CONNECTING YOUR CLINICIAN PROGRAMMER

BENEFITS OF CONNECTING TO A SECURE, INTERNAL WI-FI NETWORK

Connect to a secure, internal network because it:

- Enables easier access to internal networked printers.
- Ensures your clinician programmer and software have access to mobile device management enabling secure monitoring, management, and configuration.
- Allows wireless transfer of reports to your computers or EMR endpoints.
- Provides the most secure connection.

CONNECTION COMPARISON

<table>
<thead>
<tr>
<th></th>
<th>Secure, Internal Wi-Fi Network</th>
<th>Other/Guest Wi-Fi Network</th>
<th>No Wi-Fi Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to internal networked printers</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Wireless transfer of reports to PC</td>
<td>✔</td>
<td>-</td>
<td>✗</td>
</tr>
<tr>
<td>Seamless flow of data to the cloud</td>
<td>✔</td>
<td>-</td>
<td>✗</td>
</tr>
<tr>
<td>Software updates</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>VMWare Workspace One Mobile Device Management (e.g., remote wipe if stolen)</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
</tbody>
</table>

LIMITATIONS OF OTHER WI-FI NETWORKS

Connecting to other networks may have limitations.

- Access to networked printers may be restricted or limited.
- Mobile device management will not be available if the Wi-Fi connectivity is interrupted or lost.
- Data may not consistently flow to cloud software.
THE PROGRAMMER IS SAFE TO CONNECT TO YOUR NETWORK

Security is a top priority. The diagram below summarizes how data flows and is protected. Medtronic uses industry leading standards to encrypt, protect, and manage data.

---

**VMWare Workspace**
- App Whitelist
- Data Wipe
- Controlled Updates
- Root Detection

**Digital Health Platform**
- Restricted Access
- Status Checking
- Data Protection
- Responsible Data Use

**Clinician Programmer Tablet**
- Connection Encryption
- Communication Integrity Checks
- Code Integrity Checks

**Clinician Application**
- Device Encryption
- Password Protection
- Application Sandboxing
- Permissions

**Patient Data Service**
- Debugger and Root Detection
- Resource and Session Data Encryption
- Code Encryption, Obfuscation, and Integrity Checks
- Digital Signature Checks

**Communications Manager**
- Debugger and Root Detection
- Resource Data Encryption
- Code Encryption, Obfuscation, and Integrity Checks
- Digital Signature Checks

**Implanted Device**
- Connection Encryption
- Communication Integrity Checks
- Code Integrity Checks

**Communicator**
- MDT Proprietary Telemetry
- Proximal Communication
- Communication Integrity Checks

**SynchroMed™ II Pump**
- SSL Encryption

**IntelliS™ Neurostimulator**

---

**TALK TO YOUR IT DEPARTMENT AND GET CONNECTED**

Talk with your IT department about the need to establish a secure Wi-Fi connection with the clinician programmer to enable you to do your work with ease.

- Share this document with the clinic IT department to address initial security concerns.
- Consider creating a new system user account for the tablet on the internal network.
- Send additional cyber security questions to the Digital Connectivity inbox.

**HOW TO CONTACT DIGITAL CONNECTIVITY**

Email: rs.digitalconnectivity@medtronic.com

---

© 2021 Medtronic. All rights reserved. Medtronic, Medtronic logo and further, together are trademarks of Medtronic. Third-party brands are trademarks of their respective owners. All other brands are trademarks of Medtronic company. UC201912616a EN