What you need to know about Network Connected Medical Device Security:

As with all technologies, medical device benefits are accompanied by cybersecurity challenges. An emerging threat is the hacking of network connected medical devices. This can jeopardize patient safety by affecting operations in an unintended manner.

Listed to the right are important tips to follow.

Action—Report

Contact your IT administrator, practice manager, or immediate supervisor with any suspicious activity. Add their name and number to this sheet for reference.

Quick action is imperative. This threat is real!

For more resources and to learn more about how you can protect your patients from cyber threats, check out the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publication at 405d.hhs.gov.

HHS 405(d)
Knowledge on Demand

What should I ask?

Know your organization's protocols in the event of a potential shutdown or attack against network connected medical devices. Help patients and staff by understanding the processes and procedures; this can help mitigate the impacts.

Be sure to ask:

- ☑ How do we notify patients if their network connected medical devices are compromised?
- ☑ Are network connected medical devices kept up to date and protected against compromise?

When should I ask?

Knowledge of your organization's protocols for potential attacks on connected medical devices should be shared during new hire orientation or at security training. These protocols should also be communicated to patients when they are given connected medical devices.

Who should I ask?

Each organization should have IT security professionals to help answer any questions on the policy and governance associated with connected medical devices. If your organization does not, ask your supervisor for information and/or resources to learn more about this threat.

Reporting

Report to:

Contact Info: