SPACELABS HEALTHCARE
An OSI Systems Company

Qube (91390) Security Manual

P/N 070-3005-00 Rev. A | www.spacelabshealthcare.com

August 2020

OPERATIONS MANUAL

Spacelabs Healthcare considers itself responsible for the effects on safety, reliability and performance of the equipment only if:

- *assembly operations, re-adjustments, modifications or repairs are carried out by persons authorized by Spacelabs Healthcare, and*
- *the electrical installation of the relevant room complies with the requirements of the standard in force, and*
- *the equipment is used in accordance with the operations manual.*

In the event of a serious incident, notify Spacelabs and the competent authority of the EU Member State.

Spacelabs Healthcare will make available, on request, such circuit diagrams, component part lists, descriptions, calibration instructions or other information which will assist appropriately qualified technical personnel to repair those parts of the equipment which are classified by Spacelabs Healthcare as field repairable.

Spacelabs Healthcare is committed to providing comprehensive customer support beginning with your initial inquiry through purchase, training, and service for the life of your Spacelabs Healthcare equipment.

CORPORATE OFFICES

Corporate Headquarters

Spacelabs Healthcare, Inc.
35301 SE Center Street
Snoqualmie, WA 98065
U.S.A.
Telephone: (1) 800 287 7108
Telephone: (1) 425 396 3300

Authorized EC Representative

EC REP *MediMark® Europe. 11 rue E. Zola 38100 Grenoble. France*

- **Rx Only** U.S. Federal law restricts the devices documented herein to sale by or on the order of a physician.
- Before use, carefully read the instructions, including all warnings and cautions.

Table of Contents

This page is intentionally blank.

About This Manual

Overview

This manual provides instructions on how to use specific security features of the Qube®.

This manual have questions from the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form and the answers are specifically about the Qube bedside monitor. The sections that are not from the MDS2 are noted.

Read this manual before use and pay attention to all warnings and cautions.

Conventions used in this manual

Certain conventions are used throughout this manual for consistency and to aid in the search for information about the Qube bedside monitor

- Non-blue *italicized* typeface are references to information outside this manual. They indicate references to other manuals or information which is available in another form, as identified by a title or a part number.
- **Bold** typeface indicates text labels, phrases, or titles that show on an LCD or display which are part of a Spacelabs Healthcare software application.
- A non-bold term with Leading Capital Letters identifies the formal name of an icon, control, or view. These items do not include text as part of their identification, such as Home Screen, Patient View, or Setup Window.

- Numbered steps are presented to accomplish a task. Some steps conclude in a step result—unnumbered indented text. For an example of task steps, refer to Manually set the date and time on page 2-9.
- Warnings and cautions are included before pertinent content to alert you to important information on the use of the monitor Notes are placed after pertinent content. An example of each follows.

Warnings indicate potentially harmful conditions that can lead to injury or death.

Cautions indicate conditions that can lead to damage to or malfunction of the device.

Note:

Notes alert the user to relevant facts and conditions.

Qube Security

Qube (91390) Description

Spacelabs 91390 Qube® is a compact patient monitor with a 12-inch touchscreen that is well-suited for use in high acuity neonatal, pediatric and adult care, as well as perioperative environments. The Qube stores up to 96 hours of trends, and features remote viewing, Alarm Watch, and three user-selectable screen formats harmonized with Xprezzon® and Qube Mini to facilitate learning and navigation. With wireless networking and two batteries, Qube supports extended transport for up to eight hours. When deployed with the Spacelabs Xhibit® Central Station and Intesys® Clinical Suite, the Qube offers enterprise connectivity.

