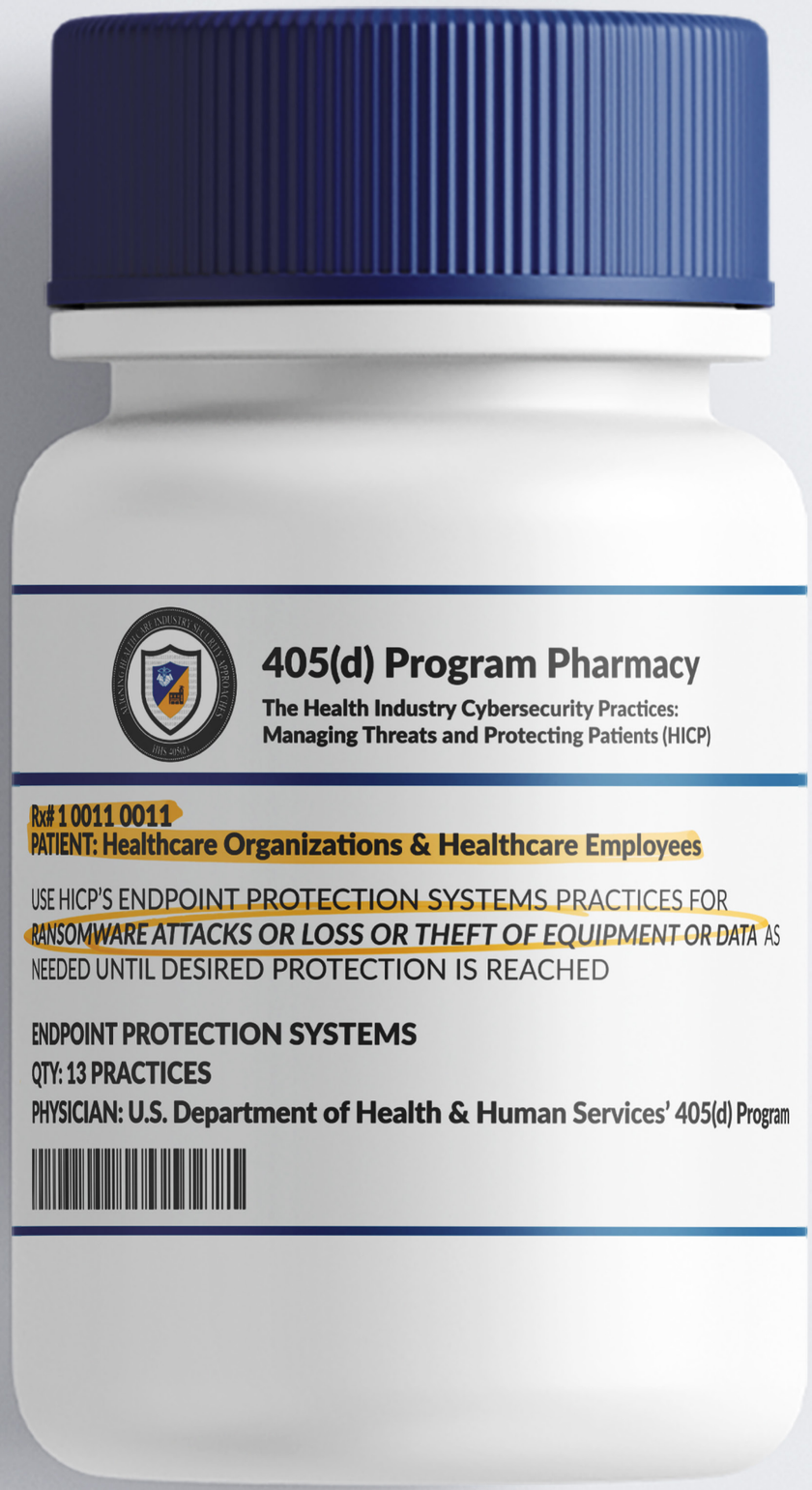

PRESCRIPTION:

Endpoint Protection Systems

An organization's endpoints must be protected. Endpoints include desktops, laptops, mobile devices, and other connected hardware devices (e.g., printers, medical equipment). Because technology is highly mobile, computers are often connected to and disconnected from an organization's network.

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

For Small Organizations:

- Remove administrative accounts as most users in an organization do not need to be authorized as system administrators with expanded system access and capabilities. Removing this access can mitigate the potential damage caused by an attacker who compromises that endpoint.
- Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, rendering it more difficult for hackers to gain access.
- Implement Basic Endpoint Protection Controls such as antivirus software, full disk encryption and patching. Each endpoint in your organization should be equipped with these controls and configured to update automatically.

For Medium/Large Organizations:

In addition to instituting the tips for Small Organizations be sure to incorporate the following

- Automate the provisioning of endpoints. When using value-added resellers (VARs), ensure they preconfigure endpoints before delivering them to your enterprise.
- Use Mobile Device Management (MDM) technologies. MDM technologies manage the configuration of devices connected to the MDM system.
- Implement Endpoint Detection and Response technologies. These technologies allow cybersecurity departments to query large fleets of endpoints for suspicious activity.

For more Endpoint Protection Systems practices, please visit www.phe.gov/405d 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!