Put Patients First: Protect Network Connected Medical Devices

Know your organization's protocols in case of a potential shutdown or attack against medical devices

Consider this: Your organization is afflicted by a phishing attack that affects a file server that's connected to multiple heart monitors. While scanning the network for devices, the attacker takes control of all of the heart monitors in the Intensive Care Unit, powering them off, continuously rebooting them, and putting multiple patients at risk.

To protect your patients, ask your IT security professionals about your organization's governance and policies associated with medical devices.

Common vulnerabilities in medical devices can include legacy or older equipment. Always make sure your medical equipment is up-to-date and and new validated software patches are installed and tested promptly.

For more tips on the five main cybersecurity threats, check out the HICP publication on the 405(d) website.
www.405d.hhs.gov