Figure 2-1: Qube - Front and Back

System Details

Component:	Details:
Hardware	Qube
Software version	3.08.00
OS version	VxWorks 6.6

Network

Connectivity:	Capable:
Wired	Yes
Wireless	Yes
Internet Ready	No
Bluetooth	No
Remote Access	No

Data Classification

Data Type	Process/ Display	Transmit	Store
Electronic Personal Health Information (ePHI)	Yes	Yes	Yes

Spacelabs 91390 Qube® is a compact patient monitor with a 12-inch touchscreen that is well-suited for use in high acuity neonatal, pediatric and adult care, as well as perioperative environments. Its clever design and compatibility with the Spacelabs Command Modules, Spacelabs Capnography Pod, and Exergen Temporal Artery Thermometer provide a versatile solution with a full range of measurement choices.

Qube stores up to 96 hours of trends, and features remote viewing, Alarm Watch, and three user-selectable screen formats harmonized with Xprezzon® and Qube Mini to facilitate learning and navigation. With wireless networking and two batteries, Qube supports extended transport for up to eight hours. When deployed with the Spacelabs Xhibit® Central Station and Intesys® Clinical Suite, Qube offers enterprise connectivity to your hospital

Electronic Medical Records (EMR), ECG management systems, paging systems, and remote access solutions.

Security and Privacy Controls for the Qube Monitor

Spacelabs provides its customers with capabilities to configure the Qube to meet their own security policies and requirements. The areas of responsibilities are shown below:

Security feature	Area of responsibility
	Customer
Authentication and Authorization	✓
Protection of Data in Transit	✓
Remote Access	**N/A**
Internal System Connection	✓
Protection of Data at Rest	**N/A**
Audit Event Logging	**N/A**
Time Stamps	✓
Secure Configuration Baseline	✓
Bug Reporting and Cybersecurity Product Updates	✓
Antivirus	**N/A**
Incident Response	✓

User Authentication and Authorization

Ability of the device to authenticate users and to determine the authorization of users.

#	Questions	Responses
1	Does the device support user/operator-specific username(s) and password(s) for at least one user?	Yes, see below*

#	Questions	Responses
2	Does the device support unique user/operator specific IDs and passwords for multiple user?	No
3	Can the device be configured to authenticate users through an external authentication service (example: MS Active Directory, NDS, LDAP, etc)?	No
4	Can the device be configured to lock out a user after a certain number of unsuccessful logon attempts?	N/A
5	Can default passwords be changed at/prior to installation?	Yes
6	Are any shared user IDs used in this system?	Yes
7	Can the device be configured to enforce creation user account passwords that meet established complexity rules?	No
8	Can the device be configured so that account passwords expire periodically?	No
9	Can the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes, see below*
10	Can users be assigned different privilege level within an application based on ‘roles’ (example: guest, regular users, power users, administrators, etc)?	Yes, see below*
11	Can the device owner/operator obtain unrestricted administrative privileges (example: access operating system or application via local root or admin account)?	No

*The device provides bedside monitoring information to healthcare staff and is intended to be operated in Kiosk mode, in an always on/functional mode - healthcare workers do not have to log on to get access to the monitor information. All elevated permissions functions (used to setup or configure the device) are not accessible in the unauthenticated Kiosk interface, but can be accessed via shared accounts for clinical, biomed, and service personnel. The password for the clinical and biomed accounts can be controlled by the Healthcare Organization.

Note:

- *Operating System (OS): OS level user accounts are not applicable on this device. This device has an embedded operating system which does not allow for usernames/passwords.*
- *Database: This device has no direct communication with Intesys Clinical Suite (ICS) and no user accounts.*

Device Group Roles

Level	Type	Use
0	Kiosk	Users can admit patients and view vitals No password
1	Clinical	Users can change some configuration items related to clinical settings. Refer to Operations Manual, 070-070-2112-04 Rev E) Change default password
2	Biomed/Clinical Engineers	Users can set device wide settings as well as change passwords for Biomed (Level 2) and/or Clinical (Level 1). Refer to Systems Administration Guide, 070-2380-03 Rev R. Change default password
3	Service – Spacelabs Field Service Engineers (FSEs)	Users can change licensure on the bedside monitor. Refer to the Qube Service Manual, 070-2451-04 Rev D. This is configured by Spacelabs Field Service Engineers (FSEs)

How to set up password for group roles:

- It is recommended that the default password be change prior to use. Each role can only change the password for that respective role and the roles below it.

  For example: a BIOMED user can change both a CLINICAL user and BIOMED user password, but not a SERVICE user password. The instructions for doing so are below:

  Once logged into the role for the password that requires changing, touch **Change Password** at the bottom of the screen and follow the prompts to change the password.

How to distribute password for group roles:

1. Distribution of passwords is left up to the customer.
2. The customer should follow the best practices implemented in its individual organization.

Protection of Data in Transit

The ability of the device to ensure the confidentiality and integrity of transmitted data

#	Questions	Responses
1	Can PII/ePHI data be transmitted only via a point-to-point dedicated cable?	No
2	Is PII/ePHI data encrypted prior to transmission via a network?	No
3	Is PII/ePHI data transmission restricted to a fixed list of network destinations?	Yes
4	Does the device support any mechanism intended to ensure data is not modified during transmission?	Yes

Wired Connectivity

Qube monitors use the IEEE 802.3 standard for communications. This device is not capable of encrypting data transmissions.

Note:

It is recommended that this device be placed on a separate VLAN for medical devices to limit network communication.

Wireless Connectivity

This device uses IEEE 802.11 Wireless communications. If wireless connectivity is used, the customer has an option to utilize WPA2 encryption for all data transmitted between the monitor and the associated wireless access point.

- It is recommended that this device be placed on a separate VLAN for medical devices to limit network communication.
- It is recommended that WPA2 encryption be used.

Remote Access

#	Questions	Responses
1	Can the device be serviced remotely?	No
2	Can the device restrict remote access to/from specified devices or users or network locations (specific IP addresses)?	Not Applicable

3	Can the device be configured to require the local user to accept or initiate remote access?	Not Applicable

Note:

Remote Service is not available for this device.

Internal Systems Connections

The questions in this section are not included on the MDS2 form.

Qube monitors can communicate with Xhibit Central Stations, so that nurses have multiple people watching over the patients and their vital signs. Qube bedside monitors can communicate with the ICS Monitor Loader to send the data to the database and even to the hospital's electronic medical records database.

#	Questions	Responses
1	Can this device connect to other Spacelabs products?	Yes
2	Can this device connect to other non-Spacelabs products?	No

Protection of Data at Rest

The device ability to ensure unauthorized access does not compromise the integrity and confidentiality of data stored on the device.

#	Questions	Responses
1	Can the device encrypt data at rest?	No
2	Are the device components maintaining PII/ePHI data physically secure (i.e. cannot be remove without tool?	Yes
3	Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes

This device cannot be encrypted during normal operations. The bedside monitor must be connected to a Command Module for the data to be viewable. Once a patient has been discharged from the monitor, that patient information will be removed from the device.

Audit Event Logging

The ability to reliably audit activity on the device is explained in section, Device Group Roles on page 2-5.

#	Questions	Responses
1	Can the device create an audit trail?	No
2	Indicate which of the following events are recorded in the audit log:	
2a	Login/Logout	Not Applicable

#	Questions	Responses
2b	Display/presentation of data	Not Applicable
2c	Creation/modification/deletion of data	Not Applicable
2d	Import/export of data from removable media	Not Applicable
2e	Receipt/transmission of data to/from external (example network) connection	Not Applicable
2f	Remote service activity (Remote Access)	Not Applicable
2g	Other events	Not Applicable
3	Indicate what information is used to identify events recorded in the audit log	
3a	User ID	Not Applicable
3b	Date/Time	Not Applicable
4	Can the device send event logs to a SEIM	Not Applicable

This device is capable of capturing patient vitals and trends; however, this device has no system event logging capabilities.

Time Stamps

The questions below are not included on the MDS2 form.

#	Questions	Responses
1	Does the medical device use an internal clock for time stamps?	Yes
2	Can the time stamps be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)?	Yes

If Intesys® Clinical Suite (ICS) has been purchased, all monitors will receive their time from the Monitor Loader component of ICS. This can be configured in the monitor itself. This process is done on the Monitor Loader component and will be discussed elsewhere (refer to 070-2922-00, ICS Security Manual).

