



### Security Information for the PACEART System

This information describing the security features of the Medtronic Paceart system is provided to help our customers comply with “Health Insurance Reform: Security Standards” (HIPAA Security Rule) found at 45 C.F.R. Parts 160, 162, and 164. This information applies to Paceart 2004 First Edition and later software versions. Paceart displays the software version on the user logon screen.

Medtronic Paceart engaged an independent security expert to help proactively assess the Paceart system we currently market with respect to the standards and implementation specifications of the Security Rule. The following 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 the use of Medtronic Paceart products that are reasonable and appropriate for your institution.

Understanding Paceart’s capabilities, using Paceart security features and implementing recommended procedures can assist you in safeguarding electronic patient data as you use the Paceart System in the management of heart rhythm patients. 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 Medtronic Paceart system is a computer software application that organizes relevant patient, cardiac device and programmer information to help clinics manage follow-up of implantable cardiac device patients. Paceart’s principle objective is to provide heart rhythm management solutions designed to allow clinicians and the cardiac device industry to optimize the care of patients with implanted cardiac devices.

The Paceart system is installed on Intel-compatible hardware running Microsoft Windows operating systems. The Paceart system uses Microsoft SQL Server for database hosting. Other components of the technical environment will include Microsoft Internet Information Server (IIS) if the provider has selected Paceart’s Web Access option.

### Patient Data

#### *Data Recording*

The Paceart system creates an electronic patient record, which may contain patient-specific electronic protected health information (ePHI) data, including ECG and other monitored parameters and therapy events such as defibrillation and pacing. Patient data stored by the Paceart system can include for each patient: name, address, city and state, postal code, telephone numbers, fax numbers, Social Security number, medical record number, health plan beneficiary numbers, account numbers, certificates and license numbers, device numbers, date of admission and date of service.

#### *Data Storage*

The number of patient records managed by the Paceart system is dependent upon the storage capacity of the computer server hosting the ePHI data. Data are stored in a Microsoft SQL Server database.



### Security Information for the Paceart System

#### Data Retrieval

Clinicians access ePHI via the Paceart system’s Windows-based user interface. Paceart allows the clinic’s system administrator to create and manage unique user identifications and passwords for each clinician accessing the system. User profiles controlling access to data can be created and assigned to individual user identifications and passwords. The Paceart System Administrator’s Manual details instructions for the creation and management of user identifications and passwords.

#### Data Transmission

For patient care or data archiving purposes, data may be transferred from the Paceart system to another data management tool employed by the clinic. Information is transferred via Paceart’s Export Module, which creates an XML-based message that is transmitted by the clinic’s network infrastructure.

### Potential Security Exposures

The following table represents examples of potential information security exposures associated with the Paceart system. Other information security exposures may exist depending on how this product is used within your organization.

Security Exposures	Hostile or Intentional Activities	Non-Hostile or Unintentional Activities
External	<p>The Paceart system-equipped computer is physically damaged, thereby preventing or delaying access to ePHI required for delivery of care.</p> <p>Theft of a Paceart system-equipped computer from the building results in ePHI being destroyed or disclosed.</p> <p>Physical access to the Paceart system-equipped computer permits the copying of ePHI to portable media for removal and later disclosure.</p> <p>The copying of ePHI data to portable media for removal and later disclosure.</p>	<p>ePHI is disclosed to service provider when Paceart system-equipped hardware is repaired or serviced and software support is provided.</p> <p>ePHI is left on Paceart system-equipped computers when equipment is retired, and a salvage company discovers patient data.</p>
Internal	<p>Employee copies ePHI to a portable media for removal and later disclosure.</p> <p>Employee intentionally deletes or modifies ePHI.</p>	<p>Employee spills liquids or causes other accidental damage to the Paceart system-equipped computer, thereby preventing or delaying access to ePHI required for delivery of patient care.</p> <p>Employee accidentally deletes ePHI from Paceart system database.</p>



