		Category: Tier IV Labeling Title: QR-2003-01	
Version 03	State Effective	Effective Date 05-JUN-2020	Document ID 332012
Document Name MDS2 Form for Security		Product Family N/A	Change Order Number DCO-20-004

Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:53 PM UTC • Page 1 of 15

Manufacturer Disclosure Statement for Medical Device Security -- MDS2


Sway Medical 4.1.1 QR-2003-01 4-Apr-2020

Question ID	Question	Answer	See note
DOC-1	Manufacturer Name	Sway Medical	—
DOC-2	Device Description	Sway System	—
DOC-3	Device Model	4.1.1	—
DOC-4	Document ID	QR-2003-01	—
DOC-5	Manufacturer Contact Information	Sway Operations LLC 212 S. Front Street 76008, USA P: 855-792-9633	—
DOC-6	Intended use of device in network-connected environment:	<p>The Sway Balance 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. The Sway Balance software application is a classified as a Pre-amendment device, FDA product code LXV.</p> <p>The Sway Cognitive System is intended for use as a computerized cognitive assessment aid to be administered by a qualified health profession to assess cognitive function. The Sway Cognitive software application is classified as a Class II exempt device, FDA product code PKO.</p>	—
DOC-7	Document Release Date	4/4/2020	—
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	—	—
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	—	—
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	—
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	Yes	21
DOC-11.1	Does the SaMD contain an operating system?	No	—
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	Yes	—
DOC-11.3	Is the SaMD hosted by the manufacturer?	No	21
DOC-11.4	Is the SaMD hosted by the customer?	Yes	21


Yes, No, N/A, or See Note Note #

MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION

MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	1
--------	--	-----	---

		Category: Tier IV Labeling Title: QR-2003-01		
		QR-2003-01	4-Apr-2020	
Version	Does the device maintain personally identifiable information?	State Effective	Effective Date	Document ID
MPII-2	03	Yes	05-JUN-2020	332012
Document Name	Product Family	Change Order Number		
MDS2 Form for Security	N/A	DCO-20-004		
MPII-2.1	Does the device temporarily store personally identifiable information in volatile memory (e.g., RAM) until cleared by power-off or reset?	Yes	2	
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	No	—	
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	No	2	
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	—	
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	2	
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	No	—	
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	2	
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	N/A	—	
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	—	
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	No	—	
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	3	
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	No	—	
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)?	No	—	
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	—	
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	No	—	
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	Yes	2	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	2	
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	—	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	—	
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	—	

Management of Private Data notes:

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01 4-Apr-2020
Version 03	State Effective	Effective Date 05-JUN-2020	Document ID 332012	
Document Name AUTOMATIC LOGOFF (ALOF) MDS2 Form for Security		Product Family N/A	Change Order Number DCO-20-004	

Unauthorized users if device is left idle for a period of time. Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:53 PM UTC • Page 3 of 15

ALOF-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	---
ALOF-2	Is the length of inactivity time before auto-logout/screen lock user or administrator configurable?	No	---


AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the device.

AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	---	
AUDT-1.1	Does the audit log record a USER ID?	Yes	---	
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No	---	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	---	5
AUDT-2.1	Successful login/logout attempts?	Yes	---	5
AUDT-2.2	Unsuccessful login/logout attempts?	No	---	
AUDT-2.3	Modification of user privileges?	Yes	---	5
AUDT-2.4	Creation/modification/deletion of users?	Yes	---	5
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	No	---	
AUDT-2.6	Creation/modification/deletion of data?	Yes	---	5
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	N/A	---	
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	No	---	
AUDT-2.8.1	Remote or on-site support?	N/A	---	
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes	---	5
AUDT-2.9	Emergency access?	No	---	
AUDT-2.10	Other events (e.g., software updates)?	Yes	---	5
AUDT-2.11	Is the audit capability documented in more detail?	No	---	
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	---	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	No	---	
AUDT-4.1	Does the audit log record date/time?	Yes	---	
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	---	
AUDT-5	Can audit log content be exported?	Yes	---	
AUDT-5.1	Via physical media?	No	---	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	---	
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No	---	
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	Yes	---	
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	No	---	
AUDT-7	Are audit logs protected from modification?	Yes	---	
AUDT-7.1	Are audit logs protected from access?	Yes	---	
AUDT-8	Can audit logs be analyzed by the device?	No	---	

AUTHORIZATION (AUTH)

The ability of the device to determine the authorization of users.

