

Manufacturer Disclosure Statement for Medical Device Security – MDS ²				
DEVICE DESCRIPTION				
Device Category	Manufacturer	Document ID	Document Release Date	
Mobile Software Application	Sway Medical	QSR-15-02	7/26/2018	
Device Model	Software Revision		Software Release Date	
Sway	3.0.0		7/24/2018	
Manufacturer or Representative Contact Information	Company Name	Manufacturer Contact Information		
	Sway Medical	Sway Operations LLC		
	Representative Name/Position	212 S. Front Street 76008, USA		
	Chase Curtiss, Chief Product Officer	P: 855-792-9633		
Intended use of device in network-connected environment:				
The Sway System is intended for use to assess sway as an indicator of balance. Individual suitability for assessment must be judged on a case by case basis, by a qualified individual including those certified and/or licensed in their state to prescribe and/or use balance devices such as certified athletic trainers and coaches, physical therapists, nurses and physicians.				
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	1
	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)?	Yes	1
	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	2
	C.2	Store private data persistently on local media?	No	—
	C.3	Import/export private data with other systems?	No	—
	C.4	Maintain private data during power service interruptions?	N/A	—
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	3
	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.)?	No	—
	D.5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	2
	D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	2
	D.7	Import private data via scanning?	No	—
	D.8	Other?	N/A	—
Management of Private Data notes:	<p>1. Sway collects and maintains the following ePHI (electronic Protected Health Information) First and Last Name, Date of birth, results of the balance test.</p> <p>2. The data is collected by the Sway Application on the mobile device and transferred to the database via cellular data (e.g. iPhone with AT&T or Verizon data plan) or WiFi connection. Data is not permanently stored on the mobile device. Data is stored on the device for the duration the user is logged in to the application. Local storage can be remotely wiped and a device logged out when an access token is revoked.</p> <p>3. The Sway Application can display patient information when the user enters patient profile edit page. The user can also access this information on the Web Portal. The Portal includes a feature allowing the healthcare professional to print a report containing the patient's name, height, weight, age, gender and balance test scores for reimbursement.</p>			

HN 1-2013

Page 18

Device Category	Manufacturer	Document ID	Document Release Date	
Mobile Software Application	Sway Medical	QSR-15-02	43307	
Device Model	Software Revision	Software Release Date		
Sway	3.0.0	43305		
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	4
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.)		No	—
1-1.2	Can auto-logout/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user ?		No	—
ALOF notes:	4. Authentication timeouts on the portal are used to automatically log out inactive accounts in order to safeguard unattended data.			
2	AUDIT CONTROLS (AUDT)			
	The ability to reliably audit activity on the device .			
2-1	Can the medical device create an audit trail ?		Yes	5
2-2	Indicate which of the following events are recorded in the audit log:			
2-2.1	Login/logout		No	—
2-2.2	Display/presentation of data		No	—
2-2.3	Creation/modification/deletion of data		Yes	5
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		No	—
2-3.2	Date/time		Yes	5
AUDT notes:	5. Sway Medical maintains an audit log that contains auditstamp of operations performed by users such as adding, removing or modifying profile information, adding new test results.			
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	6
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	7
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:	6. Access to Sway Application account is controlled with user id (email address) and password. 7. Account Administrator has ability to create users and assign them to groups.			

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

Device Category	Manufacturer	Document ID	Document Release Date	
Mobile Software Application	Sway Medical	QSR-15-02	43307	
Device Model	Software Revision	Software Release Date		
Sway	3.0.0	43305		
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?	See Note	8	
	5-1.1 Can security patches or other software be installed remotely?	—	—	
CSUP notes:	8. Any patches or updates to the iOS device are performed and maintained independtely of the Sway application. All updates to the Sway application can be applied as they become available in the App Store.			
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)?	Yes	9	
DTBK notes:	9. All data is stored in a database maintained in Secure Data Storage compliant with ISO 27000. Data is not permanently stored on the mobile device, web portal or any removable media. This inherently prevents from loss of data on the device.			
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	10	
EMRG notes:	10. No special procedures or features are implemented or needed since all data is electronically stored on a cloud therefore access by authorized individuals is not limited to a specific device or location. Data managed by healthcare professionals can be accessed in accordance with the heathcare professional organization's procedures.			
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	11	
IGAU notes:	11. The integrity of the ePHI data is assured through the use of SQL database in two main ways. One is the built-in functionality of the database management system provided by the vendor and its inherent handling of the data; and second way is the structure of the schema and appropriate design and development of the data base e.g. using appropriate form keys to ensure that certain types of data cannot be related to other kinds of data that don't exist or are not compatible. All data transmitted between a user's web browser and the web server is encrypted using 2048-bit SSL encryption. The data is hosted in Secure Data Storage compliant with ISO 27001.			

