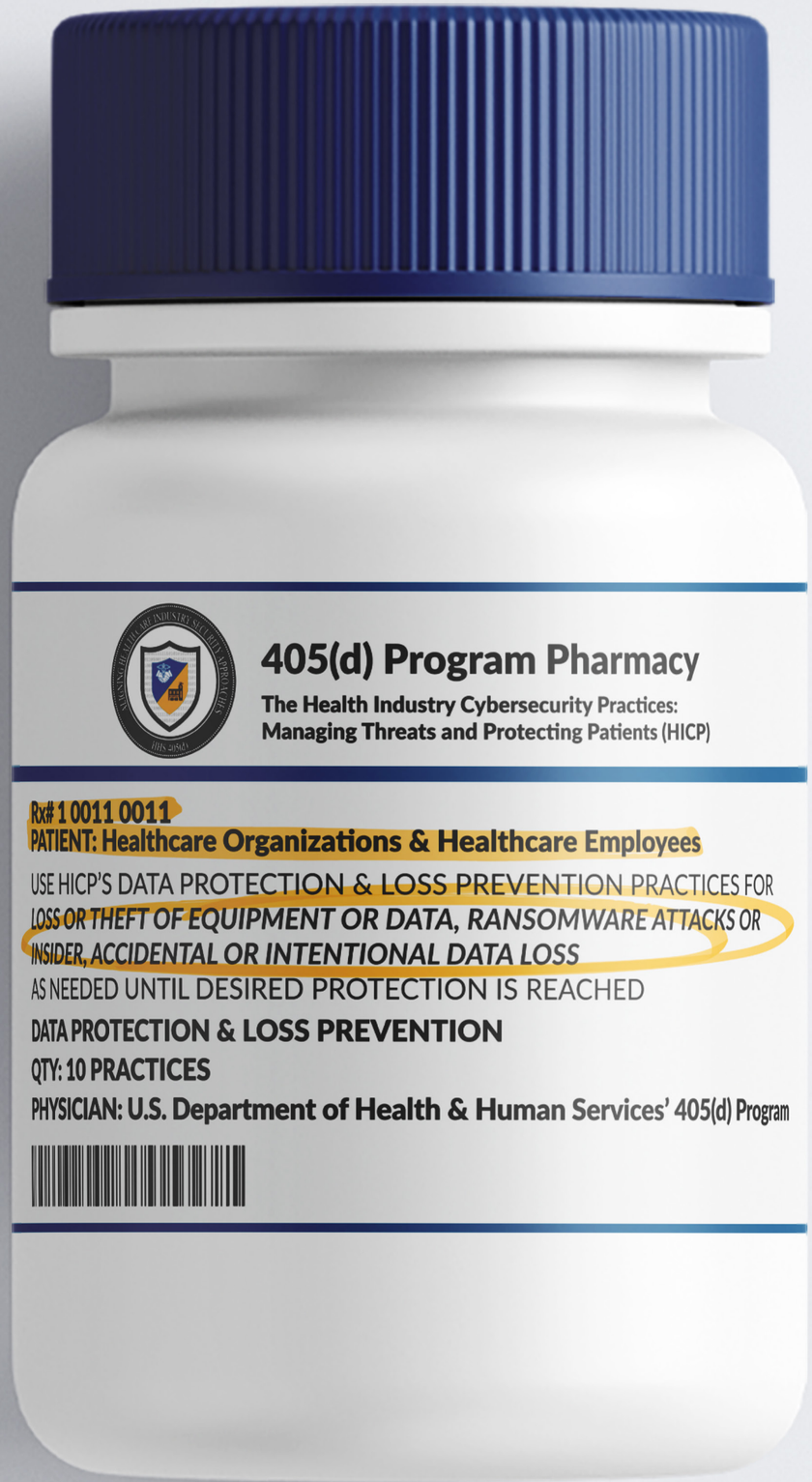

PRESCRIPTION:

Data Protection and Loss Prevention

A security breach is the loss or exposure of sensitive data, including information relevant to the organization's business and patient PHI. Impacts to the organization can be profound if data are corrupted, lost, or stolen.

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

For Small Organizations:

- Instill proper procedures for data protection throughout your organization. These policies and procedures manage sensitive data and can ensure consistency, reduce errors, and provide clear and explicit instructions for users
- Implement proper Data Protection and Loss Prevention Education within your organization.
- Prohibit the use of unencrypted storage, such as thumb drives, mobile phones, or computers. Require encryption of these mobile storage mediums before use.

For Medium/Large Organizations:

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

- Use a classification structure for all of the data you use in your organization. You can prioritize your data using four labels: Highly sensitive, sensitive, internal and public to build a classification scheme and labeling scheme
- Incorporate backup Strategies that encompass each mission critical asset in your environment. Backups can be executed using a variety of methods including disk-to-tape, disk-to-disk, or disk-to cloud backups.
- Establish Data Loss Prevention (DLP) systems. DLP systems should be implemented to ensure that sensitive data is used in compliance with standard data policies and also establish Advanced DLP systems that include cloud storage, onsite file storage, and web-based scanning

*For more Data Protection and Loss Prevention practices, please visit **www.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!*