Take the First Step in Achieving Compliance: Implementing a Records Management Program Is Critical

Most businesses don't understand the needs of document management.

Companies in all industries must be compliant and protect their important documents, digital or hard copy. From the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Gramm-Leach-Bliley (GLB) Act to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and Sarbanes-Oxley (SOX). If not, they may face fines and possible criminal charges.

Determining what your company needs to do in order to comply with all these rules and regulations can be a difficult undertaking. DoxVault can help you navigate the jungle. For example, FACTA details how businesses must dispose of information in consumer reports and records but only provides recommendations on what proper disposal involves. We use double cross shredding techniques to help you dispose of sensitive documents. Meanwhile, SOX requires accounting firms to keep audit work papers for seven years and imposes penalties if a business inappropriately destroys its records. If it is physical storage or cloud storage, we use the most up-to-date polices and procedures to keep your records secure for the life time of the record.

Developing a Compliant Records Management Plan

When developing a compliant program, one of the critical decisions to make is whether to rely on internal resources or to utilize the services of a records management provider. This decision is made easier when considering the costs involved. When handled in-house, managers spend an average of four weeks each year searching for or waiting on misfiled, mislabeled, untracked or lost information. Office workers can waste up to two hours a day looking for misplaced paperwork. Large organizations also lose a document every 12 seconds while the average cost of recreating a one-page document is $180.

Along with the decision on how to store records, other key areas that need to be considered for the program to be successful are:

Development of a records retention policy and procedures

Workflow to organize data

Proper Destruction of Records

Disaster Recovery Plans

The retention policy dictates how long a record should be stored before it is destroyed. To develop an effective policy, the company must first have a thorough understanding of its record types. Research must be conducted to determine what compliance rules at the federal, state, and local levels need to be followed based on these record types. Whether dealing with electronic files or hard copies, the company must be able to account for this information in order to be compliant. Following compliance guidelines as well as the needs of the department will help determine how long these records must be kept before they can be destroyed.

The next important step is to properly organize the records by title, name, or detail. Then store them in a secure location. Doxvault will be able to store these records utilizing, system-driven workflows, and

your specific requirements. This approach protects your records while keeping them easily accessible. If a company needs to find a specific document, it can be located immediately using the index and inventory system. Storing records in-house would require a significant investment in space, time, or personal and run the risk of not being able to find the documents.

Once a record reaches the end of its lifecycle based on the retention policy, the company should ensure its proper destruction. The FTC considers proper destruction to include burning, pulverizing, or shredding the information so that it is unreadable and can't be reassembled. If using a records destruction vendor for this process, a company should require a written report and authentication of records that are ready for destruction, prior written approval, final verification, certified shredding, and the creation of a Certificate of Destruction as proof of compliance.

Disaster recovery plans is another key area of the records management program. By keeping the data off-site, or in the cloud. A company can reduce risks should disaster strike. After all, it doesn't matter to the government why a company can't produce a file. Just like with hard copy records storage, data should be inventory to quickly track the location of files. The off-site location should be in an environment combined with cutting-edge security systems to ensure the safe storage of data.

Since many of the steps involved in the compliance process are typically not part of a company's core business, it makes sense to utilize the services of records management providers. We have the experience to help companies develop a program that is both compliant and meets all of their business needs. And by taking advantage of economies of scale, these providers usually cost significantly less than if a company handled all the steps involved in records management internally.