If the monitors will not be connected to an ICS server, the date and time will have to be manually updated. The process is as follows:

Manually set the date and time

1. Log onto the BIOMED role on the device.
2. Click on the **Time/Date** Tab in the **Biomed Privileged Access** Menu.

Figure 2-2 Time/Date Tab

3 Touch the field that requires change.
4 Touch **Clear** on the keypad below the **Time and Date** fields.
5 Use the on-screen keypad to enter numbers.
6 Touch **Enter**.
7 The numbers selected will be entered in the field.
8 After any changes to the time, date, or selected to change the time display, touch **Update** to refresh the monitor.

Secure Configuration Baseline

The ability to configure/re-configure device security capabilities to meet user needs.

#	Questions	Responses
1	Can the device owner/operator/admin reconfigure product security features/capabilities?	Yes

Spacelabs customers are responsible for following their own Change Control Processes. Spacelab devices do not have the ability to auto-detect changes in configuration. Spacelabs recommends that after the device has been customized to the customer's requirements, a document should be created detailing that baseline. This baseline document can then be used for the device configuration testing.

Spacelabs customers can make changes to the following security features:

- BIOMED and CLINICIAN role password
- Secure WiFi connections

Security configuration (Recommended)

- Passwords: Spacelabs recommend that the default passwords be changed for the BIOMED and CLINICAL user roles. Spacelabs recommends using the industry best practices on password complexity and rotations.
- Network Security – Spacelabs recommends that Spacelabs devices be placed on its own separate VLAN behind the customers Firewall.
- WiFi Security: Spacelabs recommends only using secured WiFi networks, specifically WPA2 or greater
- This device is not internet ready and does not require access to the internet.
- This device has Domain Name System (DNS) services configured but have no internet configuration and do not interact with the internet. Domain Name System Security Extensions (DNSSEC) is not required.
- This device does not include an Intrusion Detection System (IDS) nor an Intrusion Prevention System (IPS). The customer can configure its respective IDS/IPS system to capture network activity on its device.

Ports, Protocols and Services

See table below:

Ports	Protocol	Service	Purpose	Source	Destination	Data Exchanged
51374 and specific offsets above [Port numbers calculated and set during configuration]	UDP Multicast – Spacelabs proprietary	Monitoring	Transport of physiological waveforms and configurations	Monitor (91390, 91393, 91389)	Other Spacelabs monitors, ICS Monitor loader (92810), Xhibit Central Station and XC4 (96102, 96501)	Patient physiological data (waveforms, alarms, etc.)
6105, 6106	TCP – Spacelabs proprietary	Communications (Genie)	Configuration of Spacelabs plug-in modules (e.g. Command Module)	Configuration PC	Monitor	Configuration settings
6105, 6106	TCP – Spacelabs proprietary	Communications (Genie)	Sharing monitor settings	Monitor (91390, 91393, 91389)	Monitor (91390, 91393, 91389)	Configuration settings
1494	TCP – Citrix ICA Spacelabs DNA client	Communication with Citrix Metaframe servers	Spacelabs DNA client – communication	Monitor (91390, 91393, 91389)	Customer Citrix Metaframe servers	Desktop remote access
80, 443	TCP-http and https	Spacelabs DNA client – browse for services	Communication with Citrix Metaframe servers	Monitor (91390, 91393, 91389)	Customer Citrix Metaframe servers	Location of server (IP address)
1023-65534	TCP-Citrix ICA	Spacelabs DNA client – communication	Communication with Citrix Metaframe servers	Monitor (91390, 91393, 91389)	Customer Citrix Metaframe servers	Desktop remote access
1604	UDP-Citrix ICA	Spacelabs DNA – browse for services	Communication with Citrix Metaframe servers	Monitor (91390, 91393, 91389)	Customer Citrix Metaframe servers	

Bug Reporting and Cybersecurity Product Updates

The ability of on-site service staff, remote service staff or authorized customer staff to install/upgrade device security patches. The ability to report security bugs or product defects.

