Restorative Therapies RTILink Database & System IT Information

RTILink Overview

RTILink is a database that resides on a server at www.RTILink.com (IP address: 69.89.6.226).

The purpose of RTILink is to:

- download patient therapy parameter data to the control unit interface (the controller for the device / ergometer)
- upload patient therapy result data from the control unit interface
- download automatic software updates to the control unit interface

RTILink is compliant with the HIPAA security rule.

Patients are identified by a seven-digit ID number including a 1-digit checksum) that is created when a new patient record is created in RTILink by a clinician. Only the clinician is able to match this RTILink ID with their actual patient.

System Interface Overview – The Device

The system interface for the device is a control unit, a tablet PC running Windows 10. The control unit is configured to run Restorative Therapies' proprietary software application upon startup which is hardcoded to only connect to RTILink or restorative-therapies.com. Users are not able to utilize the control unit for other Internet functions from within the application.

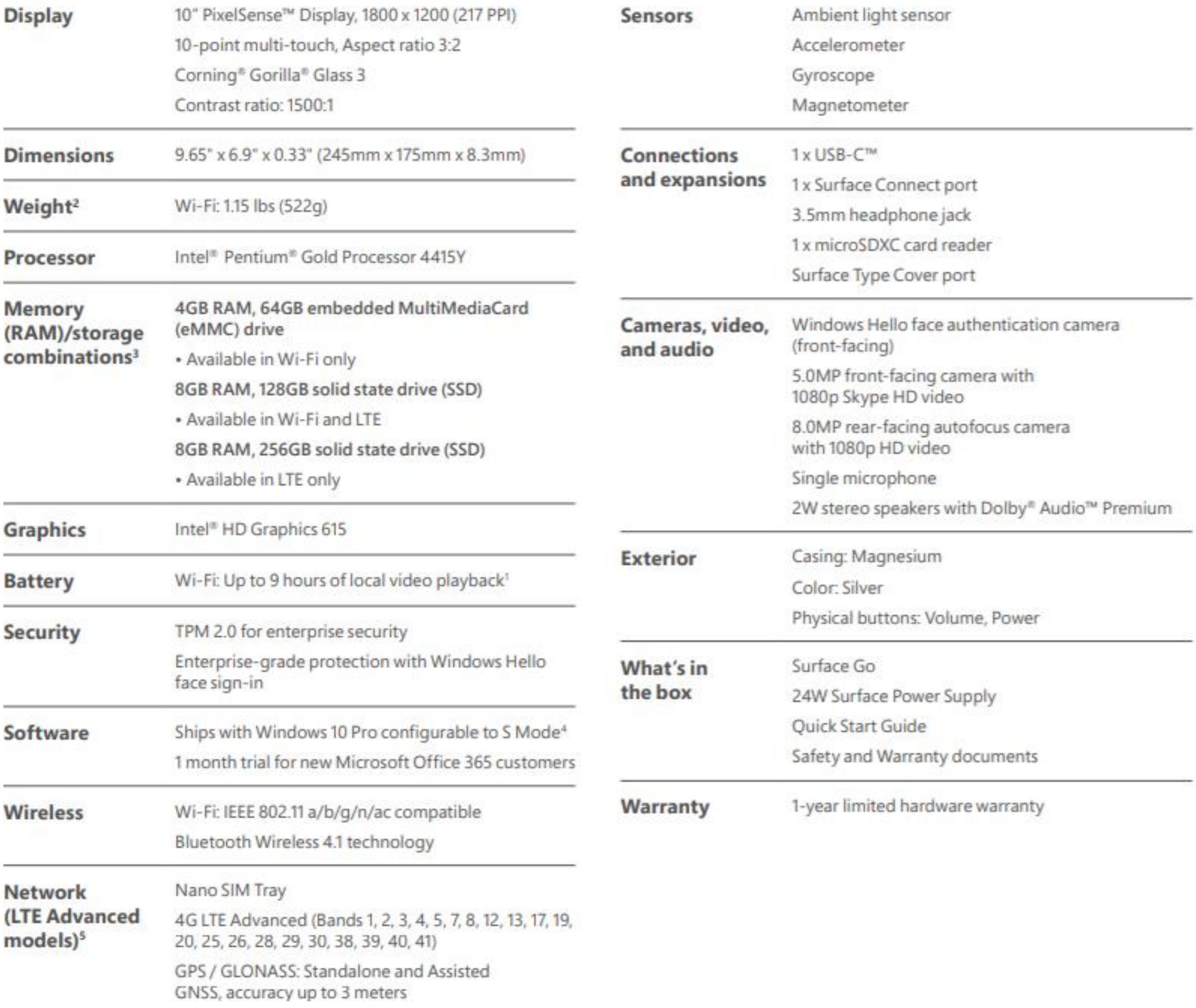
RT300 system

RT300 systems use a Microsoft Surface GO. It connects to the Internet via a WiFi network supporting 802.11 a/b/g/n.

