Physio-Control

# Security Information for the LIFEPAK® 12 Defibrillator/Monitor Series

This information about security features of the LIFEPAK 12 defibrillator/monitor series is provided to help our customers comply with the HIPAA[1] Security Standards by their compliance date. This information applies to software versions 3011371-**095** and above (with **095** or higher as the last three digits). The software version is displayed onscreen when the device is first turned on and is printed at the bottom of the strip chart recording.

Physio-Control engaged an independent security expert to help us proactively assess the LIFEPAK products we currently market with respect to the standards and implementation specifications of the Security Rule. The following security information describes the security features and potential risks we have identified as a result of our assessment. In addition, it identifies possible administrative, physical and technical safeguards to help you, as a Covered Entity, establish process and procedures for use of the Physio-Control products that are reasonable and appropriate for your institution.

Understanding the device capabilities, using its security features and implementing recommended procedures can assist you in safeguarding electronic patient data as you use the LIFEPAK 12 defibrillator/monitor in cardiac emergencies and transmit data to treatment teams. This information is not intended as an exhaustive list of recommendations. Your organization's particular needs and security requirements may call for additional actions and controls.

## Product Use/Technical Features

The LIFEPAK 12 defibrillator/monitor series is an acute cardiac care response system used by authorized healthcare providers in and out of the hospital. Created for emergency medical services and hospital teams, the device provides multi-parameter therapeutic and diagnostic functions in a single, portable device.

The operating system that supports the device is Vx Works®.

## Patient Data

### Data recording

The LIFEPAK 12 defibrillator creates an electronic Patient Record, which may contain patient-specific data, including ECG and other monitored parameters and therapy events such as defibrillation and pacing. Each Patient Record contains the device serial number and date and time of use. Product options permit the operator to add the patient's name, identification number, age and gender to the Patient Record.

### Data storage

Up to 50 Patient Records are stored in the unit's archives. After the limit is reached, the records will be overwritten. The device record storage media uses flash RAM.

### Data retrieval

Once patient care is completed and the product is powered off, the Patient Record is archived within the LIFEPAK 12 defibrillator. With software versions 3011371-**095** and higher, the device can be set to restrict access to archived Patient Records by requiring a passcode. The operating manual includes instructions for setting a passcode—a static token consisting of four user-defined digits.

1. Health Insurance Portability and Accountability Act of 1996, 45 CFR Part 164.

### Data transmission

For patient care or data archiving purposes, data may be transferred from the LIFEPAK 12 defibrillator to a computer running Physio-Control medical informatics software, such as the LIFENET® RS receiving station, LIFENET EMS or CODE-STAT™ Suite. Patient Records can be transmitted from the LIFEPAK 12 defibrillator using cellular phone modems, analog phone modems, wireless connections or serial connections.

The LIFENET BLUE product option uses Bluetooth® encryption technology, which helps protect electronic patient data during wireless transmission from the LIFEPAK 12 defibrillator to a cell phone or directly to a computer running medical informatics software.

## Potential Security Exposures

Examples of possible risks to electronic patient data include:

- Accidental deletion before Patient Records are backed up
- Unintentional disclosure during servicing of the device
- Improper disclosure due to unauthorized employee access to archived Patient Records
- Improper disclosure or loss of Patient Records resulting from theft of the device

## LIFEPAK 12 Defibrillator Security Features

These security features and recommended procedures for proper use of the defibrillator/monitor are intended to facilitate your HIPAA security compliance efforts.

### Administrative Safeguards

| HIPAA Standard | Security Issue and Feature | Recommended Action |
|---|---|---|
| Information Access Management (to implement policies and procedures authorizing access to electronic patient data) | For each device use, the defibrillator maintains a Patient Record that includes the device serial number and date and time of use. The healthcare provider has the option of adding patient name, age, gender and identification number. | To help prevent improper disclosure or loss of electronic patient data, implement procedures to delete the Patient Record from the device after each use and when the Patient Record has been downloaded to backup storage.<br>To help prevent improper disclosure of electronic patient data, have servicing performed only by personnel trained in handling protected health information. |
| Contingency Plan (to respond to an occurrence that damages systems containing electronic patient data) | Medtronic's CODE-STAT Suite medical informatics system can be used to support backup and recovery of Patient Records stored temporarily in the *12's* archives. | If long-term retention of Patient Records is desired, transfer those records to the CODE-STAT Suite application before deleting them from the device. |

