Top 10 Ways to Mitigate the Risk and Effect of Cyberattacks on Medical Devices

This list of tips was developed by members of AAMI’s Wireless Strategy Task Force (WSTF).

1. **Use strong passwords.** Do not use default passwords. For guidance, consult the National Institute of Standards and Technology password guidelines.

2. **Encrypt data** while in motion and at rest.

3. Ensure that **security patches** are implemented safely and kept up to date.

4. **Provide redundancy** for critical systems.

5. **Use state-of-the-art security solutions**, such as WPA2 (Wi-Fi Protected Access II) enterprise for Wi-Fi. Do not use WEP (wired equivalent privacy), PSK (pre shared key), or four-digit Bluetooth codes.

6. **Limit network access** by employing role-based network policies.

7. **Include cybersecurity testing requirements** in RFQs (requests for quotations).

8. **Perform periodic reviews** of system vulnerabilities and mitigations, including:
   - Bluetooth
   - Wi-Fi
   - Bring your own device (BYOD)
   - Hardwired
   - USB

9. **Extend security policies** beyond Wi-Fi to include IoT (Internet of Things), Bluetooth, cellular, etc.

10. **Periodically evaluate your BYOD policy** for security flaws.

The WSTF is comprised of approximately 30 wireless experts who collaborate to address the wireless-related needs of the healthcare technology management community.

That mission includes managing the wireless spectrum to ensure that medical devices are able to effectively communicate with one another, as well as addressing wireless cybersecurity vulnerabilities.

For more information, visit [www.aami.org/WSTF](http://www.aami.org/WSTF).