The WiFi manager is capable of WEP, WPA, and WPA2 encryption. It can also be configured for a static IP connection, or a proxy server connection. 802.11 and 802.1x authentication methods are also supported using various methods of authentication such as PEAP and EAP.

The MAC address for the WiFi adapter is available from the SAGE software (Help | About).

RT300 system Control Unit Technical Specifications



Display	10" PixelSense™ Display, 1800 x 1200 (217 PPI) 10-point multi-touch, Aspect ratio 3:2 Corning® Gorilla® Glass 3 Contrast ratio: 1500:1
Dimensions	9.65" x 6.9" x 0.33" (245mm x 175mm x 8.3mm)
Weight[2]	Wi-Fi: 1.15 lbs (522g)
Processor	Intel® Pentium® Gold Processor 4415Y
Memory (RAM)/storage combinations[3]	**4GB RAM, 64GB embedded MultiMediaCard (eMMC) drive** • Available in Wi-Fi only **8GB RAM, 128GB solid state drive (SSD)** • Available in Wi-Fi and LTE **8GB RAM, 256GB solid state drive (SSD)** • Available in LTE only
Graphics	Intel® HD Graphics 615
Battery	Wi-Fi: Up to 9 hours of local video playback[1]
Security	TPM 2.0 for enterprise security Enterprise-grade protection with Windows Hello face sign-in
Software	Ships with Windows 10 Pro configurable to S Mode[4] 1 month trial for new Microsoft Office 365 customers
Wireless	Wi-Fi: IEEE 802.11 a/b/g/n/ac compatible Bluetooth Wireless 4.1 technology
Network (LTE Advanced models)[5]	Nano SIM Tray 4G LTE Advanced (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 19, 20, 25, 26, 28, 29, 30, 38, 39, 40, 41) GPS / GLONASS: Standalone and Assisted GNSS, accuracy up to 3 meters
Sensors	Ambient light sensor Accelerometer Gyroscope Magnetometer
Connections and expansions	1 x USB-C™ 1 x Surface Connect port 3.5mm headphone jack 1 x microSDXC card reader Surface Type Cover port
Cameras, video, and audio	Windows Hello face authentication camera (front-facing) 5.0MP front-facing camera with 1080p Skype HD video 8.0MP rear-facing autofocus camera with 1080p HD video Single microphone 2W stereo speakers with Dolby® Audio™ Premium
Exterior	Casing: Magnesium Color: Silver Physical buttons: Volume, Power
What's in the box	Surface Go 24W Surface Power Supply Quick Start Guide Safety and Warranty documents
Warranty	1-year limited hardware warranty