#	Questions	Responses
1	Can relevant OS and device security patches be applied to the device as they become available?	Yes
2	Can security patches or other software be installed remotely?	No
3	Can product security bugs be reported?	Yes

Security Bugs/Defect Identification and Reporting

- Internal Spacelabs testing teams identified defects are forwarded to Spacelabs Research and Development for investigation, analysis, and remediations.
- Customer identified defects are reported to Spacelabs by calling Spacelabs Global Technical Support (GTS) via phone (800-522-7025), via email (techsupport@spacelabs.com) or via the Internet link (https://www.spacelabshealthcare.com/support/feedback-submission/)

Complaint management: Once a defect/complaint is received by Spacelabs, the GTS team will work with the customer to remedy the defect or issue reported. If GTS is unable to remedy the customer's issue, it will be escalated to "higher level escalation teams" who work on the defect/complaint in conjunction with Spacelabs Research and Development. The customer will be involved on an as needed basis.

Patch Updates and Process: Spacelabs customer will need to contact Spacelabs to schedule time for a Spacelabs FSE to come to the site to update the device.

Antivirus

The ability of the device to effectively prevent, detect and remove malicious software (such as malware, virus, etc…)

#	Questions	Responses
1	Does the device support the use of anti-virus software?	No
2	Can the user independently re-configure anti-virus settings?	N/A
3	Does notification of virus/malware detection occur in the device interface?	N/A

#	Questions	Responses
4	Can only manufacturer-authorized persons repair systems when virus/malware has been detected?	N/A
5	Can the device owner install or update anti-virus software?	No
6	Can the device owner/operator (technically/physically) update virus definitions on manufacturer-install anti-virus software?	N/A

Note:

This device does not support antivirus software.

Incident Response

#	Questions	Responses
1	Does the manufacturer provide support to investigate security incidents involving the device?	Yes

Customer can report security incidents by calling into Spacelabs Global Technical Support (GTS):

- Via phone at 800-522-7025;
- Via email at techsupport@spacelabs.com; and/or
- Via the internet at https://www.spacelabshealthcare.com/support/feedback-submission/

Once the incident is received, Spacelabs will investigate and prioritize appropriately.

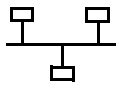
Appendix G — Symbols

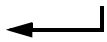
The following list of international and safety symbols describes all symbols used on Spacelabs Healthcare products. No one product contains every symbol.

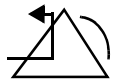
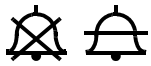
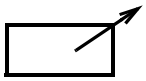
Note:

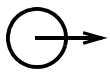
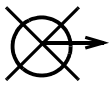
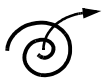
Graphic elements of certain keys and symbols may vary between product lines.

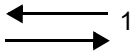
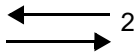
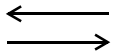
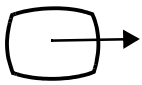
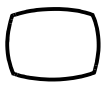
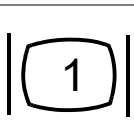
	HELP Key
?	HELP (Explain Prior Screen) Key
	MONITOR SETUP Key
	REMOTE Key

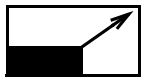
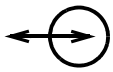
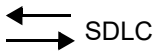
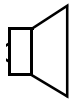
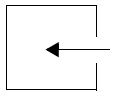
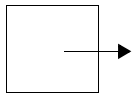
	TRENDS Key
	RECORD Key
	SPECIAL FUNCTIONS Key
	NORMAL SCREEN Key
	SAVE Key
	No Network Connection
	Network Connection
	Do Not Connect to Network
	No Connection to Intesys® Clinical Suite (ICS)
	Compression
	Magnifying Glass
	File Cabinet

