The Health Insurance Portability and Accountability Acts of 1996 (HIPAA) led to the development of regulations surrounding protected health information (PHI) in any form or media, including electronic (ePHI), paper or oral. These regulations have widespread implications for state and local governments as HIPAA-protected information exists in documents supporting public health departments, health and human services, information shared by state authorities and more.

Skagit County, WA, worked with the U.S. Department of Health and Human Services to develop a framework for HIPAA compliance. Mike Almvig, Skagit County’s Director of Information Services, has been instrumental in applying policies and procedures for managing Skagit County’s ePHI; here, he shares lessons learned and best practices for government organizations navigating HIPAA compliance.

The lessons shared herein address the issue of management of unstructured documents containing ePHI, which are documents such as Microsoft Word, Excel and Adobe PDF. These practices may not be applicable to database systems.

SKAGIT COUNTY: SPREADING THE WORD

In 2014, Skagit County, WA, was involved in the first Health Insurance Portability and Accountability Act (HIPAA) violation settlement with a county government. The county was fined for a security breach in which individuals’ electronic protected health information (ePHI) was accessed by unknown parties after being inadvertently moved to a publicly accessible server.

Skagit County turned the series of unfortunate events into an opportunity for education and improvement. Mike Almvig, Skagit County’s Director of Information Services, was part of the team tasked with developing a framework for HIPAA compliance—a time-intensive and meticulous process requiring an intimate knowledge of HIPAA requirements and the guidance of the U.S. Department of Health and Human Services.

Today, Almvig speaks to other organizations that host HIPAA-protected information to spread awareness of potential vulnerabilities and share best practices.

“Many organizations are aware of the HIPAA requirements, but have not performed a full vulnerability assessment and do not fully grasp the severity of a breach,” Almvig says. “There are costs to breaches that more than warrant a discussion with your organization about security measures and risk assessment.”
Audit Controls

HIPAA requires covered organizations to implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, as outlined in 45 CFR § 164.312(b). To satisfy this requirement, Almvig recommends that organizations:

- Implement Laserfiche Audit Trail, which enables organizations to track activities performed in an electronic repository. Information about who accesses and makes changes to documents is logged and used in reports that Audit Trail generates to show an organization's compliance with HIPAA.
- Use Active Directory as a compliance tool that allows designated government employees to manage access rights to ePHI for individuals without exposing ePHI to access rights managers.

Information Access Management

Organizations in compliance with HIPAA have technical policies and procedures in place for authorizing access to ePHI to authorized personnel, for example, through access to workstations, transactions, programs, processes or other mechanisms (45 CFR § 164.308 (4)(i)). Additionally, compliant organizations apply access authorization policies to establish, document, review and modify a user’s right of access to a workstation, transaction, program or process. Access to ePHI should be role-based and limited to the “minimum necessary.”

To address these tenets, Almvig suggests that organizations:

- Use Laserfiche Authentication service, enabling users to implement policies and procedures for accessing ePHI such as enabling two-factor authentication for remote access.
- Apply a “two-person rule” to grant or modify access that aims to ensure employees in charge of managing the active directory are making appropriate decisions. For example, have one person in IT give access in Active Directory, then have another department, such as the health department, audit the Active Directory group.

---

**Track activities taken on secured electronic records using Laserfiche Audit Trail.**
**Data Segregation**

How data is organized plays a critical role in access management. In addition to storing HIPAA-protected data on a separate server, organizations should ensure repository design and folder structure segregate information in a way that allows for effective ePHI access management (45 CFR § 164.308 [4][i]). Almvig explains that compliant organizations:

- Maintain a separate server and repository for ePHI.
- Develop a folder structure within that repository based on HIPAA-protected data types using Laserfiche Repository Administration, enabling organizations to apply unique security settings to various folders and subfolders. This allows for data segregation and access tracking. For example, all information related to tuberculosis would be contained in a different root folder than information related to mental health, ensuring that users with access to tuberculosis information are not unnecessarily given access to mental health data, and vice versa.
- Assign an asset number to each folder and track folders as if they were a physical asset.

Many organizations are aware of the HIPAA requirements, but have not performed a full vulnerability assessment and do not fully grasp the severity of a breach.

**Mike Almvig**
Director of Information Services, Skagit County
Workstations

HIPAA Technical Standards outline that policies and procedures surrounding workstations should specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings in a specific workstation or class of workstation that can access ePHI (45 CFR § 164.310 (2)(b)). Workstations that access ePHI should also have physical safeguards to restrict access to authorized users (45 CFR § 164.310 (2)(c)).

To ensure that workstations are in compliance with HIPAA rules, organizations should:

• Implement policies and procedures for securely processing information that is captured from scan stations. If you’re using Laserfiche Quick Fields, then look at where the ePHI is being caught and secure accordingly. If it’s on a hard drive, make sure you’re securing the hard drive.
• Track and certify destruction of any hard drive (server, workstation, laptop, etc.) that contained, even temporarily, ePHI.
• Ensure that the transmission of data containing ePHI is secured and encrypted between the workstation and wherever ePHI is moved.
• Encrypt the workstation hard drive so that unauthorized removal does not compromise any ePHI that may have been stored on it.

Encryption

Encryption is an addressable implementation specification in HIPAA compliance (45 CFR § 164.312 (A)(2)(iv)). If an organization chooses not to encrypt data, however, it must document why encryption would not be reasonable and appropriate, and implement an equivalent alternative measure if reasonable and appropriate.

Addressable implementation specifications are still advisable, according to Almvig, who recommends:

• At a minimum, encrypt data at rest using Laserfiche encrypted and secured volumes.
• Encrypt data in transmission by establishing a virtual private network and firewall as data is transmitted through the network from the workstation to the data center.
• Implement policies, procedures and training for exporting content from the data center to laptops, USB drives and other mobile devices.