Device Category	Manufacturer	Document ID	Document Release Date		
Mobile Software Application	Sway Medical	QSR-15-02	43307		
Device Model	Software Revision	Software Release Date			
Sway	3.0.0	43305			
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)?		N/A	—	
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:					
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	11	
12-1.1	Does the device support unique user/operator -specific IDs and passwords for multiple users?		Yes	11	
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	
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?		Yes	12	
12-7	Can the device be configured so that account passwords expire periodically?		No	—	
<p>11. Access to Sway Application account is controlled with user id (email address) and password. Account Admin can create additional users and assign them to self-created groups. Each user has a unique ID (email address) and can access only the patient profiles within the particular group.</p> <p>12. Account administrators are authenticated by sending a Welcome Email to an email address provided by the person requesting Sway Account. Email contains randomly generated password that the user is required to change at first log-in. Passwords must be at least 6 characters in length. Passwords can be reset using the Sway customer web portal, which sends an email with a link to the email address on file for the account that is requesting a password reset. Sway cannot view nor has access to users' passwords.</p>					
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)?		Yes	13	
<p>13. Data on the device is temporarily stored in the internal memory of the device. Permanent data is stored in a database maintained in Secure Data Storage compliant with ISO 27000 hosted by Windows Azure which provides all appropriate physical security features.</p>					
PLOK notes:					

the Healthcare Information and Management Systems Society.

Device Category	Manufacturer	Document ID	Document Release Date	
Mobile Software Application	Sway Medical	QSR-15-02	43307	
Device Model	Software Revision	Software Release Date		
Sway	3.0.0	43305		
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 14
14-2	Is a list of other third party applications provided by the manufacturer available?			N/A
RDMP notes:	<p>14. The Sway Application runs on Apple devices (e.g. iPhone, iPad, iPod) running iOS version 9.3 or higher and Android devices running 6.0 or higher. The data is stored in a database maintained in Secure Data Storage compliant with ISO 27000 hosted by Windows Azure. Windows Azure, is audited by independent external auditors under industry standards, including ISO 27001. The audit scope includes controls that address HIPAA security practices as recommended by the U.S. Department of Health and Human Services. Additional information on security, privacy, and compliance certifications is available at the Windows Azure Trust Center http://www.windowsazure.com/en-us/support/trust-center/</p>			
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.			See Note 15
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?			N/A
15-3	Does the device have external communication capability (e.g., network, modem, etc.)?			N/A
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)?			N/A
15-5	Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?			N/A
15-6	Are all shared resources (e.g., file shares) which are not required for the intended use of the device , disabled?			N/A
15-7	Are all communication ports which are not required for the intended use of the device closed/disabled?			N/A
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?			N/A
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?			N/A
15-10	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?			N/A
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?			N/A
SAHD notes:	<p>15. Sway application is installed on iOS and Android devices and does not modify the mobile device characteristics or its operating system. Any hardening measures on the mobile device by the mobile device manufacturer. Any hardening measures of the computers used to access the data through the Web Portal are under discretion of customers' organizations.</p>			
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
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:	<p>16. Sway provides documentation on the software's security features including the MDS2 form and information on the Sway website.</p>			

Device Category	Manufacturer	Document ID	Document Release Date		
Mobile Software Application	Sway Medical	QSR-15-02	43307		
Device Model	Software Revision		Software Release Date		
Sway	3.0.0		43305		
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	17	
STCF notes:	17. All data on the device is stored within a SQLite database, which is fully encrypted using 256-bit AES encryption with a private key. Credentials are never stored and an access token is issued from the Sway API upon successful authentication for use in subsequent calls to the Sway API. Local storage is encrypted with 256 bit AES and can be remotely wiped by revoking access token.				
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	18	
18-3	Is private data transmission restricted to a fixed list of network destinations?		No	—	
TXCF notes:	18. All network communications with the Sway Application is limited only to the RESTful API. The communication with this API is secured via SSL (2048 bit) and utilize a JSON transport. All API calls from the device made beyond the initial login API call are authenticated using an issued authorization token from the RESTful API.				
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.)		Yes	19	
TXIG notes:	19. The integrity of the ePHI data is assured through the use of SQL database in two main ways. One is the built-in functionality of the database management system provided by the vendor and its inherent handling of the data; and second way is the structure of the schema and appropriate design and development of the data base e.g. using appropriate form keys to ensure that certain types of data cannot be related to other kinds of data that don't exist or are not compatible. All data transmitted between a user's web browser and the web server is encrypted using 2048-bit SSL encryption. The data is hosted in Secure Data Storage compliant with ISO 27001.				
20 OTHER SECURITY CONSIDERATIONS (OTHR)					
Additional security considerations/notes regarding medical device security.					
20-1	Can the device be serviced remotely?		N/A	—	
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:					



Category: Design History File
Title: MDS2 2015

Version 03	State Effective	Effective Date 26-JUL-2018	Document ID 93628
Document Number QSR-15-10	Document Owner Chase Curtiss		Design History File Design Output

Printed by alem.boukadoum@swaymedical.com from app.zenqms.com on 28-Jul-2018 at 2:06:42 PM UTC • Page 8 of 8

REVISION HISTORY

Version 01 Effective on 04-Dec-2017 by Scott Bednar

Initial upload of Sway Medical approved archive

Version 02 Effective on 30-May-2018 by Chase Curtiss

Updated to reflect SW Version 2.2.3 and GDPR requirements.

Version 03 Effective on 26-Jul-2018 by Chase Curtiss

Updated document to reflect DC1804.

DOCUMENT ELECTRONIC SIGNATURES

DOCUMENT APPROVAL WORKFLOW

Author Approval

Chase Curtiss

I am the author of this document.

Signed 1:13:48 PM UTC 26-Jul-2018

Additional Steps Added

Alem Boukadoum

I have reviewed and approve this document.

Signed 1:15:18 PM UTC 26-Jul-2018

Scott Bednar

I have reviewed and approve this document.

Signed 3:26:35 PM UTC 26-Jul-2018