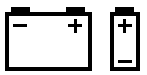
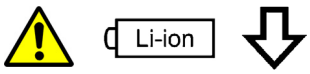
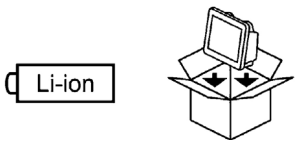
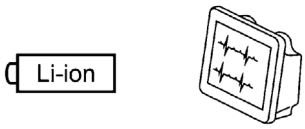
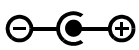
	List of Rooms
	Printer
	Service Message
 	PREVIOUS MENU Key
	HOME Key
 	Arrows
	STANDBY Key Power ON/OFF Key
	ENTER Key
	Delete
	Nurse Alert Interface
	ALARM SUSPEND/TONE RESET Key
	ALARMS Key
	Alarm, General

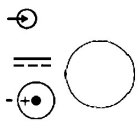
	Alarm Reset
	Alarm Audio ON
	Alarm Audio OFF
	Alarm Audio Paused
	Alarm Indicator. On the display, the color of the symbol designates the priority of the alarm: • cyan = low • yellow = medium • red = high On monitor hardware, this symbol indicates Alarm Output.
	Alarms Paused
	Alarm OFF or equipment has no alarm system
---	Parameter below measurement range
+++	Parameter above measurement range
???	Parameter measurement indeterminate
	Indicator — Remote Control
	Normal Screen
	Clock/Time Setting Key
	Slow Run
	Activate Recorder for Graphics

	Reset
	START (NIBP) Key
	Power Indicator LED
	Activate Telemetry Recorder
	Output (Non-terminated)
	Data Input/Output
	Input
	No Output (Terminated)
	Indicator — Local Control
	Indicator — Out of Paper
	Recorder Paper
	Menu Keys
	Waveform/Parameter Keys
	Return to Prior Menu
	Monitor Setup Select Program Options

	Set Initial Conditions Menu
	Access Special Function Menu
	Return Unit to Monitor Mode
	Keypad
	Serial Port 1
	Serial Port 2
	Serial Port
	Auto Mode (NIBP)
	External Marker Push Button Connection
	Arterial Pulse
	Gas Exhaust
	Video Output
	Television; Video Display
	Video Output, Primary
	Video Output, Secondary

	Enlarge, Zoom
	Input/Output
	PCMCIA Card
	Touchscreen, External
	Universal Serial Bus
 SDLC	SDLC Port
	Hard Drive
	Antenna
	Electrocardiograph or Defibrillator Synchronization
	Foot Switch
	Audio Output, Speaker
	Event
	Gas Sampling Port
	Gas Return Port

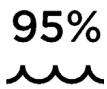
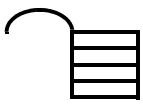
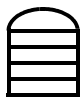
	Battery Replace only with the appropriate battery.
	Battery Status
	Battery Replace only with the appropriate battery.
	Low Battery
	Replace only with the appropriate battery. (+ / - signs may be reversed)
	Check battery switch on bottom of unit.
	Battery off. Shipping and service mode.
	Battery on. Regular operating mode.
	All batteries should be disposed of properly to protect the environment. Lithium batteries should be fully discharged before disposal. Batteries such as lead-acid (Pb) and nickel-cadmium (Ni-Cd) must be recycled. Please follow your internal procedures and or local (provincial) laws regarding disposal or recycling.
	This symbol indicates that the waste of electrical and electronic equipment *must not* be disposed as unsorted municipal waste and must be collected separately. Please contact an authorized representative of the manufacturer for information concerning the decommissioning of your equipment.
	Caution - hazardous voltages. To reduce risk of electric shock, do not remove the cover or back. Refer servicing to a qualified field service engineer (U.S.A.). DANGER - High Voltage (International)
	Protective Earth Ground
	Replace Fuse Only as Marked
	Power supply jack polarity. (+ / - signs may be reversed)

