

Manufacturer Disclosure Statement for Medical Device Security – MDS ²			
DEVICE DESCRIPTION			
Device Category Programmable ambulation exoskeleton, clinical. GMDN: 58943	Manufacturer NextStep Robotics	Document ID MDS2-001	Document Release Date January 27th, 2025
Device Model AMBLE	Software Revision v1.0.0	Software Release Date February 28th, 2025 (est).	
Manufacturer or Representative Contact Information	Company Name NextStep Robotics Representative Name/Position Bryson Boettger/Project Manager	Manufacturer Contact Information 800 W Baltimore St., Suite 151 Baltimore, MD 21201 Tel: +1 (443) 869 - 3518	
Intended use of device in network-connected environment: The AMBLE device, a body-worn powered exerciser, is intended to restore ankle function during walking. AMBLE is designed to provide temporary, active external assistance to the ankle during walking in individuals who have impaired lower extremity function. AMBLE is a prescriptive device. Rehabilitation Providers must successfully complete a training program prior to operating the device.			
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)?	No 1
	B.2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	Yes 2
	B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes 3
	B.4	Open, unstructured text entered by device user/operator ?	Yes 4
	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)?	No
	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?	No
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 5
	D.2	Generate hardcopy reports or images containing private data ?	No
	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.)?	No
	D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes 6
	D.7	Import private data via scanning?	No
	D.8	Other?	No

Management of
Private Data notes:

- 1) Some demographic information, such as gender, age, condition, and date of onset of condition are optional fields on the Add Patient screen.
- 2) AMBLE requires a unique "Patient ID." This patient ID is able to be anything that the Provider wishes. We recommend that they use the patients' medical record # or similar ID used with other systems to ensure there is traceability, but that is up to the provider. Additionally, each time a therapy trial is completed, the completion date and time is saved.
- 3) Robot-data is saved with each trial. This includes output metrics such as trial duration, visit duration, number of steps, heel first strikes (%), Human Autonomy Index (custom metric), Assistive Torque, Peak Swing Angle, and Angle at Initial Contact
- 4) There are 2 spots that the Provider is able to add whatever free-text they wish. The Add Patient screen, and then the Report Card screen. These are simply to allow the Provider to add any relevant details that are kept on the Patients file, or specific to a therapy trial, that are not subsumed in the automatically collected data.
- 5) AMBLE is controlled via a iPad Application, and therefore the data (specifically Patient ID) is able to be viewed on the iPad display screen.
- 6) The information described earlier on the Add patient screen, as well as the therapy report card metrics, are transmitted via WiFi to NextStep Robotics secure cloud server.

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

Device Category Programmable ambulation exoskeleton, clinical. GMDN: 58943	Manufacturer NextStep Robotics	Document ID MDS2-001	Document Release Date January 27th, 2025
Device Model AMBLE	Software Revision v1.0.0	Software Release Date February 28th, 2025 (est).	

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	—
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
1-1.2	Can auto-logout/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user ?		Yes	2
ALOF notes:	1) The inactivity time is fixed to 5 minutes. 2) There is a "logout" button on all screens on the AMBLE Application which will log the user out at any point.			
2	AUDIT CONTROLS (AUDT)			
	The ability to reliably audit activity on the device .			
2-1	Can the medical device create an audit trail ?		Yes	1
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	2
2-2.4	Import/export of data from removable media		No	—
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection		Yes	3
2-2.5.1	Remote service activity		N/A	—
2-2.6	Other events? (describe in the notes section)		Yes	4
2-3	Indicate what information is used to identify individual events recorded in the audit log:			
2-3.1	User ID		Yes	5
2-3.2	Date/time		Yes	5
AUDT notes:	1) The medical device saves a record of each time the device is used for therapy. The information is saved on AMBLE's "Admin Portal" which is accessible by credentialed Providers. The information saved is primarily metrics calculated through the robot to indicate patient performance. Additional information that is saved is the Provider name, and the date/time that the "trial" was completed. 2) Each time a record is created or modified, the respective timestamp is stored in the AMBLE database. 3) The audit log only exists through a WiFi connection. If there is no WiFi connection, the trial information is not able to be saved (and thus no "Audit" log). 4) As mentioned in (1) above, the events that are saved are simply robot-calculated metrics and input parameters that were used for a specific therapy trial. These include: Trial Duration, Number of steps, Heel-first strikes (%), Peak Swing Angle, Angle at Initial Contact, Human Autonomy Index, Assistive Torque, etc. 5) The Patient ID, Provider Name, and date/time are recorded with each AMBLE trial (in addition to the metrics mentioned above).			
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	1
3-2	Can users be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular users , power users , administrators, etc.)?	No	2
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) To operate AMBLE, a Provider must be trained and given login credentials by a NextStep Robotics employee. Only then will they be able to login to the AMBLE App, and connect to the AMBLE device to perform therapy. 2) There is only one access level to operate AMBLE: "Provider"		