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01	4-Apr-2020
Version 03	Does the device prevent access to unauthenticated users through user login requirements or other mechanisms?	State Effective		Effective Date 05-JUN-2020	Document ID 332012
AUTH-1		Yes			6
Document Name MDS2 Form for Security		Product Family N/A		Change Order Number DCO-20-004	

Can the device be configured to use federated credential management for users of other domains (e.g., LDAP, OAuth)?					
AUTH-1.1	Printed by: matthew.waddekin@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:53 PM UTC				Page 4 of 15
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No		—	
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No		—	
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes			7
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	No		—	
AUTH-4	Does the device authorize or control all API access requests?	Yes		—	
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	No		—	

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.

CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	See Notes			8
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	N/A		—	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A		—	
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A		—	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A		—	
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A		—	
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	N/A		—	
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A		—	
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A		—	
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A		—	
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A		—	
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	N/A		—	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A		—	

		Category: Tier IV Labeling Title: QR-2003-01			QR-2003-01	4-Apr-2020
Version	State	Effective Date	Document ID			
03	Effective	05-JUN-2020	332012			
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
Document Name MDS2 Form for Security		Product Family N/A		Change Order Number DCO-20-004		
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A		Printed by Matthew.Wadden@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:53 PM UTC • Page 5 of 15		
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	N/A				
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A				
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A				
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	N/A				
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A				
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A				
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	N/A				
CSUP-8	Does the device perform automatic installation of software updates?	N/A				
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	N/A				
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	N/A				
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	N/A				
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	N/A				
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	N/A				
CSUP-11.2	Is there an update review cycle for the device?	N/A				

HEALTH DATA DE-IDENTIFICATION (DIDT)

The ability of the device to directly remove information that allows identification of a person.

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01	4-Apr-2020
Version 03	State Effective	Effective Date 05-JUN-2020	Document ID 332012		
D1DT-1 Does the device provide an integral capability to de-identify personally identifiable information?	No	Product Family N/A	Change Order Number DCO-20-004		
D1DT-1.1 Does the device support de-identification profiles that comply with the DICOM standard for identification?	No	Product Family: N/A			

DATA BACKUP AND DISASTER RECOVERY (DTBK)

The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.

DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	Yes		9
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	Yes	—	
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	—	
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes		
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes		
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	—	

EMERGENCY ACCESS (EMRG)

The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.

EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	See Notes		10
--------	---	-----------	--	----

HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)

How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.


IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes		11
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes	—	

MALWARE DETECTION/PROTECTION (MLDP)

The ability of the device to effectively prevent, detect and remove malicious software (malware).

MLDP-1	Is the device capable of hosting executable software?	N/A	—	
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	N/A	—	
MLDP-2.1	Does the device include anti-malware software by default?	N/A	—	
MLDP-2.2	Does the device have anti-malware software available as an option?	N/A	—	