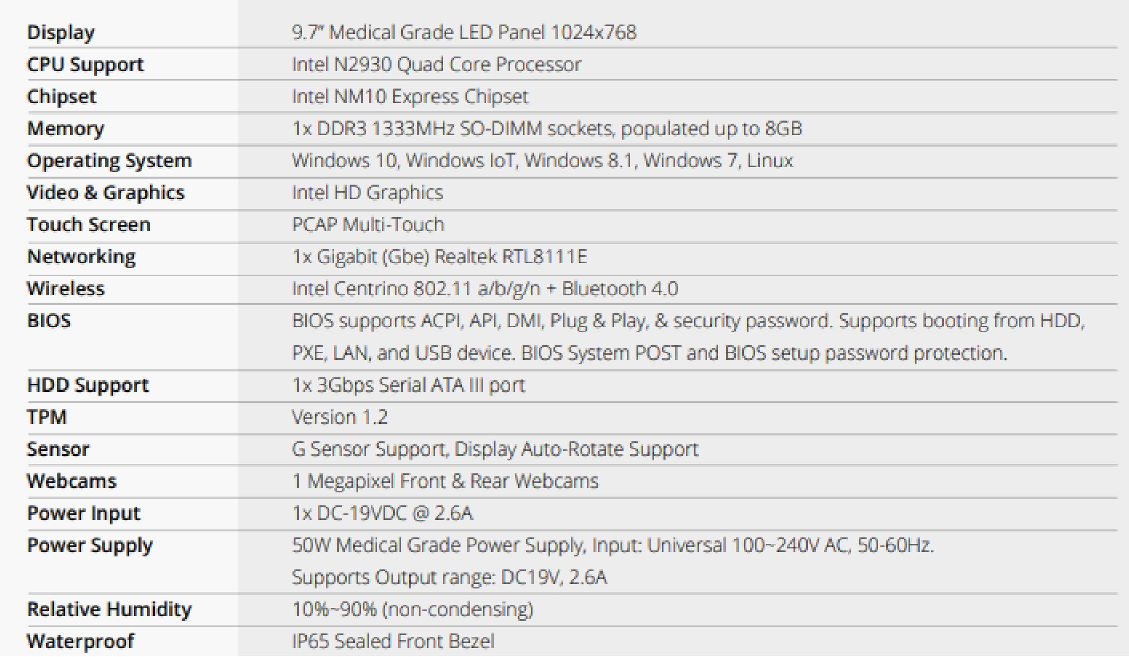
RT200, RT600, Xcite systems

RT200, RT600 and Xcite systems use a tablet pc manufactured by Cybernet Manufacturing, Model T10C. It connects to the Internet via a WiFi network supporting 802.11 a/b/g/n, or a wired LAN connection up to 1Gbps.

The WiFi manager is capable of WEP, WPA, and WPA2 encryption. It can also be configured for a static IP connection, or a proxy server connection. 802.11 and 802.1x authentication methods are also supported using various methods of authentication such as PEAP and EAP.

The MAC address for the WiFi adapter is available from the SAGE software (Help | About).

RT200, RT600, and Xcite systems Control Unit Technical Specifications



Display	9.7" Medical Grade LED Panel 1024x768
CPU Support	Intel N2930 Quad Core Processor
Chipset	Intel NM10 Express Chipset
Memory	1x DDR3 1333MHz SO-DIMM sockets, populated up to 8GB
Operating System	Windows 10, Windows IoT, Windows 8.1, Windows 7, Linux
Video & Graphics	Intel HD Graphics
Touch Screen	PCAP Multi-Touch
Networking	1x Gigabit (Gbe) Realtek RTL8111E
Wireless	Intel Centrino 802.11 a/b/g/n + Bluetooth 4.0
BIOS	BIOS supports ACPI, API, DMI, Plug & Play, & security password. Supports booting from HDD, PXE, LAN, and USB device. BIOS System POST and BIOS setup password protection.
HDD Support	1x 3Gbps Serial ATA III port
TPM	Version 1.2
Sensor	G Sensor Support, Display Auto-Rotate Support
Webcams	1 Megapixel Front & Rear Webcams
Power Input	1x DC-19VDC @ 2.6A
Power Supply	50W Medical Grade Power Supply, Input: Universal 100~240V AC, 50-60Hz. Supports Output range: DC19V, 2.6A
Relative Humidity	10%~90% (non-condensing)
Waterproof	IP65 Sealed Front Bezel