Device Category Programmable ambulation exoskeleton, clinical. GMDN: 58943	Manufacturer NextStep Robotics	Document ID MDS2-001	Document Release Date January 27th, 2025
Device Model AMBLE	Software Revision v1.0.0	Software Release Date February 28th, 2025 (est).	
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 1
CNFS notes:	1) The iPad in which the AMBLE App runs off is able to be configured to meet the needs of the user. For example, an iPad passcode may be added (and is encouraged) in addition to the Provider login on the App itself. NextStep Robotics controls most features on the iPad through a Mobile Device Management system (MDM).		
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 1
	5-1.1 Can security patches or other software be installed remotely?		Yes —
CSUP notes:	1) Both the iPad and the AMBLE App will require occasional updates. These can both be initiated remotely (but might require some user input to complete the action).		
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 1
DIDT notes:	1) The device does not provide a de-identification capability because there is no PHI required to operate AMBLE. Should the Provider decide to enter PHI through a free-text field, then that information would not be de-identified.		
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 1
DTBK notes:	1) There are currently no backup capabilities with AMBLE until it reaches the database. As a reminder, no data is stored locally on the iPad. If there is any interruption in the middle of a therapy trial (dead battery, Bluetooth disconnect, etc.) then that data would be lost. All of AMBLE's data is stored on a remote database, which has standard data backup and disaster recovery measures implemented.		
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 1
EMRG notes:	1) There is no emergency access feature to access AMBLE.		
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 1
IGAU notes:	1) AMBLE uses JSON web token based authorization so that there can be no unauthorized access to AMBLE's data. Additionally, AMBLE's backend sanitizes bad data as much as it can.		

the Healthcare Information and Management Systems Society.

Device Category	Manufacturer	Document ID	Document Release Date	
Programmable ambulation exoskeleton, clinical. GMDN: 58943	NextStep Robotics	MDS2-001	January 27th, 2025	
Device Model	Software Revision	Software Release Date		
AMBLE	v1.0.0	February 28th, 2025 (est).		
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)?		No	1
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) This is not necessary on an iPad and therefore is not implemented.			
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	1
NAUT notes:	1) As mentioned previously, AMBLE uses JSON web token based authorization so that there can be no unauthorized access to AMBLE's data.			
12 PERSON AUTHENTICATION (PAUT)				
Ability of the device to authenticate users				
12-1	Does the device support user/operator -specific username(s) and password(s) for at least one user ?		Yes	
12-1.1	Does the device support unique user/operator -specific IDs and passwords for multiple users?		Yes	1
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	2
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	3
12-7	Can the device be configured so that account passwords expire periodically?		No	
PAUT notes:	1) AMBLE both supports, and requires unique usernames/passwords for each user of the device within an organization. 2) The AMBLE App requires the user change the default password after their first login. 3) The complexity rules for user passwords on the AMBLE App are that they be 8 characters, with one capital letter and one number.			
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)?		N/A	—

PLOK
notes:

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

Device Category Programmable ambulation exoskeleton, clinical. GMDN: 58943	Manufacturer NextStep Robotics	Document ID MDS2-001	Document Release Date January 27th, 2025
Device Model AMBLE	Software Revision v1.0.0	Software Release Date February 28th, 2025 (est).	
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).	Yes	1
14-2	Is a list of other third party applications provided by the manufacturer available?	No	1
RDMP notes:	1) To access the web portal, any operating system that can support a browser such as Chrome or Safari is sufficient. For the AMBLE App, NextStep Robotics provides an iPad that has the required iPadOS version pre-installed. Currently, iPadOS 17.0 is the minimum required OS version to operate AMBLE.		
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	1
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	2
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?	No	3
15-10	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No	—
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	No	—
SAHD notes:	1) AMBLE uses Bluetooth to communicate with the Firmware, and WiFi to transmit trial data to AMBLE's database. 2) The organization has the ability to disable Provider access for individuals who are no longer responsible for operating the device 3) Most native iPad OS applications are disabled, however a few are still allowed such as the camera app, notes, clock, and translate apps, in case they can be supplemental for either AMBLE therapy or troubleshooting/diagnostics (ex: Taking a picture with the iPad of a hardware issue) . ANEESH/JOE: Should I delete all non-AMBLE Apps??		
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	1
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	—

1) AMBLE's User Guide provides details for basic security features such as logging in/out of the iPad App, resetting their password, etc.

SGUD notes:

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

Device Category Programmable ambulation exoskeleton, clinical. GMDN: 58943	Manufacturer NextStep Robotics	Document ID MDS2-001	Document Release Date January 27th, 2025
Device Model AMBLE	Software Revision v1.0.0	Software Release Date February 28th, 2025 (est).	
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 stored on device or removable media .			
17-1	Can the device encrypt data at rest?		Yes 1
STCF notes:	1) AMBLE does not store any information locally on the iPad at rest. However, AMBLE's database stores all of its data and it supports standard file-level encryption provided by AWS.		
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 1
18-3	Is private data transmission restricted to a fixed list of network destinations?		Yes 2
TXCF notes:	1) Data is encrypted via https SSL/TLS. 2) AMBLE's data is transmitted to an AWS EC2 server located in Virginia, USA.		
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 1
TXIG notes:	1) AMBLE uses https SSL/TLS encryption for transmitting data, which means it cannot be accessed or modified during transmission.		
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)?		No —
20-2.1	Can the device be configured to require the local user to accept or initiate remote access?		No —
OTHR notes:	AMBLE is currently not able to be serviced remotely.		