

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Prone Breast Biopsy System	Hologic, Inc	MAN-05009	10/21/2016
Device Model	Software Revision		Software Release Date
Affirm Prone	1.0.1		4/11/2016
Manufacturer or Representative Contact Information	Company Name	Manufacturer Contact Information	
	Hologic, Inc	Chris.Fischer@hologic.com	
	Representative Name/Position		
	Chris Fischer		

Intended use of device in network-connected environment:
 The Hologic® Affirm™ Prone Breast Biopsy System is a 2D/3D™ imaging prone breast biopsy system designed to target lesions found in the patient’s diagnostic work up. The system is fully functional with no network connectivity, however it can be interfaced to a RIS to retrieve patient demographic information and to a PACS to archive biopsy procedure images.

MANAGEMENT OF PRIVATE DATA

		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.		
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 ?	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	—
	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	—
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?	No	—
	D.8 Other?	No	—

Management of Private Data notes:

Device Category Prone Breast Biopsy System	Manufacturer Hologic, Inc	Document ID MAN-05009	Document Release Date 10/21/2016
Device Model Affirm Prone	Software Revision 1.0.1	Software Release Date 4/11/2016	

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	#
--	---------------------------------	---

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
1-1.2	Can auto-logout/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user ?	Yes	—
	1. Inactivity logout interval configurable by customer.		
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	—
2-2.6	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	—
	Audit trail available to all Manager level users through the Hologic software.		
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)?	Yes	—
AUTH	notes:		
	System supports individual operator accounts and differing operator roles (Technologic and Manager.) Manager level users can create new accounts and revoke existing accounts.		

Device Category	Manufacturer	Document ID	Document Release Date	
Prone Breast Biopsy System	Hologic, Inc	MAN-05009	10/21/2016	
Device Model	Software Revision	Software Release Date		
Affirm Prone	1.0.1	4/11/2016		
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	—
CNFS notes:				
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?		No	—
	5-1.1 Can security patches or other software be installed remotely?		No	—
CSUP notes:	Hologic Affirm Prone Biopsy is an FDA regulated medical device, all software updates and patches need to be validated by the manufacturer. Patches are deployed on a regular basis through tested software updates.			
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:	1. Patient data can be de-identified through the standard software			
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	—
DTBK notes:	System only acts as a temporary store of patient data before it is transmitted to PACS. Any disaster recovery will be performed by Hologic Service.			
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	—
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?		No	—
IGAU notes:	System only acts as a temporary store of patient data before it is transmitted to PACS.			

Device Category	Manufacturer	Document ID	Document Release Date	
Prone Breast Biopsy System	Hologic, Inc	MAN-05009	10/21/2016	
Device Model	Software Revision	Software Release Date		
Affirm Prone	1.0.1	4/11/2016		
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)?		Yes	—
10-1.1	Can the user independently re-configure anti-malware settings?		Yes	—
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?		Yes	—
10-2	Can the device owner install or update anti-virus software ?		Yes	—
10-3	Can the device owner/ operator (technically/physically) update virus definitions on manufacturer-installed anti-virus software ?		Yes	—
MLDP notes:	Hologic validates most general Anti-Virus/Anti-Malware packages and provides instructions for installation by the customer. Automatic virus definition updates are supported.			
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?		No	—
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?		Yes	—
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?		Yes	2
12-7	Can the device be configured so that account passwords expire periodically?		Yes	—
PAUT notes:	1. Applications login for training and Service account for system maintenance are shared account. Password can be changed if needed. 2. Number of access attempts before account lockout and password complexity rules configurable by customer.			
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	—
PLOK notes:				

Device Category	Manufacturer	Document ID	Document Release Date		
Prone Breast Biopsy System	Hologic, Inc	MAN-05009	10/21/2016		
Device Model	Software Revision	Software Release Date			
Affirm Prone	1.0.1	4/11/2016			
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	
14-2	Is a list of other third party applications provided by the manufacturer available? Microsoft Windows 7 Professional SP1			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.			Yes	
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	—
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?			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?			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?			Yes	—
15-10	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?			Yes	—
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools? The Product Development Life Cycle (PDLC) of the device incorporates numerous security scans and other vulnerability assessments which are incorporated into the product design.			Yes	—
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 ?			No	—
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)? Hologic provides a Cyber Security Best Practices document on its website that provides recommendations on network security with the Affirm Prone product.			Yes	—
SGUD notes:					

Device Category	Manufacturer	Document ID	Document Release Date	
Prone Breast Biopsy System	Hologic, Inc	MAN-05009	10/21/2016	
Device Model	Software Revision	Software Release Date		
Affirm Prone	1.0.1	4/11/2016		
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?			Yes <u> </u>
STCF notes:	All PHI at rest is encrypted. System is only a temporary store of ePHI. System can be configured to automatically remove studies shortly after completion and successful transmission to PACS, and supports manual removal of patient records.			
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 <u> </u>
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 <u> </u>
18-3	Is private data transmission restricted to a fixed list of network destinations?			Yes <u> </u>
TXCF notes:	Device can be configured to only transmit to specific IP addresses. DICOM provides no native method to encrypt data, but TLS can be used on a local network.			
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 <u> </u>
TXIG notes:				
20 OTHER SECURITY CONSIDERATIONS (OTHR)				
Additional security considerations/notes regarding medical device security.				
20-1	Can the device be serviced remotely?			Yes <u> </u>
20-2	Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)?			Yes <u> </u>
20-2.1	Can the device be configured to require the local user to accept or initiate remote access?			No <u> </u>
OTHR notes:				