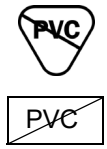
	Alternating Current
	Both Direct and Alternating Current
	Functional Earth Ground
	Fuse
	Equipotentiality Terminal
	Direct Current
	Input Power. Use only Spacelabs Power Supply.
	AC/DC Input
	Loop Filter
	Audio Output, Speaker
	IEC 60601-1 Type B equipment. The unit displaying this symbol contains an adequate degree of protection against electric shock.
	IEC 60601-1 Type BF equipment which is defibrillator-proof. The unit displaying this symbol is an F-type isolated (floating) patient-applied part which contains an adequate degree of protection against electric shock, and is defibrillator-proof.
	IEC 60601-1 Type BF equipment. The unit displaying this symbol is an F-type isolated (floating) patient-applied part providing an adequate degree of protection against electric shock.
	IEC 60601-1 Type CF equipment. The unit displaying this symbol is an F-type isolated (floating) patient-applied part providing a high degree of protection against electric shock, and is defibrillator-proof.

	IEC 60601-1 Type CF equipment. The unit displaying this symbol is an F-type isolated (floating) patient-applied part providing a high degree of protection against electric shock.
	IEC 60601-1 Class II equipment, double-isolated. The unit displaying this symbol does not require a grounded outlet.
	Warning: Do not modify this equipment without authorization of the manufacturer.
	Operates on Non-Harmonized Radio Frequencies in Europe
	Adult Noninvasive Blood Pressure (NIBP)
	Fetal Monitor Connection (Analog)
	Fetal Monitor Connection RS-232 (Digital)
	Physiological Monitor Connection RS-232 (Digital)
	Noninvasive Blood Pressure (NIBP), Neonate
	Symbol Set, Adult/Pediatric Cuff Sizes
	Symbol Set, Neonatal Cuff Sizes
	NIBP Cuff, Neonatal 1
	NIBP Cuff, Neonatal 2
	NIBP Cuff, Neonatal 3
	NIBP Cuff, Neonatal 4

	NIBP Cuff, Neonatal 5
	NIBP Cuff, Single Hose
	NIBP Cuff, Dual Hose
THIS SIDE TO PATIENT	NIBP Cuff, Surface Applied to Patient
CHILD	NIBP Cuff, Child Size (12 to 19 cm)
CHILD, LONG	NIBP Cuff, Child Size, Long (12 to 19 cm)
SMALL ADULT, LONG	NIBP Cuff, Small Adult Size, Long (17 to 25 cm)
SMALL ADULT	NIBP Cuff, Small Adult Size (17 to 25 cm)
ADULT, LONG	NIBP Cuff, Adult Size, Long (23 to 33 cm)
LARGE ADULT, LONG	NIBP Cuff, Large Adult Size, Long (31 to 40 cm)
LARGE ADULT	NIBP Cuff, Large Adult Size (31 to 40 cm)
ADULT	NIBP Cuff, Adult Size (23 to 33 cm)
INFANT	NIBP Cuff, Infant Size (8 to 13 cm)
NEONATAL 1	NIBP Cuff, Neonatal 1 Size (3 to 6 cm)
NEONATAL 2	NIBP Cuff, Neonatal 2 Size (4 to 8 cm)
NEONATAL 3	NIBP Cuff, Neonatal 3 Size (6 to 11 cm)

NEONATAL 4	NIBP Cuff, Neonatal 4 Size (7 to 13 cm)
NEONATAL 5	NIBP Cuff, Neonatal 5 Size (8 to 15 cm)
THIGH	NIBP Cuff, Thigh Size (38-50 cm)
NYLON	NIBP Cuff, Nylon Material
SOFT	NIBP Cuff, Soft Material
VINYL	NIBP Cuff, Vinyl Material
QTY	Quantity
ARTERY	Place Artery Symbol and Arrow over Brachial or Femoral Artery
	eIFU = electronic Instructions for Use (CD-ROM or website) is available
	Consult Instructions For Use
	Follow Instructions For Use
	Warning—Potential danger to patient or user (consult accompanying documents)
	Caution—Potential damage to equipment (consult accompanying documents)
Note	Note
	Keep Dry