## Physical Safeguards

| HIPAA Standard | Security Issue and Feature | Recommended Action |
|---|---|---|
| Device and Media Controls (to govern receipt, movement and removal of hardware and electronic media) | To support the timely delivery of patient care in critical and emergency situations, the device is designed to grant caregivers immediate access to the product's patient care features. The device should be kept out of the hands of unauthorized users to reduce the chance of them gaining access to archived Patient Records. Policies and procedures must balance the need to protect the device from unauthorized physical access while keeping it readily available to operators. | To increase protection of Patient Records, implement procedures to physically secure the device from the time of service until electronic patient data is deleted from the device. |

## Technical Safeguards

| HIPAA Standard | Security Issue and Feature | Recommended Action |
|---|---|---|
| Access Controls (to allow access only to those granted access rights) | To provide for rapid response to cardiac emergencies, the device does not require users to log-on in order to use it.<br><br>Once patient care is completed and the product is powered off, the Patient Record is archived within the device.<br><br>To balance the need for ready access to archived data with the need to prevent access by unauthorized users, the device provides the ability to set a passcode—a static token consisting of 4 digits, which is not user-unique.<br><br>In all software versions, the device can be set to require a four-digit passcode before set-up options can be changed (such as which phone numbers the device dials when transmitting data).<br><br>With software versions 3011371-**095** and higher, the device may be set to require a four-digit passcode in order to view the archive and/or to delete Patient Records. | Prior to placing the device into service, change the default set-up passcode.<br><br>With software versions 3011371-**095** and higher, use the option to set a passcode to prevent unauthorized users from accessing or deleting archived data.<br><br>Turn off the device after each use, as this archives the Patient Record.<br><br>Periodically ensure that device access is restricted to authorized individuals.<br><br>Implement procedures to physically secure the device from the time of service until electronic patient data is deleted from the device.<br><br>Customers with software versions below 3011371-**095** may wish to contact your service rep to arrange for purchase and installation of the higher security software version. |

## Technical Safeguards (continued)

| | | |
|---|---|---|
| | Setting the optional security passcodes increases data protection, but does not absolutely prevent someone who has physical access to the device from ultimately ascertaining the access code (through, for example, a trial and error approach.<br><br>The product's proprietary data management and store location strategy make data difficult to read without specialized software. | |
| Integrity (to protect electronic patient data from improper alteration or destruction) | The device maintains a Patient Record for each device use and can store up to 50 records. After the limit is reached, the records will be written over. | To reduce risk of data loss, implement procedures to download the Patient Record after each use or at the end of each day. |
| Transmission Security (to protect electronic patient data transmitted over an electronic communications network) | To facilitate patient care or to archive data, the device can transfer Patient Records via cellular phone modems, analog phone modems, wireless connections or serial connections.<br><br>The LIFENET BLUE product option uses Bluetooth technology to encrypt data during wireless transmission from the LIFEPAK 12 defibrillator. This protects Patient Records as they are transmitted to a cell phone or ***directly*** to a computer running medical informatics software. Typically, however, data from the defibrillator is first sent to a cell phone and then transmitted to a computer. No encryption of Patient Records is provided during transmission from the cell phone to the analog modem on the computer that receives the data. | When data is sent from a cell phone to a computer running medical informatics software, implement policies and mechanisms as appropriate to secure data transmission. Customers who regularly transmit electronic patient data may contact Physio-Control at 1.800.442.1142 for more information on transmission security. |

## IMPORTANT NOTE

This document provides a description of certain security features of the LIFEPAK 12 defibrillator/monitor series. In addition, it provides recommended actions and suggested controls that may help you mitigate or otherwise address the information security risks that are associated with the product's use. However, these security features, recommended actions, and suggested controls may not ensure that all security incidents can be avoided, such as those related to the inadvertent or the unauthorized disclosure, deletion, or modification of a patient's health information. In addition, this document is not intended to provide, and should not be relied upon as, a comprehensive description or an exhaustive list of recommended actions and controls. As a result, depending upon the particular security requirements and needs of your organization, additional actions and controls may need to be implemented by your organization.



Physio-Control • 11811 Willows Road NE • PO Box 97006 • Redmond, WA 98073-9706 • 800.442.1142 • www.physio-control.com