## Security Information for the Paceart System

### Paceart System Security Features

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

#### Administrative Safeguards

HIPAA Standard	Security Issue and Feature	Recommended Action
<p><b>Information Access Management</b></p> <p>(To implement policies and procedures authorizing access to electronic patient data.)</p>	<p>Paceart security features are based upon the customer's selection of security model. There are two options. The first option utilizes the Microsoft SQL Server security model. The second option utilizes the Microsoft Windows security model. Both models provide for controlling access to the Paceart system application and ePHI. Both models allow for audit logging capabilities. Use of the Microsoft Windows security model allows for the use of Microsoft Windows security groups and logging.</p>	<p>To help prevent improper disclosure or loss of ePHI, installation of the full version of Microsoft SQL Server with use of the Microsoft Windows security model is recommended. This will permit the use of Windows event logging to track user activities. This will also permit the use of Windows groups for role-based administration of user access.</p> <p>Clinics should enable Windows event logs for both successful and failed events and implement policies and procedures for backup and protection of audit logs.</p>
<p><b>Contingency Plan</b></p> <p>(To respond to an occurrence that damages systems containing electronic patient data.)</p>	<p>Paceart provides for the backup and recovery of ePHI using either the standard Microsoft SQL Server utilities or the backup capabilities of the Windows server. Data backups can be used to store ePHI on portable media or clinic-based storage systems.</p>	<p>Clinics should establish policies, standards, and procedures for the backup and recovery of ePHI.</p> <p>Clinic should establish policies, standards, and procedures for the protection of portable media that contain ePHI.</p>
<p><b>Protection from Malicious Software</b></p> <p>(To implement technology designed to protect ePHI from attack from software viruses.)</p>	<p>Paceart relies on the security controls implemented for the hosting platform on which it is installed. Customers are responsible for providing a secure platform on which the Paceart system can operate.</p>	<p>Clinics should install anti-virus software on the computer used to process and manage ePHI used by the Paceart application. The procedure should call for the timely updating of virus definitions. Security updates to the operating system are recommended upon consultation with Paceart Technical Services.</p>



## Security Information for the Paceart System

### Physical Safeguards

HIPAA Standard	Security Issue and Feature	Recommended Action
<p><b>Workstation Security</b> (To implement policies and standards to physically secure access to and the integrity of Paceart system managed ePHI at the local workstation level.)</p>	<p>The Paceart system allows for the storage of electronic patient data on either a local workstation or a network-enabled server. In either case, the Paceart System utilizes Microsoft SQL Server to host the data. The Paceart system workstation client connects via ActiveX Data Objects (ADO [SQLOLEDB]) to the Microsoft SQL Server database, whether that database resides directly on the local workstation, on the clinic's network, on a Virtual Private Network (VPN), or on a remote network accessed through dial-up. Customers are responsible for ensuring access to Paceart system-managed ePHI is secure.</p>	<p>Implement policies and standards for physical security for those workstations used to interface with the Paceart database, either on a local workstation or server environment.</p> <p>Implement necessary network security measures to ensure data transmitted via the ADO interface between the Paceart workstation client and the Microsoft SQL Server database are secure.</p> <p>Implement workstation user authentication policies that manage the access of ePHI by user role.</p> <p>Use of a password protected screen saver is recommended.</p>



## Security Information for the Paceart System

### Technical Safeguards

HIPAA Standard	Security Issue and Feature	Recommended Action
<p><b>Access Controls</b> (To manage access and use of ePHI stored in the Paceart system database.)</p>	<p>Microsoft SQL Server is used to provide database support for the Paceart application. The Paceart application can provide for the use of unique user accounts and passwords in conjunction with either the Microsoft Windows security model or the Microsoft SQL Server security model. The Microsoft Windows security model provides additional benefits in the form of coordination with Microsoft Windows security groups, Microsoft Windows password policies and Microsoft Windows event logging.</p>	<p>Clinics should administer user access procedures consistent with the customer's policies, procedures and standards for administration of applications and systems that maintain ePHI.</p> <p>Clinicians and other users should be assigned unique user accounts and appropriate user access permissions for accessing the Paceart application.</p>
<p><b>Integrity</b> (To implement policies and procedures designed to protect the integrity of system-managed ePHI.)</p>	<p>The accuracy and completeness of the Paceart system's data depend in part on the policies and standards implemented on the host operating system. Risk to Paceart stability can be introduced from weak local security policies on the host platform. Security patches to the OS should be applied after consult with Medtronic Paceart Technical Services.</p>	<p>Implement policies and standards to secure and protect the host operating system on which the Paceart client application is to be operated.</p> <p>Implement policies and standards to secure and protect the host operating system on which the Paceart database is to be hosted. These policies and standards should be appropriate for a system that maintains ePHI.</p> <p>Utilize the Microsoft Windows security model.</p> <p>Utilize an external Uninterruptible Power Supply (UPS) in conjunction with workstations or servers used to connect to or host a Paceart database.</p>



### Security Information for the Paceart System

#### Important Notes

This document provides a description of certain security features of the Paceart system. 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, your organization may need to implement additional actions and controls, depending upon your particular security requirements and needs.

#### Caution

Federal law (USA) restricts this device to sale by or on the order of a physician (or properly licensed practitioner). Refer to the technical manual for complete directions for use and full disclosure.