Internet Connection

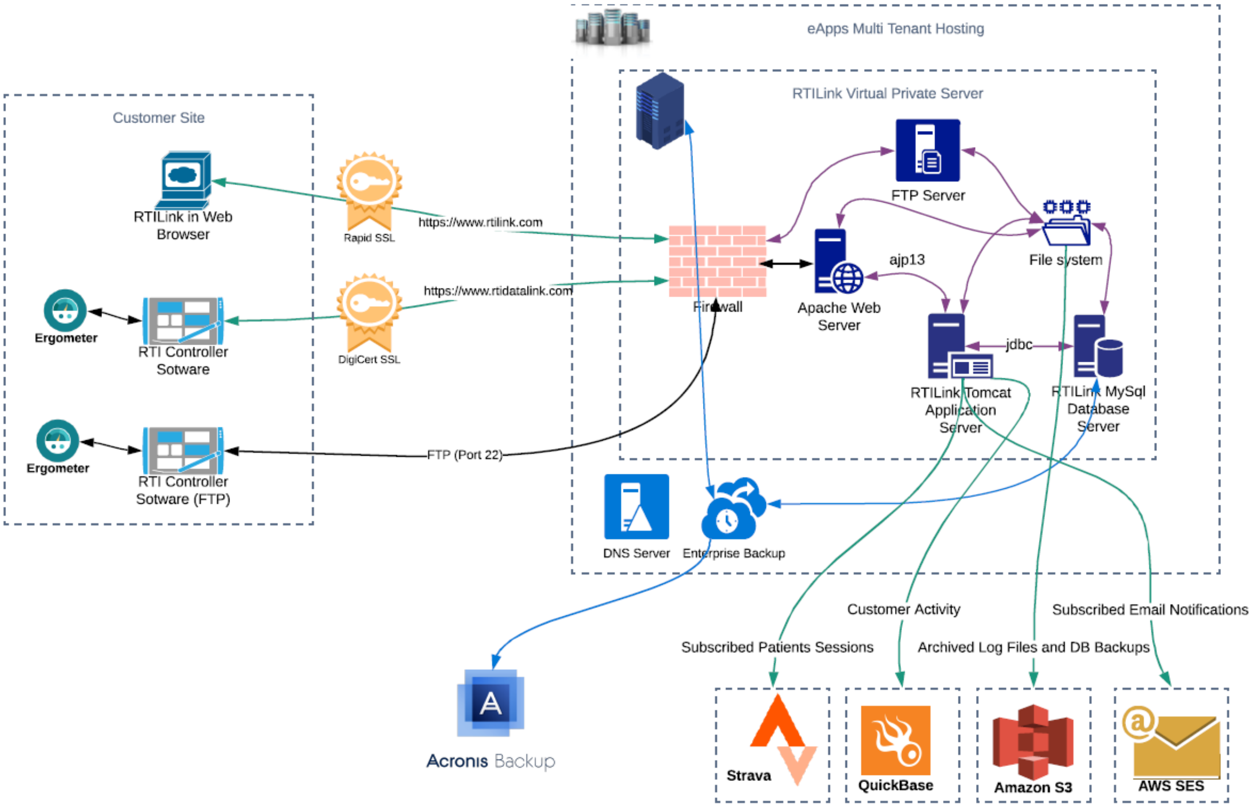
Overview

- The control unit communicates directly with the RTILink database across the internet – a connection to a facility's intranet is NOT necessary.
- The communication protocol for transmission of information is HTTPS.
- The control unit initiates all communications with RTILink.com.

Clinicians are able to log on to RTILink using a username and password to add, view or edit patient therapy settings and produce session and progress analysis reports. Two factor authentication using Google Authenticator or Microsoft Authenticator is available. This can be enforced as a clinic setting by the clinic administrator or used by individual clinicians.

The control unit can connect to a wireless network utilizing a hyperlink within the Restorative Therapies application to access the Windows 10 wireless manager. For RT300 systems, a USB-c to ethernet adapter can be used to achieve a hard-wired connection to the RTILink database.

Network Diagram and Data Flow



PHI

Below is a list of the 18 PHI identifiers and their status in RTILink.com. Note that RTILink.com provides a setting which can be optionally set for a clinic to prohibit storage of any identifying information (see column 3 in the table below). This provides Safe Harbor de-identification.

#	Identifier	RTILink.com	Can be prohibited
1	Names	Not stored	N/A
2	All geographical subdivisions smaller than a State	Not stored	N/A
3	All elements of dates (except year) for dates directly related to an individual	Birthdate can be entered into patient record	Yes
4	Phone numbers	Not stored	N/A
5	Fax numbers	Not stored	N/A
6	Email addresses	Email address can be entered into patient record. Required if patient is to receive progress Emails.	Yes
7	Social Security numbers	Not stored	N/A
8	Medical record numbers	MRNs can be entered into patient records as a means of cross referencing the RTILink.com ID number.	Yes
9	Health plan beneficiary numbers	Not stored	N/A

#	Identifier	RTILink.com	Can be prohibited
10	Account numbers	Not stored	N/A
11	Certificate/license numbers	Not stored	N/A
12	Vehicle identifiers and serial numbers	Not stored	N/A
13	Device identifiers and serial numbers	Only clinic device identifiers are stored as part of session data. These do not identify a patient.	N/A
14	Web Universal Resource Locators	Not stored	N/A
15	Internet Protocol (IP) address numbers	Not stored	N/A
16	Biometric identifiers	Not stored	N/A
17	Full face photographic images	Not stored	N/A
18	Any other unique identifying number, characteristic, or code	Not stored	N/A

Other Data

The following data is also maintained for each patient.