		Category: Tier IV Labeling Title: QR-2003-01			QR-2003-01	4-Apr-2020
Version	Document Name	State	Effective Date	Document ID		
03	Does the device documentation allow owner/operator to install or update anti-malware software?	Effective	05-JUN-2020	332012		
MLDP-2.3	MDS2 Form for Security	N/A	—	—		
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	N/A	—	—		
MLDP-2.5	Does notification of malware detection occur in the device user interface?	N/A	—	—		
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	N/A	—	—		
MLDP-2.7	Are malware notifications written to a log?	N/A	—	—		
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	N/A	—	—		
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	N/A	—	—		
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	N/A	—	—		
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	N/A	—	—		
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	—	—		
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	N/A	—	—		
<p>NODE AUTHENTICATION (NAUT) <i>The ability of the device to authenticate communication partners/nodes.</i></p>						
NAUT-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 (e.g. Web APIs, SMTP, SNMP)?	No	—	—		
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	N/A	—	—		
NAUT-2.1	Is the firewall ruleset documented and available for review?	N/A	—	—		
NAUT-3	Does the device use certificate-based network connection authentication?	N/A	—	—		
<p>CONNECTIVITY CAPABILITIES (CONN) <i>All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.</i></p>						
CONN-1	Does the device have hardware connectivity capabilities?	N/A	—	—		
CONN-1.1	Does the device support wireless connections?	Yes	—	—		
CONN-1.1.1	Does the device support Wi-Fi?	Yes	—	—		
CONN-1.1.2	Does the device support Bluetooth?	N/A	—	—		
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	Yes	—	—		
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	N/A	—	—		
CONN-1.2	Does the device support physical connections?	N/A	—	—		
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	N/A	—	—		

		Category: Tier IV Labeling Title: QR-2003-01			QR-2003-01	4-Apr-2020
CONN-1.2.2	Version 03	Does the device have available USB ports?	State Effective	N/A	Effective Date 05-JUN-2020	Document ID 332012
CONN-1.2.3	Document Name MDS2 Form for Security	Does the device require, use, or support removable memory devices?		Product Family N/A		Change Order Number DCO-20-004

CONN-1.2.4 Does the device support other physical connectivity? N/A
 Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? N/A
 CONN-2
 CONN-3 Can the device communicate with other systems within the customer environment? N/A
 CONN-4 Can the device communicate with other systems external to the customer environment (e.g., a service host)? N/A
 CONN-5 Does the device make or receive API calls? N/A
 CONN-6 Does the device require an internet connection for its intended use? N/A
 CONN-7 Does the device support Transport Layer Security (TLS)? N/A
 CONN-7.1 Is TLS configurable? N/A
 CONN-8 Does the device provide operator control functionality from a separate device (e.g., telemedicine)? N/A


PERSON AUTHENTICATION (PAUT)

The ability to configure the device to authenticate users.

PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes		12
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes		12
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	—	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	—	
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	—	
PAUT-5	Can all passwords be changed?	Yes	—	
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	—	
PAUT-7	Does the device support account passwords that expire periodically?	No	—	
PAUT-8	Does the device support multi-factor authentication?	No	—	
PAUT-9	Does the device support single sign-on (SSO)?	No	—	
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	—	
PAUT-11	Does the device support biometric controls?	No	—	
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	—	
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	Yes	—	
PAUT-14	Does the application or device store or manage authentication credentials?	Yes	—	
PAUT-14.1	Are credentials stored using a secure method?	Yes	—	

PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01	4-Apr-2020		
PLOK-1	Version 03	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	State Effective	Yes	Effective Date 05-JUN-2020	Document ID 332012	14
Document Name MDS2 Form for Security		Product Family N/A		Change Order Number DCO-20-004			

PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secured (i.e., cannot remove without tools)?	N/A	N/A	N/A	N/A	N/A	N/A
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	N/A	N/A	N/A	N/A	N/A	N/A
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	N/A	N/A	N/A	N/A	N/A	N/A

ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

Manufacturer's plans for security support of third-party components within the device's life cycle.

RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	Yes	—	—
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	Yes	—	15
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	Yes	—	—
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	Yes	—	—

SOFTWARE BILL OF MATERIALS (SBOM)


A Software Bill of Material (SBOM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.

