How to Implement Data Security

Data Security for Medium-sized 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?

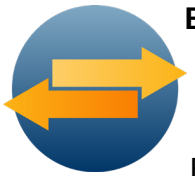
Properly securing data can prevent your organization from suffering major data losses during a cyber-attack. All staff of an organization, regardless of size, are the first line of defense when it comes to cyber-attacks. If you prepare your work force to recognize and identify potential cyber threats,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

Data security mitigates:

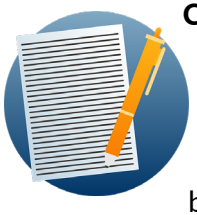
- Ransomware
- Loss or Theft of Equipment
- Insider, Accidental, or Intentional Data Loss

Implementation Tips:

Encrypt sensitive data at rest. Ensure that sensitive data stored on servers are encrypted. If you are utilizing cloud-based services to store your data, enable native encryption capabilities to prevent exposures if the cloud provider is hacked. Restrict users from accessing highly sensitive information, such as SSNs, by masking it unless authorized. Permit SSN access only to members who require it as part of their job function.



Encrypt sensitive data in transit. Ensure that secure transport methods are used for both internal and external movement. Ensure that websites containing sensitive data use encrypted transport methods, such as Hypertext Transfer Protocol Secure (HTTPS). Enable internal encryption methods when moving data in the organization. Never send unencrypted sensitive data outside of the organization.



Confirm that your data retention policies are enforced. Set retention policies and quotas on e-mail systems to reduce the amount of data that can be exposed. Ensure that legal retention requirements are met for documents that are required to remain in your possession for longer periods of time. If your document retention procedures are outsourced to third-party vendors, ensure they are contractually bound to destroy your data when terminating contracts. Use standard destruction forms and require vendors to attest that data have been destroyed pursuant to those forms.

Train personnel on how to identify what types of data should be protected. Data can easily be used to commit financial fraud or cause significant damage to the organization's reputation. Examples of such data for patients include SSNs, credit card numbers, mental health information, substance abuse information, and sexually transmitted infection information. Access to these data should be restricted to users who require it and who demonstrate proper authentication at login. Such data must be managed in compliance with applicable regulatory requirements.

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!*