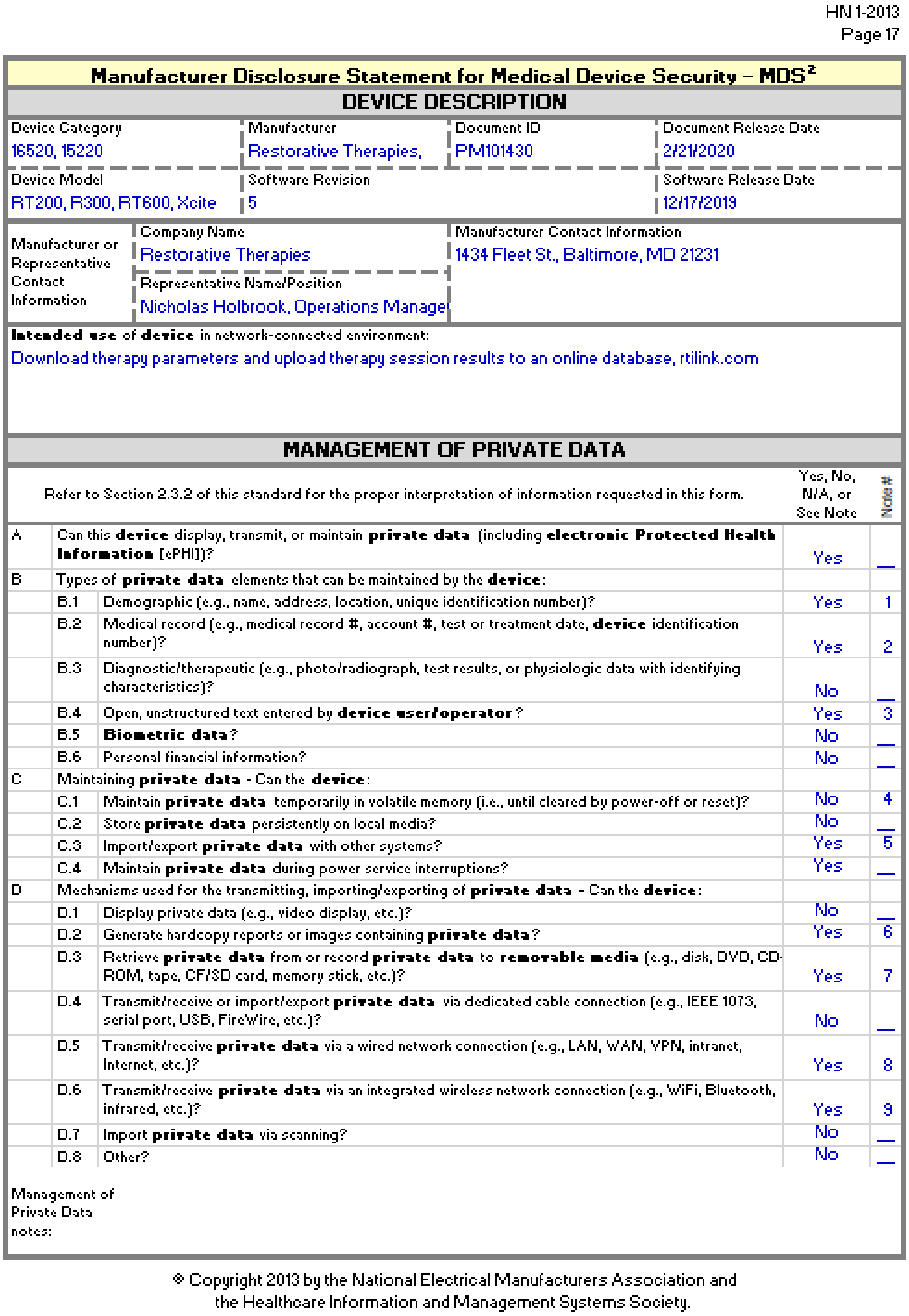
#	Data	Description
1	ID number	Seven-digit auto generated RTILink ID number (includes checksum) used to identify the patient within RTILink.
2	PIN number	Four digit PIN used to confirm the ID number when downloading a therapy. This defaults to patient month & year of birth if available (mmyy).
	Country	Country where the patient is using the system.
	Last used controller serial number	Serial number of the last system the patient used – in a clinic environment this will be a clinic system.
	Date privacy acknowledged	The date the patient acknowledged Restorative Therapies' privacy practices.
	Month & year born	Used to auto generate the PIN and set pediatric status. Can be prohibited (see item 3 in table above).
	Weight	Used to calculate MET minutes and for RT600 sessions.
	Pediatric	Used to set therapy defaults.
	Condition	Patient's condition can be selected from a list of conditions.
	Session efficiency	Used to calculate MET minutes. Set automatically in certain circumstances.
	Clinic	Clinic patient is attending.
	Prescribing clinic	Clinic that originally prescribed the system.
	2nd prescribing clinic	2nd clinic that prescribed the system.

#	Data	Description
	Clinician	Login of current clinician.
	2nd clinician	Login of 2nd clinician.
	Therapies	Table of therapy data for the patient. Patient can have multiple therapies. History of each therapy is maintained. An example is shown in Appendix B.
	Therapy results	Table of therapy result data for the patient. An example is shown in Appendix C.

Manufacturer disclosure statement

See manufacturer disclosure statement for medical device security in Appendix A.