SBOM-1	Is the SBOM for this product available?	Yes	Yes	—	—
SBOM-2	Does the SBOM follow a standard or common method in describing software components?	Yes	Yes	—	—
SBOM-2.1	Are the software components identified?	Yes	Yes	—	—
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	Yes	—	—
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	Yes	—	—
SBOM-2.4	Are any additional descriptive elements identified?	Yes	Yes	—	—
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	Yes	Yes	—	—
SBOM-4	Is there an update process for the SBOM?	Yes	Yes	—	—

SYSTEM AND APPLICATION HARDENING (SAHD)

The device's inherent resistance to cyber attacks and malware.

SAHD-1	Is the device hardened in accordance with any industry standards?	See Notes	See Notes	—	16
SAHD-2	Has the device received any cybersecurity certifications?	N/A	N/A	—	—
SAHD-3	Does the device employ any mechanisms for software integrity checking?	N/A	N/A	—	—
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	N/A	N/A	—	—

		Category: Tier IV Labeling Title: QR-2003-01		
		QR-2003-01	4-Apr-2020	
Version 03	State Effective		Effective Date 05-JUN-2020	Document ID 332012
Document Name MDS2 Form for Security		Product Family N/A	Change Order Number DCO-20-004	


Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 10 of 15

SAHD-3.2	Does the device employ any mechanism (e.g., hash key, checksums, digital signature) to ensure the software updates are the manufacturer-authorized updates?	N/A		
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	N/A		
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	N/A		
SAHD-5.1	Does the device provide role-based access controls?	N/A		
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	N/A		
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	N/A		
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	N/A		
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	N/A		
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	N/A		
SAHD-9	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		
SAHD-10	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		
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	N/A		
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	N/A		
SAHD-13	Does the product documentation include information on operational network security scanning by users?	N/A		
SAHD-14	Can the device be hardened beyond the default provided state?	N/A		
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A		
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	N/A		
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	N/A		

SECURITY GUIDANCE (SGUD)

Availability of security guidance for operator and administrator of the device and manufacturer sales and service.

SGUD-1	Does the device include security documentation for the owner/operator?	Yes		17
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	No		
SGUD-3	Are all access accounts documented?	Yes		
SGUD-3.1	Can the owner/operator manage password control for all accounts?	No		

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01	4-Apr-2020
Version 03	Does the product include documentation for the recommended compensating controls for the device?	State Effective Yes	Effective Date 05-JUN-2020	Document ID 332012	
SGUD-4	Document Name MDS2 Form for Security	Product Family N/A	—	Change Order Number DCO-20-004	

Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 11 of 15

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.

STCF-1	Can the device encrypt data at rest?	Yes		18
STCF-1.1	Is all data encrypted or otherwise protected?	Yes		
STCF-1.2	Is the data encryption capability configured by default?	Yes		
STCF-1.3	Are instructions available to the customer to configure encryption?	No		
STCF-2	Can the encryption keys be changed or configured?	No	—	
STCF-3	Is the data stored in a database located on the device?	Yes	—	
STCF-4	Is the data stored in a database external to the device?	Yes	—	

TRANSMISSION CONFIDENTIALITY (TXCF)

The ability of the device to ensure the confidentiality of transmitted personally identifiable information.


TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	—	
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes		19
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	N/A	—	
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	No	—	
TXCF-4	Are connections limited to authenticated systems?	Yes	—	
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	—	

TRANSMISSION INTEGRITY (TXIG)

The ability of the device to ensure the integrity of transmitted data.

TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes		20
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	—	

REMOTE SERVICE (RMOT)				
<i>Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.</i>				
RMOT-1	Does the device permit remote service connections for device analysis or repair?	N/A	—	
RMOT-1.1	Does the device allow the owner/operator to initiate remote service sessions for device analysis or repair?	N/A	—	
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A	—	

		Category: Tier IV Labeling Title: QR-2003-01 QR-2003-01 4-Apr-2020		
Version	State Effective	Effective Date	Document ID	
RMOT-1.3 03	Can patient data be accessed or viewed on the device during the remote session?	N/A	332012	
Document Name	Product Family	Change Order Number		
RMOT-2 MDS2 Form for Security	Does the device permit or use remote service connections for predictive maintenance data?	N/A	DCO-20-004	
RMOT-3	Does the device have any other remote service functionality (e.g. software updates, remote training)?	N/A	—	


Printed by: matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 12 of 15

OTHER SECURITY CONSIDERATIONS (OTHR)

NONE

Notes:

- Note 1: Sway collects and maintains the following ePHI (electronic Protected Health Information): First and Last Name, Data of Birth, Height, Weight, Age, results of balance tests, and results of cognitive tests.
- Note 2: The data is collected by the Sway application on the mobile device and transferred to the database via cellular data (e.g. iPhone or Android 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 a device logged out when an access token is revoked.
- Note 3: The Sway Application can display patient information when the user enters patient profile edit page.
- Note 4: Authentication timeouts on the portal are used to automatically log out inactive accounts in order to safeguard unattended data.
- Note 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, logging in or out, device info.
- Note 6: Access to Sway Application account is controlled with user ID (email address) and password.
- Note 7: Account administrator has ability to create users and assign them to groups.
- Note 8: Any patches or updates to the iOS or Android device are performed and maintained independently of the Sway Application. All updates to the Sway application can be applied as they become available in the App Store or Google Play Store.
- Note 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.
- Note 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 healthcare professional organization's procedures.

		Category: Tier IV Labeling Title: QR-2003-01		QR-2003-01	4-Apr-2020
Version 03	The integrity of the PHI data is assured through the use of SQL database in two main ways. One is the	State Effective	Effective Date 05-JUN-2020	Document ID 332012	
Document Name MDS2 Form for Security	functionality of the database management system provided by the vendor and its inherent security of the data; and second	Product Family N/A	Change Order Number DCO-20-004		

Printed by: matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 13 of 15

Note 11

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.

Access to Sway Application account is controlled with user id (email address) and password. Account Admin can create

Note 12

additional users and assign them to self-created groups. Each user has a unique ID (email address) and can access only the patient profiles withing the particular group. 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.

Note 13

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 not has access to users' passwords.

Note 14

Data on the device is temporarily stored in the internal memory of the device. Permament 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.

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

Note 15


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/>

Note 16

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.

		Category: Tier IV Labeling Title: QR-2003-01 QR-2003-01		4-Apr-2020
Version 03	Sway provides documentation on the security features including the MDS2 form and information on the MDS2 Form for Security Sway website.	State Effective	Effective Date 05-JUN-2020	Document ID 332012
Note 17	Document Name MDS2 Form for Security	Product Family N/A	Change Order Number DCO-20-004	

Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 14 of 15

Note 18

All data on the device is stored within a 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.

Note 19

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.

Note 20

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.

Note 21

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. The Sway application is a mobile application available on iOS and Android mobile devices.



Category: Tier IV Labeling
Title: QR-2003-01

Version 03	State Effective	Effective Date 05-JUN-2020	Document ID 332012
Document Name MDS2 Form for Security	Product Family N/A		Change Order Number DCO-20-004

Printed by matthew.waddell@swaymedical.com from app.zenqms.com on 24-Aug-2020 at 3:36:54 PM UTC • Page 15 of 15

REVISION HISTORY

Version 01 Effective on 23-Mar-2020

Initial Release - QSR-15-10 archived.

Version 02 Effective on 04-Apr-2020

Update for 4.1.1

Version 03 Effective on 05-Jun-2020

Updated so header on first page was legible

DOCUMENT ELECTRONIC SIGNATURES

DOCUMENT APPROVAL WORKFLOW

Author Approval

Bob Steurer

I am the author of this document.

Signed 8:07:19 PM UTC 05-Jun-2020