Manufacturer Disclosure Statement for Medical Device Security – MDS[2]

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018

Device Model	Software Revision	Software Release Date
MyVue Center (M)	1.x	Feb. 2018

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	Carestream Health, Inc.	Telephone #: 1-800-328-2910
	Representative Name/Position: Technical Support	

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

Patient retrieval of study data and report for report print to paper, image print to film, image/report output to USB flash drive.

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	
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**?	No	
B.5	**Biometric data**?	No	
B.6	Personal financial information?	Yes	1
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	2
C.2	Store **private data** persistently on local media?	Yes	2
C.3	Import/export **private data** with other systems?	Yes	2
C.4	Maintain **private data** during power service interruptions?	Yes	2
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	
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	3
D.7	Import **private data** via scanning?	Yes	4
D.8	Other?	N/A	

Management of Private Data notes:	1. Insurance info only - if received in standard DICOM or HL7 messages. 2. Private data is obtained from the connected PACS system, RIS system or modalities. For the MyVue Center (M) terminal, data obtained from the connected systems is deleted from memory upon the user's study output being completed. For the MyVue Center (M) Platform Server, data obtained is aged/deleted from the system based on the data retention period defined by the customer and configured during installation. 3. Wifi only, and only if customer requires a separate wirless network to be used. 4. OCR is used to scan for specific text fields from eFilms that have been composed and sent from a modality or workstation for filming. Also, user IDs are read from barcode or magnetic card.

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018
Device Model	**Software Revision**		**Software Release Date**
MyVue Center (M)	1.x		Feb. 2018

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	1
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 Platform Server can be configured to log users off after XX minutes.		
2	**AUDIT CONTROLS (AUDT)**		
	The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	Yes	1
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	Yes	__
2-2.2	Display/presentation of data	Yes	__
2-2.3	Creation/modification/deletion of data	Yes	__
2-2.4	Import/export of data from **removable media**	Yes	__
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	Yes	__
2-2.5.1	**Remote service** activity	Yes	__
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	__
2-3.2	Date/time	Yes	__
AUDT notes:	1. The audit data is guaranteed to be available only for the configured data retention period.		
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	2
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	3
AUTH notes:	1. Passwords for the Platform Server users. Password and SecureLink VPN for Terminal desktop access. 2. Platform Server defines multiple user roles. 3. This access level is restricted to Carestream Health authorized service personnel.		

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018
Device Model	**Software Revision**		**Software Release Date**
MyVue Center (M)	1.x		Feb. 2018

	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**?	No	1
CNFS notes:	1. Security configuration is done by Carestream authorized service personnel. Https is always enabled.		
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
5-1.1	Can security patches or other software be installed remotely?	Yes	2
CSUP notes:	1. For both the MyVue Center (M) Platform Server and Terminal, the operating system is enabled to automatically download and install security patches when they are made available. 2. Certain software patches can be downloaded through RMS and installed. This can only be done by Carestream authorized service personnel.		
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**?	No	—
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. All data on the Platform Server is stored on Level 1 RAID (so any damaged drive can be reconstructed automatically). Configuration data can be backed-up and restored to/from files. But the backup files must be manually copied to the laptop PC of service personnel.		
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 customer system administrator has access to a subset of the patient data through their normal login role. Full access requires the authorized service personnel login.		
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	

IGAU
notes:

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018
Device Model	**Software Revision**		**Software Release Date**
MyVue Center (M)	1.x		Feb. 2018

	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 #
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)?	No	
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	N/A	
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	N/A	
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	
10-2	Can the device owner install or update **anti-virus software**?	No	1
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	See Note	2
MLDP notes:	1. Anti-virus software can be installed by Carestream authorized service personnel - in conjunction with the customer IT personnel. Sophos is the recommended anti-virus software. The anti-virus software must be purchased / supplied by the customer. 2. If installed, anti-virus software can be configured to automatically update on a periodic basis. This will require the customer to enable the required network ports.		
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 Platform Server sends/receives patient data only from pre-authorized devices (based on IP address, DICOM attributes) that are configured during installation. In addition, Platform Server and Terminal communication is via https and requires a proper digital certificate to be installed on the Terminal. For remote service access to Platform Server RMS/Alertlink is used - which requires configuration on both ends. For remote service access to Terminals SecureLink is used - which requires a custom digital certificate authentication to make the trusted VPN connection.		
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	
12-1.1	Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	No	
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	No	
12-4	Can default passwords be changed at/prior to installation?	Yes	
12-5	Are any shared **user** IDs used in this system?	Yes	1
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	See Note	2
12-7	Can the **device** be configured so that account passwords expire periodically?	No	

PAUT notes:	1. The cshsvc ID for web page login to the Platform Server is a single, shared ID. It is intended for installation only. Admin-level user/roles can be uniquely defined for multiple customer-specific admin login users. 2. Password complexity is not configurable. But the password is enforced to be at least 6 characters and must contain 1 numeric character.

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)?	See Note 1
PLOK notes:	1. Platform Servers must/should be located in a locked server room at the customer facility. Terminals all have locks that secure access to doors and internal compoents.	

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018
Device Model	**Software Revision**		**Software Release Date**
MyVue Center (M)	1.x		Feb. 2018

	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 #
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?	No	—
RDMP notes:	1. For Platform Server: Windows Server 2012 Standard v. 6.2.9200 Build 9200 For Terminal: Windows Embedded Standard 7 Service Pack 1		
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.	No	—
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?	No	—
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes	—
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	1
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	—
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	Yes	—
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	—
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	—
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	
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	See Note	2
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. Terminal desktop/file access is limited via user/group permissions. 2. Boot from a USB flash drive is only available for the purpose of completely reimaging the OS of the device. A custom boot key is required - available only to authorized service personnel. A BIOS change is also required to enable the boot. 3. Not normally. It is expected that such software is installed with the assistance of authorized service personnel. Only privileged administrator users can logon to the OS desktop. Once on the desktop additional software can be installed. Performance tests and other software interaction tests should be performed to ensure that the system functions as expected with the additional software installed.		
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)?	No	—

SGUD notes:	1. A "white paper" is available upon request to describe the security architecture of the MyVue Center (M) Self-Service Kiosk.

Device Category	Manufacturer	Document ID	Document Release Date
Class 1	Carestream Health, Inc.	AC7515	Feb. 2018

Device Model	Software Revision	Software Release Date
MyVue Center (M)	1.x	Feb. 2018

	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 #
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?	No	
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.)	See Note	1
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	2
TXCF notes:	1. Communications between hospital systems and MyVueCenter (M) is via standard DICOM and HL7 protocol, and thus is not encrypted. All communication between the MyVueCenter (M) Platform Server and the Terminals is via https and ftps protocol (using SSL). Patient data written to the USB flash drive is via DICOM Portable Data Interchange format and thus is not encrypted. 2. DICOM PHI data is sent to/from pre-defined nodes only. HL7 data is sent from pre-defined nodes only.		
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	
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	See Note	1
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	No	

	1. MyVueCenter (M) uses the Carestream Smartlink/RMS remote service approach. Only digitally authenticated Carestream authorized personnel are allowed remote access. All remote access is via a virtual tunnel from the Carestream RMS servers into the MyVueCenter (M) Platform Server or Terminals.
OTHR notes:	