the notes section)	N/A	__
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
	2-3.1 **User** ID	Yes	1
	2-3.2 Date/time	Yes	1
AUDT notes:	1. The Vitrea software can create audit logs that list user actions to ePHI data. ePHI information available to users is in the form of DICOM data and Reports. Any time a user exports, reports on, or burns ePHI to media from Vitrea, the action is logged in a log file. User logouts due to automatic logoff (session time out) are not tracked. 2. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.		
3	**AUTHORIZATION (AUTH)**		
	The ability of the device to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	Yes	1
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	__
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	Yes	1
AUTH notes:	1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.		

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17
Device Model	**Software Revision**		**Software Release Date**
Vitrea Advanced Visualization	7.5		28-Apr-17

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

4 CONFIGURATION OF SECURITY FEATURES (CNFS)

The ability to configure/re-configure **device security capabilities** to meet **users'** needs.

4-1 Can the **device** owner/operator reconfigure product **security capabilities**?	Yes	1

CNFS notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

5 CYBER SECURITY PRODUCT UPGRADES (CSUP)

The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches.

5-1 Can relevant OS and **device** security patches be applied to the **device** as they become available?	Yes	1, 2
5-1.1 Can security patches or other software be installed remotely?	Yes	1

CSUP notes:
1. 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.
2. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

6 HEALTH DATA DE-IDENTIFICATION (DIDT)

The ability of the **device** to directly remove information that allows identification of a person.

6-1 Does the **device** provide an integral capability to de-identify **private data**?	Yes	

DIDT notes:

7 DATA BACKUP AND DISASTER RECOVERY (DTBK)

The ability to recover after damage or destruction of **device** data, hardware, or software.

7-1 Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	No	1

DTBK notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

8 EMERGENCY ACCESS (EMRG)

The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.

8-1 Does the **device** incorporate an **emergency access** ("break-glass") feature?	No	1

EMRG notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

9 HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)

How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.

9-1 Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	No	1

IGAU notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17

Device Model	Software Revision		Software Release Date
Vitrea Advanced Visualization	7.5		28-Apr-17

	Yes, No, N/A, or See Note	Note #
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		

10 MALWARE DETECTION/PROTECTION (MLDP)

The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).

10-1 Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	Yes	1
10-1.1 Can the **user** independently re-configure **anti-malware** settings?	N/A	1
10-1.2 Does notification of **malware** detection occur in the **device user** interface?	N/A	1
10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	1
10-2 Can the device owner install or update **anti-virus software**?	Yes	1
10-3 Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	Yes	1

MLDP notes:
    1. 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.

11 NODE AUTHENTICATION (NAUT)

The ability of the **device** to authenticate communication partners/nodes.

11-1 Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	Yes	1

NAUT notes:
    1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

12 PERSON AUTHENTICATION (PAUT)

Ability of the **device** to authenticate **users**

12-1 Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	Yes	1
12-1.1 Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	1
12-2 Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	Yes	1
12-3 Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	N/A	1
12-4 Can default passwords be changed at/prior to installation?	Yes	1
12-5 Are any shared **user** IDs used in this system?	No	__
12-6 Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	1
12-7 Can the **device** be configured so that account passwords expire periodically?	N/A	1

PAUT notes:
    1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

13 PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.

13-1 Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	N/A	1

PLOK notes:
    1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17
Device Model	**Software Revision**		**Software Release Date**
Vitrea Advanced Visualization	7.5		28-Apr-17

	Yes, No, N/A, or See Note	Note #
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		

14 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

Manufacturer's plans for security support of 3rd party components within **device** life cycle.

14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	See Note	1
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	—

RDMP notes:
Microsoft Windows Server 2012 R2 Enterprise
Microsoft Windows 7 Professional 64-bit Edition with SP1
Microsoft Windows 8.1 Professional 64-bit
Microsoft Windows 10

15 SYSTEM AND APPLICATION HARDENING (SAHD)

The **device**'s resistance to cyber attacks and **malware**.

15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	Yes	1, 2
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	Yes	3
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes	3
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	Yes	3
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	Yes	3
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	Yes	3
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	3
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	Yes	3
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	No	3
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	Yes	3
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	Yes	3

SAHD notes:
1. The Vitrea software implements a Kiosk mode for the client user which prevents access to system desktop and user options.
2. Conformance: Vulnerability Monitoring & Response process results in immediate patch testing and remediation/mitigation procedures. The Vitrea software is analyzed against RMF/ATO DoD A&A standards.
3. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or

16 SECURITY GUIDANCE (SGUD)

The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.

16-1	Are security-related features documented for the **device user**?	Yes	1
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	Yes	1

SGUD notes:
1. The term "device" herein refers to the Vitrea® software and /or license. Vital Images does not manufacture hardware or operating system software and /or components which may extend these functions.

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
Class II	Vital Images, Inc.	VLC-09531	2-May-17

Device Model	Software Revision		Software Release Date
Vitrea Advanced Visualization	7.5		28-Apr-17

	Yes, No, N/A, or See Note	Note #
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		

17 HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.

17-1	Can the **device** encrypt data at rest?	No	__

STCF notes:

18 TRANSMISSION CONFIDENTIALITY (TXCF)

The ability of the **device** to ensure the confidentiality of transmitted **private data**.

18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	N/A	__
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	No	__
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	No	__

TXCF notes:

19 TRANSMISSION INTEGRITY (TXIG)

The ability of the **device** to ensure the integrity of transmitted **private data**.

19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	No	

TXIG notes:

20 OTHER SECURITY CONSIDERATIONS (OTHR)

Additional security considerations/notes regarding **medical device** security.

20-1	Can the **device** be serviced remotely?	Yes	1
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	Yes	1
	20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access?	Yes	1

1. Vital Images, Inc. Technical Support can use WebEx or VPN for remote application (Vitrea) support

OTHR notes:

© Copyright 2013 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.