

Manufacturer Disclosure Statement for Medical Device Security – MDS ²			
DEVICE DESCRIPTION			
Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	
Manufacturer or Representative Contact Information	Company Name Carestream Health, Inc. Representative Name/Position Technical Support	Manufacturer Contact Information Telephone #: 1-800-328-2910 e-mail: health.imaging.tsc@carestreamhealth.com	
Intended use of device in network-connected environment:			
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
			#
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?	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	—
C.2	Store private data persistently on local media?	Yes	—
C.3	Import/export private data with other systems?	Yes	—
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	—
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	—
D.7	Import private data via scanning?	Yes	—
D.8	Other?	No	—
Management of Private Data notes:		1. All data is written to the system hard drive. To protect against data loss/corruption it is strongly recommended to install UPS equipment to provide uninterruptible power.	

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

Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	

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-logout, session lock, password protected screen saver)?			Yes —
1-1.1	Is the length of inactivity time before auto-logout/screen lock user or administrator configurable? (Indicate time [fixed or configurable range] in notes.)			Yes —
1-1.2	Can auto-logout/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user ?			Yes —
ALOF notes:				
2	AUDIT CONTROLS (AUDT)			
The ability to reliably audit activity on the device .				
2-1	Can the medical device create an audit trail ?			Yes —
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
2-2.6	Other events? (describe in the notes section)			No —
2-3	Indicate what information is used to identify individual events recorded in the audit log:			
2-3.1	User ID			See Note 3
2-3.2	Date/time			Yes —
2. System has internal login control and activity logging. 3. Some Logging events contain the User ID, others do not.				
AUDT notes:				
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 —
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)?			No —
AUTH notes:				

Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	

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	4
CNFS notes: 4. The Web Site can configured to access by Http or Https.				
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	—
	5-1.1 Can security patches or other software be installed remotely?		Yes	5
CSUP notes: 5. Through installed remote access tool, service is able to install patches and other software remotely.				
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	6
DIDT notes: 6. When export image as Patient CD, user can select the option to hide patient information (Patient Name/Patient ID, etc.)				
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)?		Yes	7
DTBK notes: 7. This could be accomplished by the Windows operating systems backup / restore capability. For Patient data, the system may burn Patient CD and archive image to CD/DVD or removable USB disk.				
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?		Yes	—
EMRG notes:				
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?		Yes	
IGAU notes:				

Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	

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?	No	—	
10-1.2	Does notification of malware detection occur in the device user interface?	No	—	
10-1.3	Can only manufacturer-authorized persons repair systems when malware has been detected?	No	—	
10-2	Can the device owner install or update anti-virus software ?	Yes	8	
10-3	Can the device owner/ operator (technically/physically) update virus definitions on manufacturer-installed anti-virus software ?	Yes	8	
MLDP notes:	8. It is strongly recommended to install anti-virus/firewall software at both the host PC and web client PC, McAfee software is recommended to be installed along with Image Suite application.			
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	—	
NAUT notes:				
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?	No	—	
12-5	Are any shared user IDs used in this system?	Yes	—	
12-6	Can the device be configured to enforce creation of user account passwords that meet established complexity rules?	Yes	—	
12-7	Can the device be configured so that account passwords expire periodically?	Yes	—	
PAUT notes:				
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)?	No	9	
PLOK notes:	9. It is the site's responsibility to protect the PC equipment. (For example, by locking the PC to the table etc.)			

Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	

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).		Yes	10
14-2	Is a list of other third party applications provided by the manufacturer available? 10.Win 7 SP1/Win 8.1		Yes	—
RDMP notes:				
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)?		No	—
15-5	Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?		No	—
15-6	Are all shared resources (e.g., file shares) which are not required for the intended use of the device , disabled?		No	—
15-7	Are all communication ports which are not required for the intended use of the device closed/disabled?		No	—
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?		No	—
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)?		No	—
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools? 11. Only privileged users in operating system can reach the desktop and install additional software on the PC. The medical device is the Image Suite application software that is installed on a PC meeting the minimum specifications. It is the responsibility of the user to secure the PC and its OS.		Yes	11
SAHD notes:				
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	—
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	—
SGUD notes:				

Device Category 16247	Manufacturer Carestream Health, Inc.	Document ID 7K7078	Document Release Date 04/16/2016
Device Model CARESTREAM Image Suite	Software Revision 4.0 and Higher	Software Release Date 12/12/2013	

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.)	Yes	12	
18-3	Is private data transmission restricted to a fixed list of network destinations?	Yes	13	
TXCF notes: 12. Provide option to transfer PHI data via a network using HTTPS secure connection. All data is encrypted prior to transmission. But, still not encrypted prior to transmission via a removal media. 13. PHI data is sent to those predefined DICOM targets 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	14	
20-2	Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)?	Yes	15	
20-2.1	Can the device be configured to require the local user to accept or initiate remote access?	No	—	
14. Requires the site to be connected to the network and allow remote access. 15. Requires modifications to the Window's OS definitions.				
OTHR notes:				