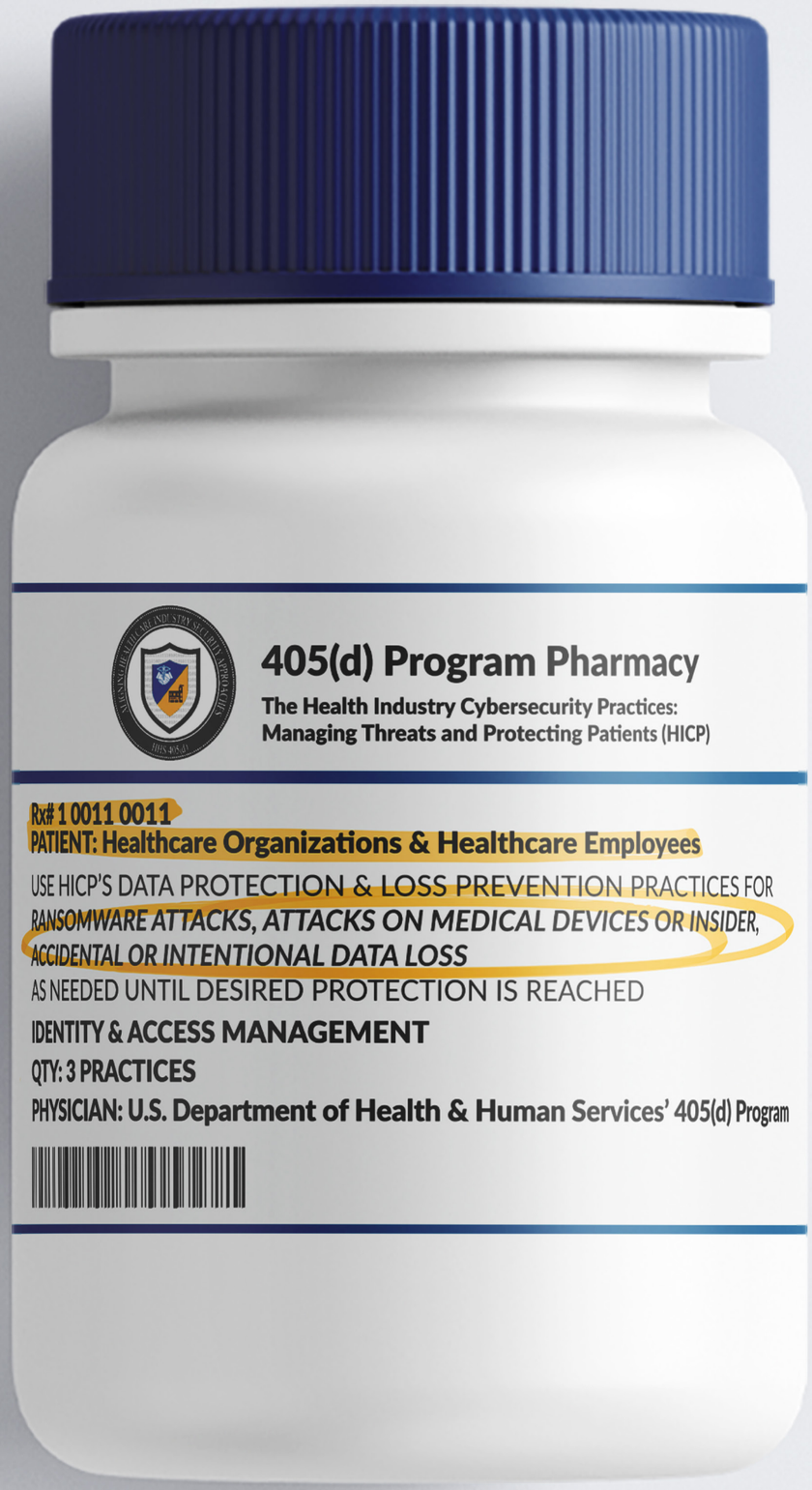

PRESCRIPTION:

Identity and Access Management

Health care organizations of all sizes need to clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Just as you may use a name badge to identify yourself in the physical work environment, cybersecurity access management practices can help ensure that users are properly identified in the digital environment, as well.

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

For Small Organizations:

- Establish a unique account for each user. Also it is important to train and regularly remind users that they must never share their passwords.
- Limit the use of shared or generic accounts. If shared accounts are required, train and regularly remind users that they must sign out upon completion of activity or whenever they leave the device, even for a moment.
- Implement Multi-Factor Authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

For Medium/Large Organizations:

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

- Instill proper Identity Management. Use a "one-person, one-identity, multiple contexts" solution to all access.
- Always ensure the consistent application of attributes, which in turn enables automated authentication and authorization by utilizing automated provisioning and deprovisioning
- Establish Federated Identity Management. Federated identity management enables identity information to be shared between organizations in a trusted manner.

*For more Access 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!*