Heart Connect™ System
IT Department Guide

Security

The **Heart Connect System** incorporates security measures for protection of Confidentiality, Integrity and Availability. These security measures are in line with industry security policies and practices.

Microsoft Surface Pro Tablet (Windows 8.1) Security Measures

- Allows role-based access; users have no access to administrator account; unique administrator passwords per device.
- Runs a supported Windows 8.1 OS
- Configured to automatically receive and install Windows OS important (security) updates
- Antivirus software used and set to automatically update signatures.

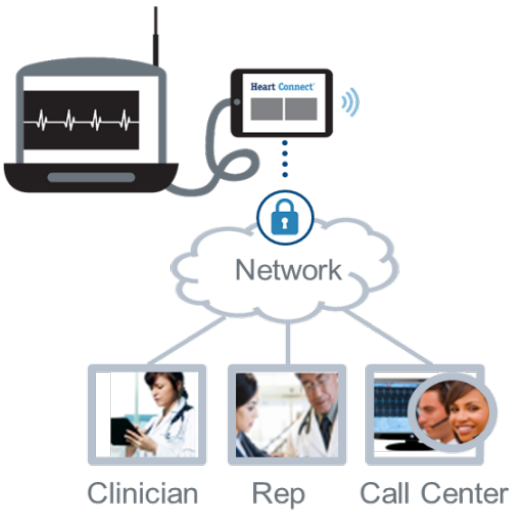
Heart Connect Meeting Security Measures

- All meeting data is transmitted via an encrypted connection to ensure patient data (PHI) and device data are protected
- Each tablet device uses a server account created/managed by Boston Scientific.
- No PHI is stored on the device. Only a pass through for streaming.

Network Configuration

Ensure network configuration allows for the following connectivity information:

- Wireless network support: 802.11 a/b/g/n/ac
- URL: heartconnect.bostonscientific.com
  - No specific IP address, uses elastic load balancing
  - Uses DHCP for IP address
  - Ports: 80, 443
- Other IP addresses:
  - 52.202.62.205, 52.202.62.206
    - Ports: 443 for SSL, 8802 for TCP
  - 52.200.215.122, 52.200.223.187
    - Ports: 8801 for TCP/UDP, 443 for SSL



Support Information

- Technical Support: 1-800-CARDIAC (request Technical Services)
- Instructions for Use: www.bostonscientific.com/ifu

CRM-457801-AA MAR2017