Medtronic Emergency Response Systems

Security Information for the LIFEPAK® 500 Automated External Defibrillator (AED) Product Family

This information about security features of the Medtronic LIFEPAK 500 automated external defibrillator (AED) is provided to help our customers comply with the HIPAA[1] Security Standards by their compliance date.

Medtronic Emergency Response Systems 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 and physical safeguards to help you, as a Covered Entity, establish process and procedures for use of the Medtronic products that are reasonable and appropriate for your institution.

Understanding the device capabilities, using its security features and implementing the recommended procedures can assist you in safeguarding electronic patient data as you use the LIFEPAK 500 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. Your organization's particular needs and security requirements may call for additional actions and controls.

Product Use/Technical Features

The LIFEPAK 500 automated external defibrillator is designed for use by first responders to cardiac emergencies in and out of the hospital, such as firefighters, police officers, flight attendants, security officers and others who are well trained in CPR and AED use.

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

Patient Data

Data recording

When used to analyze and/or defibrillate a patient, the LIFEPAK 500 AED creates an electronic Patient Record, which includes: event log data (such as the date and time the device is powered on, results of heart rhythm analyses and number of shocks administered); CODE SUMMARY™ critical event record (which also includes waveforms); continuous ECG data; and audio recordings, if the operator uses the audio recording feature. Audio recordings may contain conversations with identifiable patient information, such as name or address.

Data storage

The LIFEPAK 500 AED stores information for two patients. Each time the AED is used the oldest Patient Record is deleted.

Data transmission

The LIFEPAK 500 AED can use an analog modem or a serial connection to transmit Patient Records into the CODE-STAT™ Suite medical informatics system, which archives records for subsequent viewing. The defibrillator also can print a record directly to a printer. The device operator can add an incident identification number to the recorded data when transferring it from the LIFEPAK 500 AED to a computer or printer.

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

Potential Security Exposures

Examples of possible risks to electronic patient data include:

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

Security Features of the LIFEPAK 500 AED Product Family

The following description of security features and recommended procedures for proper use of the device are provided to facilitate your HIPAA security compliance efforts. Customers who regularly transmit electronic patient data from the LIFEPAK 500 AED may contact Medtronic Emergency Response Systems 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 patient data)	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. The LIFEPAK 500 AED operator has the option of adding an incident identification number when the Patient Record is transmitted, and the identifier is stored until the next device use.	To help prevent loss of electronic patient data, implement procedures to download the Patient Record after each use. To avoid improper access to Patient Records, implement procedures to protect the LIFEPAK 500 AED from unauthorized physical access. Consider storing the device in an accessible location (such as an unlocked storage cabinet) that will alert others when it is removed (for example, by emitting a distinct tone or triggering a flashing light). 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 CODE-STAT Suite medical informatics system can be used to support backup and recovery of Patient Records stored in the LIFEPAK 500 AED archives.	If long-term 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 500 AED 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 LIFEPAK 500 AED from unauthorized physical access while providing ready access for authorized operators. Consider storing the device in an accessible location that will alert others when it is removed (such as an unlocked storage cabinet that emits a distinct tone or triggers a flashing light when opened).

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 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 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

MIN 3205412-000 / CAT. 26500-001912