Appendix A



Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category 16520, 15220	Manufacturer Restorative Therapies,	Document ID PM101430	Document Release Date 2/21/2020
Device Model RT200, R300, RT600, Xcite	Software Revision 5		Software Release Date 12/17/2019

Manufacturer or Representative Contact Information	Company Name Restorative Therapies	Manufacturer Contact Information 1434 Fleet St., Baltimore, MD 21231
	Representative Name/Position Nicholas Holbrook, Operations Manage	

Intended use of **device** in network-connected environment:
Download therapy parameters and upload therapy session results to an online database, rtilink.com

MANAGEMENT OF PRIVATE DATA

			Yes, No, N/A, or See Note	Note #
		Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		
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)?	Yes	2
	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**?	Yes	3
	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	4
	C.2	Store **private data** persistently on local media?	No	_
	C.3	Import/export **private data** with other systems?	Yes	5
	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.)?	No	_
	D.2	Generate hardcopy reports or images containing **private data**?	Yes	6
	D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	7
	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	8
	D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	9
	D.7	Import **private data** via scanning?	No	_
	D.8	Other?	No	_

Management of Private Data notes:

Device Category	Manufacturer	Document ID	Document Release Date
16520, 15220	Restorative Therapies,	PM101430	43882
Device Model	Software Revision		Software Release Date
RT200, R300, RT600, Xcite	5		43816

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-logoff, session lock, password protected screen saver)?		Yes	__
	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.)	Yes	__
	1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	No	__
ALOF notes:				
2	**AUDIT CONTROLS (AUDT)**			
	The ability to reliably audit activity on the **device**.			
2-1	Can the **medical device** create an **audit trail**?		Yes	10
2-2	Indicate which of the following events are recorded in the audit log:			
	2-2.1	Login/logout	Yes	__
	2-2.2	Display/presentation of data	No	__
	2-2.3	Creation/modification/deletion of data	Yes	__
	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	__
	2-2.5.1	**Remote service** activity	Yes	__
	2-2.6	Other events? (describe in the notes section)	No	__
2-3	Indicate what information is used to identify individual events recorded in the audit log:			
	2-3.1	**User** ID	Yes	__
	2-3.2	Date/time	Yes	__
AUDT notes:				
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	__
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	11
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:				

Device Category 16520, 15220	Manufacturer Restorative Therapies,	Document ID PM101430	Document Release Date 43882
Device Model RT200, R300, RT600, Xcite	Software Revision 5		Software Release Date 43816

	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?	Yes	__
	5-1.1 Can security patches or other software be installed remotely?	Yes	__
CSUP notes:			
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)** The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	Yes	12
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	13
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?	N/A	__
EMRG notes:			
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)** How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	14
IGAU notes:			

Device Category 16520, 15220	Manufacturer Restorative Therapies,	Document ID PM101430	Document Release Date 43882
Device Model RT200, R300, RT600, Xcite	Software Revision 5		Software Release Date 43816

			Yes, No, N/A, or See Note	Note #
		Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		
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)?	Yes	15
	10-1.1	Can the **user** independently re-configure **anti-malware** settings?	See Note	
	10-1.2	Does notification of **malware** detection occur in the **device user** interface?	See Note	
	10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	See Note	
10-2		Can the device owner install or update **anti-virus software**?	Yes	
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?	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**?	Yes	16
	12-1.1	Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	16
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?	Yes	
12-4		Can default passwords be changed at/prior to installation?	Yes	
12-5		Are any shared **user** IDs used in this system?	Yes	16
12-6		Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	
12-7		Can the **device** be configured so that account passwords expire periodically?	Yes	
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	
PLOK notes:				

Device Category 16520, 15220	Manufacturer Restorative Therapies,	Document ID PM101430	Document Release Date 43882
Device Model RT200, R300, RT600, Xcite	Software Revision 5		Software Release Date 43816

	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	__
14-2	Is a list of other third party applications provided by the manufacturer available?	See Note	__
RDMP notes:	O/S: Windows 10, Third party software: Logmein		
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?	Yes	17
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)?	N/A	18
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?	N/A	18
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	N/A	19
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	18
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	18
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?	Yes	
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	20
SGUD notes:			

Device Category 16520, 15220	Manufacturer Restorative Therapies,	Document ID PM101430	Document Release Date 43882
Device Model RT200, R300, RT600, Xcite	Software Revision 5		Software Release Date 43816

	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	21
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.)	Yes	__
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	__
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.)	Yes	__
TXIG notes:	SSL		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	Yes	__
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	Yes	__
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	Yes	__
OTHR notes:			

Notes:

1. RTILink.com assigns each patient a unique 7-digit number (includes a checksum)

2. A MRN can be entered as a cross reference. This and all identifying data can be prohibited as an option in the clinic settings.

