Medtronic Emergency Response Systems

Security Information for the LIFEPAK® 1000 Defibrillator

This information about security features of the Medtronic LIFEPAK 1000 defibrillator is provided to help our customers comply with the HIPAA[1] Security Standards (effective April 2005).

Understanding the device capabilities, using its security features and implementing the recommended procedures can assist you in safeguarding electronic protected health information as you use the LIFEPAK 1000 defibrillator to respond to cardiac emergencies and transmit data for post-event review. *This information is not intended as a comprehensive or exhaustive list of recommendations, however. Your organization's particular needs and security requirements may call for additional actions and controls.*

Product Use/Technical Features

The LIFEPAK 1000 defibrillator is designed for use by professional first responders to cardiac emergencies in all settings including businesses, outdoor locations, schools, hospitals and homes.

The operating system that supports the device is VxWorks®, an Embedded Real-Time OS.

Patient Data

Data recording

When used to analyze and/or defibrillate a patient, the LIFEPAK 1000 defibrillator creates an electronic Patient Record, which includes: event log data (such as the time the device is powered on, results of heart rhythm analysis and number of shocks administered); CODE SUMMARY™ critical event record (which also includes waveforms); and continuous ECG data.

Data storage

Used in emergency situations, the LIFEPAK 1000 defibrillator has limited data storage capacity. Each time the device is used, the continuous ECG data for the preceding episode is deleted. The AED retains the event log summary data for the preceding episode and/or most recent use.

Data transmission

The LIFEPAK 1000 defibrillator uses an IrDA port for wireless transmission of Patient Records into a personal computer equipped with the DATA TRANSFER™ Express or CODE-STAT™ Suite medical informatics system, which archives records for subsequent viewing.

Potential Security Exposures

Examples of possible risks to patient data include:

- Unintentional overwriting of patient data before transfer
- Inadvertent disclosure of patient data during servicing of the device
- Improper disclosure due to unauthorized employee access to patient data
- Improper disclosure or loss of patient data resulting from theft of the device

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

Security Features of the LIFEPAK 1000 Defibrillator

The following description of security features and recommended procedures for proper use of the device are provided to facilitate your HIPAA compliance efforts. If you transmit electronic protected health information from the LIFEPAK 1000 defibrillator, contact Medtronic Emergency Response Systems, Inc. at 1.800.442.1142 for more information on transmission security.

Administrative Safeguards

HIPAA Standard	Security Issue and Feature	Recommended Action
Information Access Management (to implement policies and procedures authorizing access to electronic protected health information)	The device maintains a Patient Record for the last two device uses. New incoming data automatically deletes the oldest case and compresses the other case into a summary record. Each Patient Record includes the unit's serial number and the date and time of device use.	To help prevent loss of electronic patient data and improper access to patient data, implement procedures to download the Patient Record after each use. To help prevent improper disclosure of patient information, have servicing performed only by personnel trained in handling protected health information. To help prevent improper disclosure of patient information, setup the LIFEPAK 1000 defibrillator to automatically delete the Patient Record after data transfer.
Contingency Plan (to respond to an occurrence that damages systems containing protected data)	Medtronic CODE-STAT Suite medical informatics system can be used to support backup and recovery of Patient Records stored in the LIFEPAK 1000 defibrillator archives.	If data retention is desired, promptly transfer those records after each device use to CODE-STAT Suite medical informatics system.

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 timely care in cardiac emergencies, the LIFEPAK 1000 defibrillator is designed to provide caregivers with quick access to its capabilities. Policies and procedures must strike a balance between physically safeguarding the device and keeping it readily available.	Implement procedures to protect the defibrillator from unauthorized physical access while providing ready access for authorized operators.

Technical Safeguards

HIPAA Standard	Security Issue and Feature	Recommended Action
Transmission Security (to protect electronic patient data transmitted over an electronic communications network)	To facilitate patient care or to archive data, the device can transmit Patient Records by connecting via infrared (IrDA) port to a computer running LIFENET® medical informatics software. Patient records are not encrypted, but do include features to ensure the integrity of the patient data. The point-to-point nature and short range of the infrared transmission provides adequate safeguards against inadvertent disclosure of patient information.	Customers who regularly transmit electronic patient data may contact Medtronic Emergency Response Systems, Inc. at 1.800.442.1142 for more information on transmission security.

IMPORTANT NOTE

This document provides a description of certain security features of this product. In addition, it provides recommended actions and suggested controls that may help you mitigate or otherwise address the information security risks associated with the product's use. However, these security features, recommended actions, and suggested controls may not ensure all security incidents can be avoided, such as those related to the inadvertent or the unauthorized disclosure, deletion, or modification of 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.

Medtronic Emergency Response Systems • 11811 Willows Road NE • PO Box 97006 • Redmond, WA 98073-9706 • 800.442.1142 • www.medtronic-ers.com