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

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	15-Nov-19

Device Model	Software Revision	Software Release Date
Surveyor S12/S19	v3.1.0	9-Jan-17

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	Welch Allyn, Inc.	Welch Allyn, Inc. 4341 State Street Road Skaneateles Falls, NY 13153 USA
	Representative Name/Position Ching Yue Yeung, WA Marketing Manager	

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

The Welch Allyn Surveyor Patient Monitor is indicated for use in adult, adolescents and children patient populations for the monitoring the following parameters: Non-invasive blood pressure, Impedance respiration, Invasive blood pressure, Temperature, Functional arteri oxygen saturation (SpO2), End-tidal & inspired CO2, ECG monitoring with arrhythmia & ST-segment, 12-Lead resting ECG, Cardiac output. The Welch Allyn Surveyor Patient Monitor is indicated for use in infants and neonatal patient populations for the monitoring of following parameters:Non-invasive blood pressure, Impedance respiration, Invasive blood pressure, Temperature, Functional arterial oxygen saturation (SpO2), End-tidal & inspired CO2, ECG monitoring with arrhythmia, 12-Lead resting ECG. The Welch Allyn Survey Patient Monitor is a prescription device intended to be used by healthcare professionals in all areas of a healthcare facility. The 'Bed to communication' feature allows remote viewing of monitors when connected to a Surveyor Central Station.

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)?	See Note
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	No
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	No
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?	See Note
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.)?	No
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:	1. Information stored include patient name including first, middle and last, as well as patient ID, room number, gen ethnicity, date of birth, height, weight and monitoring mode – whether adult, pediatric or neonate. Patient demogra coud be entered via setup or the Surveyor Central Station.

Device Category	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	43784
Device Model	**Software Revision**		**Software Release Date**
Surveyor S12/S19	v3.1.0		42744

SECURITY CAPABILITIES

		Yes, No, N/A, or See Note
	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	
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)?	See Note
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.)	N/A
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	N/A
ALOF notes:	1. Device needs to be on and active always given its intended use.	
2	**AUDIT CONTROLS (AUDT)**	
	The ability to reliably audit activity on the **device**.	
2-1	Can the **medical device** create an **audit trail**?	No
2-2	Indicate which of the following events are recorded in the audit log:	
2-2.1	Login/logout	N/A
2-2.2	Display/presentation of data	N/A
2-2.3	Creation/modification/deletion of data	N/A
2-2.4	Import/export of data from **removable media**	N/A
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	N/A
2-2.5.1	**Remote service** activity	N/A
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	N/A
2-3.2	Date/time	N/A
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?	See Note
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	See Note
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:	1. Access to device congifuration settings requires authorization by entering a PIN. Certain protected functions are only accessible under password control to the authorized users (i.e., Responsible Organization, IT/Biomed, Mortara Service, Mortara Manufacturing). Other general functions are available to operators.	2

Device Category	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	43784
Device Model	**Software Revision**		**Software Release Date**
Surveyor S12/S19	v3.1.0		42744

		Yes, No, N/A, or See Note
	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**?	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?	See Note
5-1.1	Can security patches or other software be installed remotely?	No
CSUP notes:	1. OS patches, if needed, will be provided together with application upgrades, installed by authorized personnel using a special USB memory stick.	
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**?	See Note
DIDT notes:	1. Patient information, including trends and demographic, are deleted after patient discharge.	
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:		
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?	See Note
EMRG notes:	1. No login is required for the device to be used. Data is always available for clinical personnel at the monitor station.	
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 fr the originator.	
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	See Note
IGAU notes:	1. Data integrity mecchanism are provided by the operating system. The configuration files have an internal check-sum.	

Device Category	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	43784
Device Model	**Software Revision**		**Software Release Date**
Surveyor S12/S19	v3.1.0		42744

	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
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)?	See Note
	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**?	N/A
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	N/A
MLDP notes:	1. The device is an embedded system with a specif use and not connected to internet. Anti-malware shall not be installed avoid interferances to the real time patient monitoring.	
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**?	No
	12-1.1 Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	No
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	N/A
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	N/A
12-4	Can default passwords be changed at/prior to installation?	No
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?	N/A
12-7	Can the **device** be configured so that account passwords expire periodically?	N/A
PAUT notes:		
13	**PHYSICAL LOCKS (PLOK)**	
	Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentia 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
PLOK notes:	1. The SD card is embedded deep in the monitor requiring significant time and effort to access.	

Device Category	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	43784
Device Model	**Software Revision**		**Software Release Date**
Surveyor S12/S19	v3.1.0		42744

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

RDMP notes:

1. The operating system is Windows CE 6.0.

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?	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?	Yes
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
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No

1. The device can boot from a USB and a specific USB containing custom software needed to upgrade the device.

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	Manufacturer	Document ID	Document Release Date
Monitor	Welch Allyn, Inc.	9710-183-01-ENG A	43784
Device Model	**Software Revision**		**Software Release Date**
Surveyor S12/S19	v3.1.0		42744

	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
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** store 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
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes
	1. A dedicated WLAN network is required using WPA2 security protocol with AES encryption.	
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.)	See Note
	1. Checksums provided by WiFi protocol and TCP; encryption provided by WPA2 protocol with AES encryption.	
TXIG notes:		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)**	
	Additional security considerations/notes regarding **medical device** security.	
20-1	Can the **device** be serviced remotely?	No
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	N/A
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	N/A
OTHR notes:		

This spreadsheet is 'locked.' Only certain cells can be edited. However row height can be freely adjusted as needed if enter does not fit into the provided space.

Yes
No
N/A
See Note

:013
e 17

g of
al

: the

yor
Bed

Note #
1
1

ıder,
phic

Note #

1

1

2

:013
e 19

Note #	
	—
	1
	1
	—
	1
om	
	1

Note #

1

to

ality

1

Note #

1

1

Note #

ed

1

1

ed text