Session dates are stored. The serial number of the device which the patient used is also stored.

3. The MRN number field is a text field.

4. The device does not store any identifying information. This is only stored in RTILink.com if allowed in clinic settings.

5. RTILink.com can export patient data to xls files or clinic systems if that function is established.

6. RTILink.com can provide printed reports of session data and therapy settings.

7. Recording to removable media in not possible from the device. Recording to removable media is not a function of RTILink.com however it would be possible for a user to save the reports or exported data (see 5 & 6 above) to removable data.

8. The device can connect to RTILink.com via wired network connection using SSL

9. The device can connect to RTILink.com via WiFi network connection using SSL

10. RTILink.com creates an audit trail, the device does not

11. At the clinic level RTILink.com supports users: patients, clinicians, clinic administrators

12. RTILink.com provides a clinic setting which prevents entry of any of the 18 patient identifiers and removes any that have already been entered

13. RTILink.com is continuously backed up. The device is not backed up, but patient therapy setting are uploaded to RTILink.com.

14 Communications between device and RTILink.com has guaranteed data accuracy

15 RTI does not install antivirus software since the device can only connect to RTILink.com. Clinic can optionally install antivirus software on the device

16 The device supports a single clinician login. RTILink.com supports multiple clinician login IDs and passwords.

17 Software updates incorporate checksums.

18 Clinicians have no access to device except via the provided application software

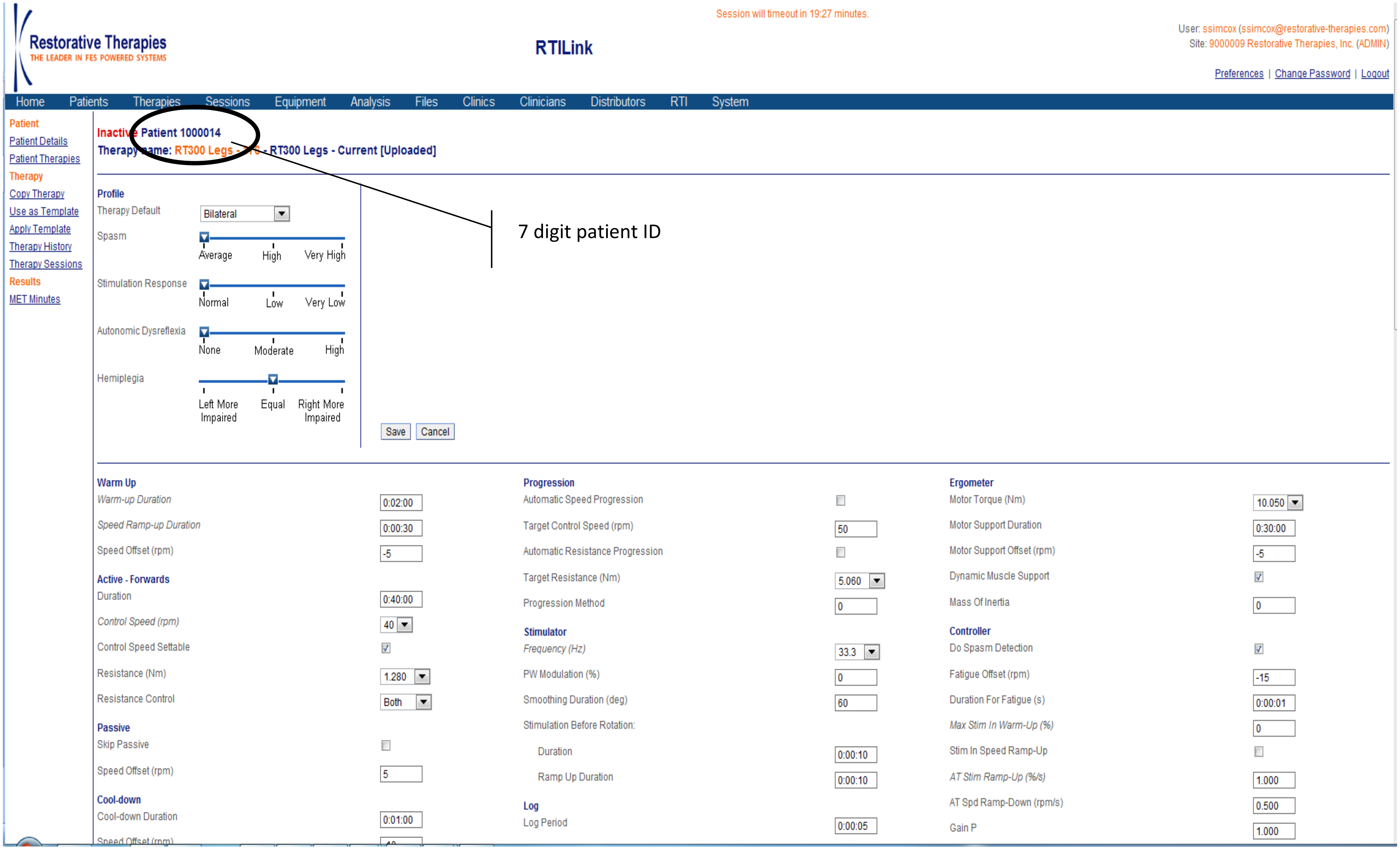
19 All ports on the device are open

20 All identifying information in RTILink.com can be erased via a clinic preference setting

21 Clinic device is encrypted. RTILink.com is encrypted at rest.

Appendix B

Example of therapy parameters shown on RTILink that are downloaded to the RT300 system controller.



7 digit patient ID

Session will timeout in 19:27 minutes.

Restorative Therapies
THE LEADER IN FES POWERED SYSTEMS

RTILink

