### Manufacturer Disclosure Statement for Medical Device Security – MDS²

#### DEVICE DESCRIPTION

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mammography System</td>
<td>Hologic, Inc</td>
<td>MAN-02859</td>
<td>8/8/2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Software Revision</th>
<th>Software Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions / 3Dimensions</td>
<td>1.9 / 2.0</td>
<td>8/8/2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manufacturer or Representative Contact Information</th>
<th>Representative Name/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td><a href="mailto:Chris.Fischer@hologic.com">Chris.Fischer@hologic.com</a></td>
</tr>
</tbody>
</table>

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

The Hologic® Selenia® Dimensions® Mammography system and 3Dimensions® Mammography system are designed to capture and transmit Conventional Mammography and 3D Mammography® images to a downstream PACS and Workstation for diagnosis.

#### MANAGEMENT OF PRIVATE DATA

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

<table>
<thead>
<tr>
<th>A</th>
<th>Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?</th>
<th>Yes, No, N/A, or See Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Types of private data elements that can be maintained by the device:</td>
<td></td>
</tr>
<tr>
<td>B.1</td>
<td>Demographic (e.g., name, address, location, unique identification number)?</td>
<td>Yes</td>
</tr>
<tr>
<td>B.2</td>
<td>Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?</td>
<td>Yes</td>
</tr>
<tr>
<td>B.3</td>
<td>Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?</td>
<td>Yes</td>
</tr>
<tr>
<td>B.4</td>
<td>Open, unstructured text entered by device user/operator?</td>
<td>Yes</td>
</tr>
<tr>
<td>B.5</td>
<td>Biometric data?</td>
<td>See Note 1</td>
</tr>
<tr>
<td>B.6</td>
<td>Personal financial information?</td>
<td>No</td>
</tr>
</tbody>
</table>

**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.)? | No |
| D.7 | Import private data via scanning? | No |
| D.8 | Other? | No |

**Management of Private Data notes:**

1. System is capable of using a biometric fingerprint scanner for user login as a convenience feature. Use of this system feature is optional and normal passwords can be used instead. Per the manufacturer, the fingerprint scanner does not store a copy of your fingerprint. Instead, it makes a map of 25 to 40 unique features of a fingerprint then puts it into a data format called a template. The template can only be interpreted by the specific biometric engine.
<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mammography System</td>
<td>Hologic, Inc</td>
<td>MAN-02859</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Security Capabilities**

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

### 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)?

- **1-1.1** Is the length of inactivity time before auto-logoff/session lock user or administrator configurable? (Indicate time [fixed or configurable range] in notes.)
  - **Yes** __
- **1-1.2** Can auto-logoff/session lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user?
  - **Yes** __

**ALOF notes:**

1. Inactivity logout interval configurable by customer.

### Audit Controls (AUDT)

The ability to reliably audit activity on the device.

2-1 Can the medical device create an audit trail?

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:**

Audit trail available to all Manager level users through the Hologic software.

### 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?

3-2 Can users be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular users, power users, administrators, etc.)?

3-3 Can the device owner/operator obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?

**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.

© Copyright 2013 by the National Electrical Manufacturers Association and the Healthcare Information and Management Systems Society.
### Device Category
Mammography System

### Manufacturer
Hologic, Inc

### Document ID
MAN-02859

### Software Revision
1.9 / 2.0

### Software Release Date
42955

---

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

---

### 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 1,2

**CNFS notes:**
1. OS Patches are validated by Hologic on a monthly basis and can be installed by the customer.
2. Because of the risk of non-validated system changes being applied and negatively impacting the performance or reliability of the device, we do not recommend this product be added to a domain.

---

### 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? No __

**CSUP notes:**
Hologic provides monthly critical and security patch validation for Dimensions and 3Dimensions Mammography platforms. Currently validated patch lists are posted to the Hologic website.

---

### 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.
### 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 __ |

Can the device owner install or update anti-virus software?

Can the device owner/operator (technically/physically) update virus definitions on manufacturer-installed anti-virus software?

Hologic validates most general Anti-Virus/Anti-Malware packages and provides instructions for installation by the customer. Automatic virus definition updates are supported.

### 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 __ |

### 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.)? | Yes 1 |
| 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 2 |
| 12-6 | Can the device be configured to enforce creation of user account passwords that meet established complexity rules? | Yes 3 |
| 12-7 | Can the device be configured so that account passwords expire periodically? | Yes __ |

1. Application can be configured for LDAP authentication.
2. Applications login for training and Service account for system maintenance are shared account. Password can be changed if needed.
3. Number of access attempts before account lockout and password complexity rules configurable by customer.

### 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)? | Yes __ |
## 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).

14-2 Is a list of other third party applications provided by the manufacturer available?

<table>
<thead>
<tr>
<th>RDMP notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 Professional SP1</td>
</tr>
</tbody>
</table>

## 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.

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?

15-3 Does the device have external communication capability (e.g., network, modem, etc.)?

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)?

15-5 Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?

15-6 Are all shared resources (e.g., file shares) which are not required for the intended use of the device, disabled?

15-7 Are all communication ports which are not required for the intended use of the device closed/disabled?

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?

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?

15-10 Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?

15-11 Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?

Ref: Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

SAHD notes:

1. The Product Development Life Cycle (PDLC) of the device incorporates numerous security scans (i.e. CIS, STIG) and other vulnerability assessments which are incorporated into the product design.

2. Application uses code signing. Installation media includes checksum testing capabilities. Application files checksum information can be provided upon request.

## 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?

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)?

SGUD notes:

1. Hologic provides a Cyber Security Best Practices document on its website that provides recommendations on network security with the Dimensions product.

2. Covered in product User Manuals.
<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mammography System</td>
<td>Hologic, Inc</td>
<td>MAN-02859</td>
<td></td>
</tr>
<tr>
<td>Device Model</td>
<td>Software Revision</td>
<td>1.9 / 2.0</td>
<td>42955</td>
</tr>
<tr>
<td>Dimensions / 3Dimensions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

### 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

STCF notes:

All PHI is encrypted at rest by the application using strong symmetric encryption. 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.

### 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.) No

18-3 Is private data transmission restricted to a fixed list of network destinations? Yes

TXCF notes:

Device can be configured to only transmit to specific IP addresses. TLS can be used on a local network.

### 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.) Yes

TXIG notes:

Device supports the use of TLS.

### 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)? Yes

20-2.1 Can the device be configured to require the local user to accept or initiate remote access? No

OTHR notes:

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