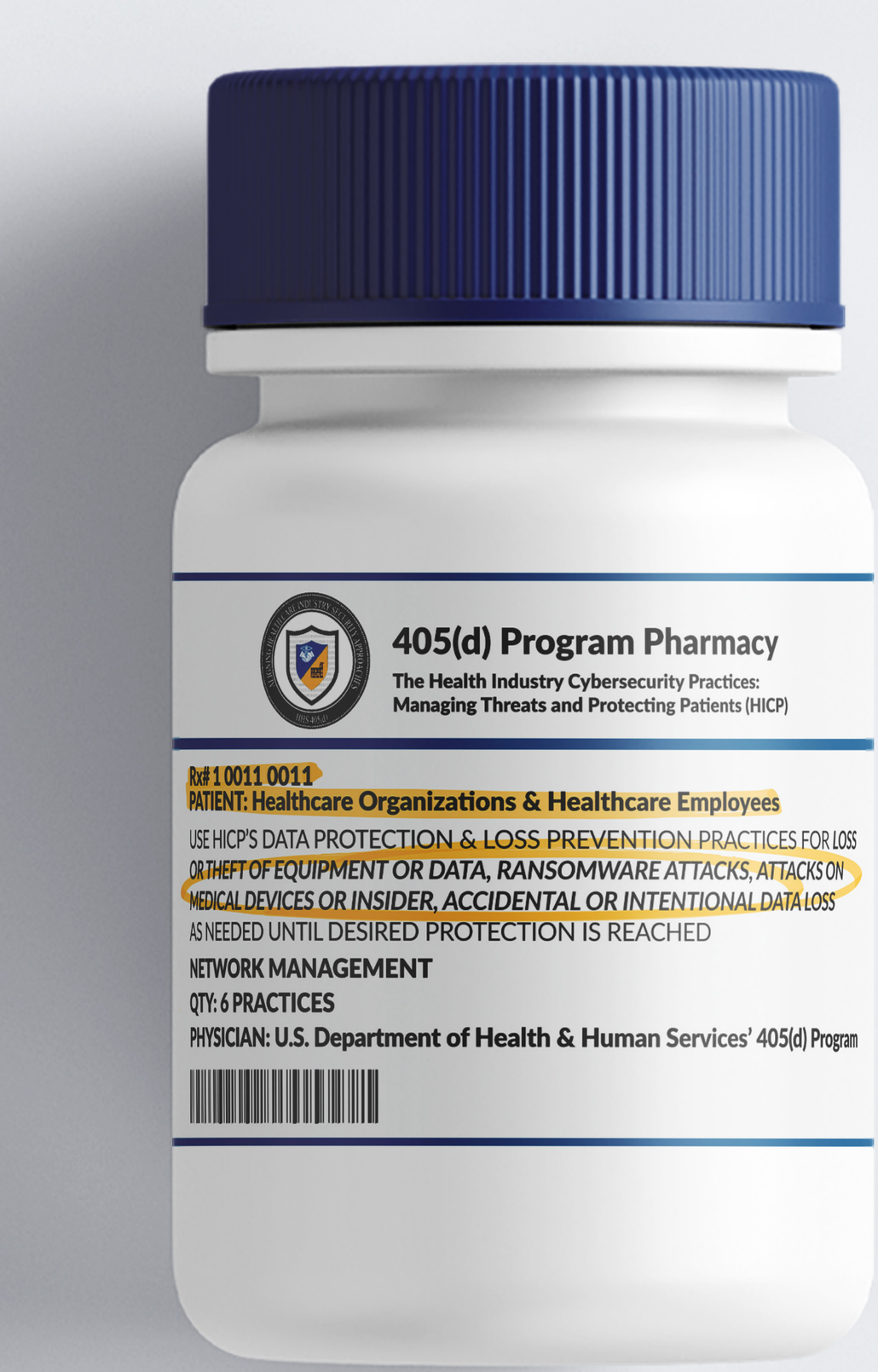

PRESCRIPTION:

Network Management

Computers communicate with other computers through networks. These networks are connected wirelessly or via wired connections (e.g., network cables), and networks must be established before systems can interoperate. Networks that are established in an insecure manner increase an organization's exposure to cyberattacks.

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

For Small Organizations:

- Network Segmentation: Configure networks to restrict access between devices to that which is required to successfully complete work. This will limit cyberattacks from spreading across your network.
- Physical Security and Guest Access: Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. As much as possible, limit the ability of your workforce to access guest networks.
- Intrusion Prevention: Implement intrusion prevention systems as part of your network protection plan to provide ongoing protection for your organization's network. Most modern firewall technologies that are used to segment your network include an intrusion prevention systems (IPS) component.

For Medium/Large Organizations:

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

- Establish Network Profiles and Firewalls. An effective network management strategy includes the deployment of firewalls and network profiles to enable proper access inside and outside of the organization.
- Implement Web Proxy Protections. Web proxy systems provide important protections against modern phishing and malware attacks.
- Utilize Network Access Control systems. NAC systems are engineered to automatically profile new IT assets that connect to network resources, such as wireless networks, wired networks, or VPN.

*For more Network Management Systems 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!*