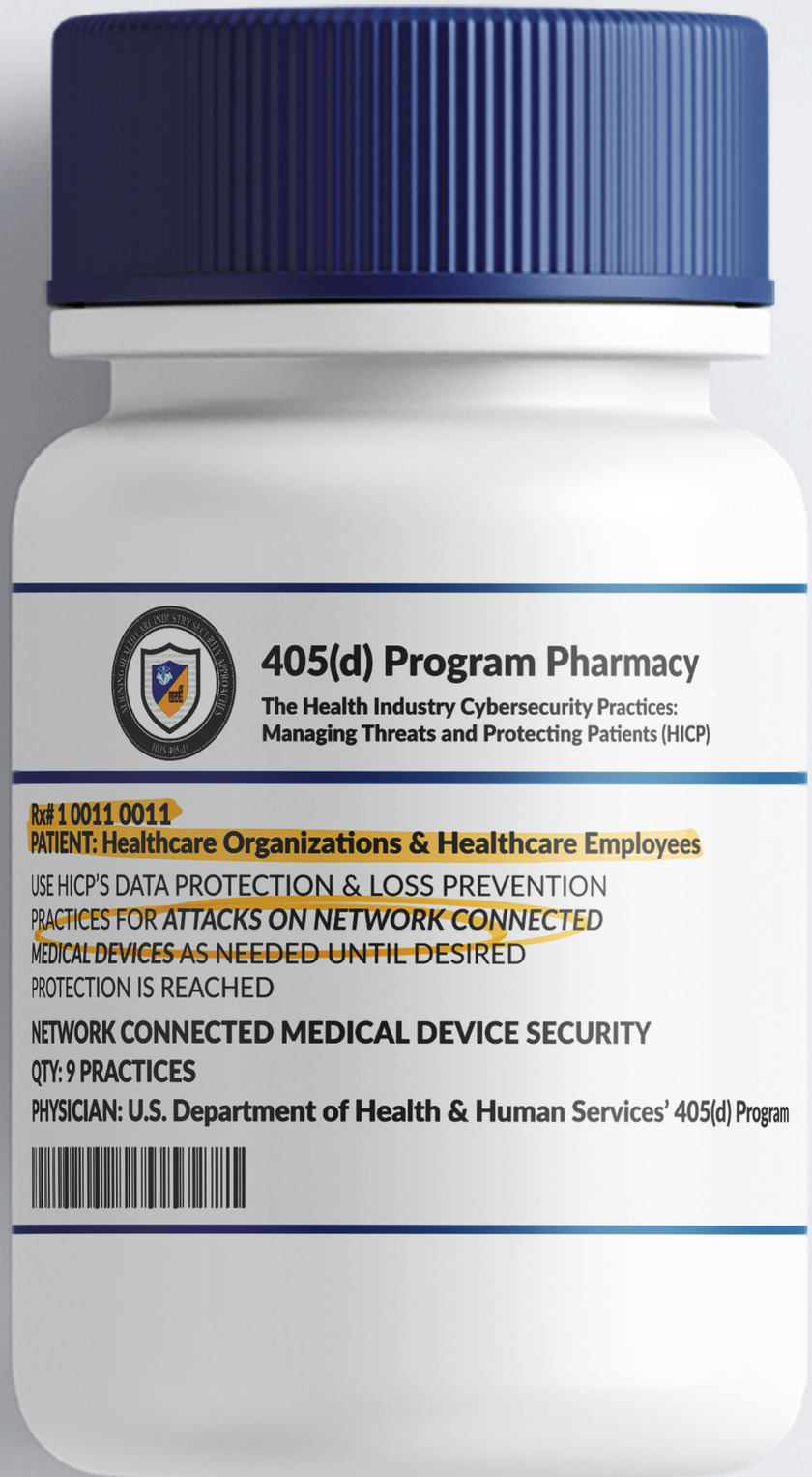


# PRESCRIPTION:

## Network Connected Medical Device Security

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and are successful in the treatment of many diseases. As with all technologies, medical device benefits are accompanied by cybersecurity challenges. Cybersecurity vulnerabilities are introduced when medical devices are connected to a network or computer to process required updates, therefore in order to protect patients it is important to protect these devices. Network connected medical devices are a specialized type of Internet of Things (IoT) device and rather than recreating cybersecurity practices for them, healthcare organizations are encouraged to extend the relevant cybersecurity practices from each of the other prescriptions, and implement them appropriately for medical device management.

***Protect yourself and your patients by following the course of treatment below:***

### For Organizations of All Sizes:

- Establish Endpoint Protection Controls. As with other endpoints, medical devices should follow similar protocols such as installing local firewalls, providing routine patching, network segmentation, and changing default passwords
- Implement Identity and Access Management Policies. Just like endpoints, network connected medical devices security should include authentication measures and remote access controls like multifactor authentication
- Institute asset Management procedures. It is important to follow your asset management procedures for medical devices just as you would for endpoints. Keep an updated list of inventory and software updates to ensure your devices are accounted for and are up to date.
- Create a Vulnerability Management Program that can consume network connected Medical Device Management disclosures and always respond accordingly when received.
- Add security terms to network connected Medical Device Management contracts that enable you to hold device manufacturers accountable.

*For more Medical Device Security practices, please visit **405d.hhs.gov** to download a copy of the HICP technical volume for your organization. Check out the available resources 405(d) has to offer by visiting our social media pages @ask405d on Facebook, Twitter, and Instagram!*