How to Implement Data Security

Data Security for Large 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:

Utilize cloud storage for sensitive data. Use cloud access security broker systems to monitor data flows into cloud systems. Label data identified as sensitive. Implement digital rights and encryption to limit access to sensitive data. Ensure that cloud-based file storage and sharing systems do not expose sensitive data in an “open sharing” construct without authentication.

Implement secure storage for inactive devices on your network. Assets that are not in circulation should be returned to the appropriate IT department for secure storage. Storage areas should be secured with physical access controls. Access should be limited to those who require it. Physical access controls may include badge readers, video camera surveillance, and door alarms. If an asset is identified for redeployment, it should be securely imaged to deploy a “fresh” computer system for the new user. This ensures that old, sensitive data are removed, and that the asset has a clean bill of health.

Consider Implementing Data Loss Prevention (DLP) software in your organization. Traditionally, DLP systems monitor email, file storage, endpoint usage, web usage, and network transmission. Prevent data breaches by monitoring the use of sensitive data on the network. Multiple DLP solutions exist and can be applicable depending on the types of data access channels that need to be monitored.

Create processes to control access to data backup files. With cyber-attacks like ransomware, attackers intend to disrupt both production and backup files. Attackers that launch ransomware attacks are aware that an organization’s first response will be to contain the ransomware and then restore the uncorrupted files from a backup source. Implement access control mechanisms that will prevent the system being backed up from accessing the disk storage, except by required access channels. This will add an extra layer of security around your data backup files.

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!*