5 Ways to Enhance Infusion Pump Cybersecurity

Infusion pumps represent more than a quarter of connected hospital devices. Because they are used throughout hospitals and interface with patient records, they could be extremely dangerous if comprised by a cyberattack. But studies have shown that 75% of infusion pumps have one or more cybersecurity vulnerabilities.

To protect IV infusion pumps from cyber threats, hospitals and health systems can use the following security measures.

1 Address fundamental vulnerability issues

Double check your basic medical device cybersecurity hygiene by taking the following actions:

- Change default credentials
- Develop and enforce password policies (14+ characters, restricted access to master lists)
- Configure automatic logoff
- Assign access levels by user privilege tiers
- Reduce attack radius by segmenting IV pump networks
- Ensure firewalls and routers are correctly installed and configured

2 Conduct vulnerability assessments

Check for system weaknesses with regular vulnerability assessments. Common issues include:

- Insecure passwords
- Inaction on software updates, patches, and recall recommendations
- Inadequate cybersecurity controls
- Use of legacy systems

3 Monitor vulnerability alerts

Implement a system that offers continuous security alert monitoring. This can:

- Prevent opportunities for cyber attacks
- Identify any live attacks in progress

4 Invest in infrastructure to implement fixes and address recalls

Make sure you have the infrastructure necessary to address any potential recalls due to cybersecurity issues:

- Designate staff who own responsive actions
- Integrate risk mitigation into staff workflows
- Assess ability to quickly identify and locate all affected medical devices

5 Secure legacy equipment

Replacing older devices isn't always financially feasible, but you can protect your legacy devices by:

- Segmenting networks to isolate legacy operating systems
- Limiting system access to critical data and services
- Conducting regular vulnerability scans
- Scheduling inventory audits in connection with vulnerability scans
- Automating patches and software updates

Cybersecurity vulnerabilities in infusion pumps pose serious threats to hospitals' reputations and bottom line, as well as patient safety. Want to know more about how you can mitigate cyberattack risk in your hospital's connected devices? Read Medical Device Cybersecurity for Connected Infusion Pumps.

ELITE BIOMEDICAL SOLUTIONS

Elite Biomedical Solutions is an ISO 13485:2016-certified, U.S.-based manufacturer. Our industry-leading QMS, cutting-edge reverse engineering process, and commitment to the highest standards produce affordable, OEM-quality parts that can boost ROI and extend the lifespan of infusion and telemetry assets.