Medtronic Emergency Response Systems

Security Information for the LIFEPAK® 20 Defibrillator/Monitor

This information about security features of the Medtronic LIFEPAK 20 defibrillator/monitor is provided to help our customers comply with the HIPAA[1] Security Standards by their compliance date.

Medtronic ERS 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 processes 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 recommended procedures can assist you in safeguarding electronic patient data as you use the LIFEPAK 20 defibrillator/monitor in cardiac emergencies or routine patient monitoring applications. *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 20 defibrillator/monitor is an acute cardiac care response system used by authorized healthcare providers in hospitals and clinics. Infrequent responders trained in basic life support can operate it as an automated external defibrillator (AED). More advanced responders can use the device to provide therapeutic functions such as manual defibrillation and external pacing as well as advanced monitoring.

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

Patient Data

Data recording
The LIFEPAK 20 defibrillator/monitor 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, age and gender, plus a patient ID and incident ID to the Patient Record.

Data storage
At least two complete Patient Records are stored in the unit's archives (more may be stored, depending on the size of each record). 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 20 defibrillator/monitor. 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, Patient Records may be transferred from the LIFEPAK 20 defibrillator/monitor to a computer with Medtronic CODE-STAT™ Suite medical informatics software. The *20* has an infrared (IrDA) port for data communication.

The device can print a CODE SUMMARY™ report that includes both an introduction with patient information and a critical event record. It also includes an event and vital signs log, and the waveforms associated with certain events. Archived Patient Records can be printed.

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 20 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 *20* 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 and gender and ID numbers for the patient and for the incident.	To help prevent improper disclosure or loss of electronic patient data, implement procedures to download Patient Records to backup storage and delete them from the device after each use. To help prevent improper disclosure of electronic patient data, service should be 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 *20'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. Policies and procedures must balance the need to protect the device from unauthorized physical access while keeping it readily available to operators.	The device should be kept out of the hands of unauthorized users to reduce the chance of unauthorized access to archived 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. Once patient care is completed and the product is powered off, the Patient Record is archived within the device. 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 passcodes—static tokens consisting of 4 digits, which are not user-unique. The device can be set to require a different four-digit passcode for four functions: • Changing set-up options • Viewing archived patient data • Deleting Patient Records • Performing maintenance 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).	Prior to placing the device into service, set passcodes to restrict access to archives and to prevent unauthorized people from changing set-up options. Change the default passcodes set at the factory. Turn off the device after each use, as this archives the Patient Record. Periodically ensure that device access is restricted to authorized individuals. Implement procedures to physically secure the device from the time of service until electronic patient data is backed up and deleted from the device.

Technical Safeguards (continued)

Integrity (to protect electronic patient data from improper alteration or destruction)	The device maintains a Patient Record for each device use and stores at least two complete Patient Records. When the memory is full, 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. Delete records from the device after they have been backed up.
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 CODE-STAT Suite medical informatics software. Although data is not encrypted before transmission, the proprietary data management and store location strategy make data difficult to read without specialized software.	Customers who regularly transmit electronic patient data may contact Medtronic Emergency Response Systems 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 20 defibrillator/monitor. 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 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.