	Indoor Use Only
	Altitude Limit
	Temperature Range
	Fragile, handle with care
	Handle with Care
	This Way Up
	Up Arrow
	Down Arrow
	Humidity Limit
	Humidity limitation
	Atmospheric pressure limitation
	Open Padlock
	Closed Padlock

	PVC-Free (Polyvinyl Chloride)
	Do Not Reuse; Single Use Only
	Single patient - multiple use
	Reusable
IPX1	Drip-Proof
IPX7	Unit can withstand accidental immersion in one meter of water for up to 30 minutes
REF	Catalog Number or Order Number
MD	Medical Device
	Use by date [YYYY-MM-DD]
	Recycle
	Non Sterile
	Latex Free – Not made with natural rubber latex
	Contains latex

	Does not contain phthalates
	Contains or presence of phthalates, such as DEHP
	Date of Manufacture
	Manufacturer
	Radio transmitting device; elevated levels of non-ionizing radiation
	A CE mark certifies that a product has met EU health, safety, and environmental requirements, which ensure consumer safety.
	XXXX is the European Notified Body number. 0123 is the number for TÜV SÜD Product Service GmbH, München, Germany.
	Canadian Standards Association Approved
	Does not contain hazardous substances — Europe
	Does not contain hazardous substances — China
	Batch Code
	Nellcor Oxisensor II Compatible
	Novametrix Compatible
	Spacelabs TruLink Compatible
	Nellcor OxiMax Compatible

	Spacelabs Compatible
	UL certified for use in the United States and Canada
	UL recognized component in Canada and United States
	Nellcor OxiMax Compatible
	Masimo SET Compatible

ABBREVIATIONS USED AS SYMBOLS ARE SHOWN BELOW.

1 - 32	Access Codes 1 Through 32
AIR	Air
A	Amperes
ANT 1 **ANT 2**	Diversity Antenna System 1 Diversity Antenna System 2
Arr1 **ArrNet2**	Arrhythmia Net 1 Arrhythmia Net 2
avDO$_2$	Arterial/Venous Oxygen Difference
CaO$_2$	Arterial Oxygen
CH **ch**	EEG, EMG, or ECG Channel EEG Channels - CH1, CH2, CH3, CH4 EMG Channel - CH5
cmH$_2$O	Centimeters of Water
C.O. **CO**	Cardiac Output
CvO$_2$	Venous Oxygen
CO2 **CO$_2$**	Carbon Dioxide

DIA **dia**	Diastolic
ECG **ecg**	Electrocardiogram
EEG **eeg**	Electroencephalogram
EMG **emg**	Electromyogram
ESIS	Electrosurgical Interference Suppression
EXT	External
FECG	Fetal Electrocardiogram
FHR1 **FHR2**	Fetal Heart Rate, Channel 1 Fetal Heart Rate, Channel 2
GND **gnd**	Ground
Hz	Hertz
Hgb	Hemoglobin
HLO **hlo**	High-Level Output
Multiview	Multi-Lead Electrocardiogram
N_2O	Nitrous Oxide
NIBP **nibp**	Noninvasive Blood Pressure
O_2AV	Oxygen Availability
O_2	Oxygen
PaO_2	Partial Pressure of Arterial Oxygen
PRESS **press** **PRS**	Pressure
PvO_2	Partial Pressure of Mixed Venous Oxygen
Ref.	Oxygen reference gas port
RESP **resp**	Respiration
SDLC	Synchronous Data Link Control

SN	Serial number
OPTIONS	Option
SVO2 SvO2 $S\bar{v}O_2$	Mixed Venous Oxygen Saturation
SYS sys	Systolic
T1 T2 T3 T4	Temperature 1 Temperature 2 Temperature 3 Temperature 4
TEMP temp	Temperature
UA	Uterine Activity or Umbilical Artery
UV	Umbilical Venous
VAC	Vacuum Connection
VO_2	Oxygen Consumption
V	Volts
W	Watts