User: ssimcox (ssimcox@restorative-therapies.com)
Site: 9000009 Restorative Therapies, Inc. (ADMIN)

Inactive Patient 1000014
Therapy name: RT300 Legs - [illegible] - RT300 Legs - Current [Uploaded]

Profile

Therapy Default	Bilateral
Spasm	[✓ Average] High Very High
Stimulation Response	[✓ Normal] Low Very Low
Autonomic Dysreflexia	[✓ None] Moderate High
Hemiplegia	Left More Impaired [✓ Equal] Right More Impaired

Warm Up

Warm-up Duration	0:02:00
Speed Ramp-up Duration	0:00:30
Speed Offset (rpm)	-5

Active - Forwards

Duration	0:40:00
Control Speed (rpm)	40
Control Speed Settable	☑
Resistance (Nm)	1.280
Resistance Control	Both

Passive

Skip Passive	☐
Speed Offset (rpm)	5

Cool-down

Cool-down Duration	0:01:00
Speed Offset (rpm)	

Progression

Automatic Speed Progression	☐
Target Control Speed (rpm)	50
Automatic Resistance Progression	☐
Target Resistance (Nm)	5.060
Progression Method	0

Stimulator

Frequency (Hz)	33.3
PW Modulation (%)	0
Smoothing Duration (deg)	60
Stimulation Before Rotation:	
Duration	0:00:10
Ramp Up Duration	0:00:10

Log

Log Period	0:00:05

Ergometer

Motor Torque (Nm)	10.050
Motor Support Duration	0:30:00
Motor Support Offset (rpm)	-5
Dynamic Muscle Support	☑
Mass Of Inertia	0

Controller

Do Spasm Detection	☑
Fatigue Offset (rpm)	-15
Duration For Fatigue (s)	0:00:01
Max Stim In Warm-Up (%)	0
Stim In Speed Ramp-Up	☐
AT Stim Ramp-Up (%/s)	1.000
AT Spd Ramp-Down (rpm/s)	0.500
Gain P	1.000

Appendix C

Example of therapy results that are uploaded to RTILink from the device controller.

Patient ID Session Date

1000014 2010-09-22_10-24-17

7 digit patient ID

SESSION DATA

Time(s)	Crank Velocity	Motor Velocity	Control/Target Speed	Power	Stimulation Level	Drive Torque	Resistance	Pulse	Saturation
1	0	0	45	0	0	9.983	0.5	-1	-1
5	0	0	45	0	0	9.983	0.5	-1	-1
6	3	5	45	0	0	9.983	2.525	-1	-1
10	6	6	45	0	0	9.983	2.525	-1	-1
15	12	13	45	0	0	9.983	2.525	-1	-1
20	17	20	45	0	0	9.983	2.525	-1	-1
25	22	26	45	0	0	9.983	2.525	-1	-1
30	29	33	45	0	0	9.983	2.525	-1	-1
35	35	40	45	0	0	9.983	2.525	-1	-1
40	36	40	45	0	0	9.983	0.5	-1	-1
45	40	40	45	0	0	9.983	0.5	-1	-1
50	41	40	45	0	0	9.983	0.5	-1	-1
55	37	40	45	0	0	9.983	2.525	-1	-1
60	37	40	45	0	0	9.983	2.525	-1	-1
65	37	40	45	0	0	9.983	2.525	-1	-1
66	37	45	45	0	0.993	9.983	2.525	-1	-1