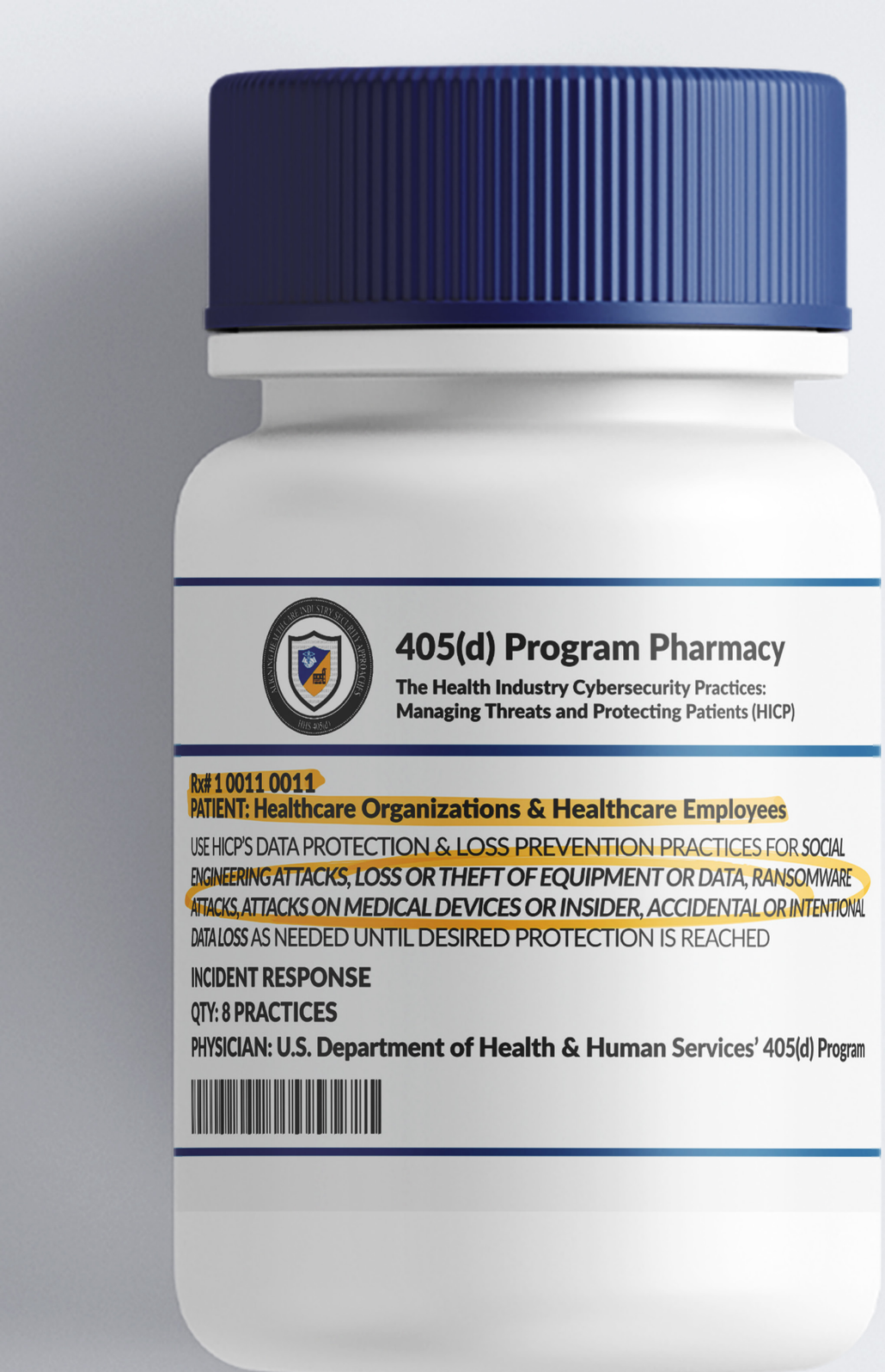

PRESCRIPTION:

Security Operations Center & Incident Response

Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breach or loss. Incident response is often referred to as the standard "blocking and tackling" of information security. Many types of security incidents occur on a regular basis across organizations of all sizes. Two common security incidents that affect organizations of all sizes are 1) the installation and detection of malware, and 2) social engineering attacks that include malicious payloads (via attachments and links).

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

For Small Organizations:

- Establish and implement an incident response plan. Before an incident occurs, make sure you understand who will lead your incident investigation
- Execute your incident response plan. Once your incident response plan is implemented, ensure compliance with the plan's elements. At minimum, your plan should describe steps to be followed in the event of malware downloaded on a computer or upon receipt of a social engineering attack.
- For malware attacks a good response is to re-image, rebuild, or reset affected computers to a known good state. For social engineering, identify malicious e-mail messages and delete from mailboxes and also identify malware that might have been installed on computers, and remediate appropriately if present.

For Medium/Large Organizations:

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

- Establish a Security Operations Center. A SOC is an organizational structure that leverages cybersecurity frameworks, people, tools, and processes to provide dedicated cybersecurity operations. Also utilize robust playbooks in your response process.
- Engage in Information Sharing and Analysis Centers or Organizations (ISACs/ISAOs). ISACs and ISAOs' primary function is to establish and maintain channels for sharing cyber intelligence. No attack is alike therefore we must learn from previous examples including auto threat intel sharing.
- Implement Incident Response Orchestration. This allows you to automate your incident response playbooks.

*For more Incident Response 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!*