# How to Implement Data Security

Data Security for Small Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

### What is data security?

A security breach is the loss or exposure of sensitive data, including information relevant to the organization's business and patient Protected Health Information (PHI). Impacts to the organization can be profound if data are corrupted, lost, or stolen. Thus, good data security practices protect the organization and its patients.

### Why is it important?

When security breaches of data occur, it can prevent your employees from completing work accurately or on time and could result in potentially devastating consequences to your patients' treatment and wellbeing. Secure organizational data is not only important for your patients, but also for your organization's financial wellbeing and reputation.

### How will this keep my organization safe?

Properly securing data can prevent your organization from suffering major data losses during a cyber-attack. All staff of an organization, regardless of size, are the first line of defense when it comes to cyber-attacks. If you prepare your work force to recognize and identify potential cyber threats, your patients, and your organization will be more secure.

### Data security mitigates:

- Ransomware
- Loss or Theft of Equipment
- Insider, Accidental, or Intentional Data Loss

## Implementation Tips:

**Train your workforce on your secure email processes.** Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how emails will be used to complete work. Remind employees to be extra careful when sending and receiving emails that contain sensitive and private data, especially Protected Health Information (PHI).

**Train staff never to back up data on uncontrolled storage devices or personal cloud services.** For example, do not permit employees to configure any workplace mobile device to back up to a personal computer unless that computer has been configured to comply with your organization's encryption and data security standards.

**Establish a data classification policy.** Ensure that each data element is protected according to its classification, for example: Sensitive, Internal Use, or Public Use. The sensitive data category should include Protected Health Information (PHI), social security numbers (SSNs), credit card numbers, and other information that must comply with regulations, which may be used to commit fraud, or may damage the organization's reputation. Public use data would include flyers or newsletters that may not need such advanced protections as they do not pose an extreme threat to the organization.


**Train employees on your data classification procedures.** Set the expectation for how your workforce is expected to manage the sensitive data at their fingertips based on your organization's data classification policies. Most healthcare employees work with sensitive data daily, so it is easy to forget how important it is to remain vigilant about data protection. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or compromised data.

*To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages:* **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*