Document Retention and Destruction: Regulations and Best Practices for Financial Institutions

LORMAN®

Published on www.lorman.com - December 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

There are many problems that record retention policies present, well beyond the destruction and the retention of records that would be adopted by companies is there were only commercial concerns such as management of risk and corporate governance to deal with. However, there are many other concerns such as financial and emotional consequences to deal with when deciding on policies of document retention.

Litigation discovery as well as document retention has built itself up to be quite an industry, with many vendors offering their services based upon the new guidelines that are becoming accepted across industry lines. Businesses must also attempt to incorporate new media into their document retention and destruction policies – for instance, are Facebook and Twitter emails subject to the legal and financial ramifications of corporate scrutiny such that they must be included in document retention policies? If so, what is the appropriate procedure to make sure that all of these issues are properly taken care of?

Overall, a company owes it to itself to educate the management and then the employees in generally accepted policies on documentation destruction and retention. Every company now has overarching guidelines that it must follow based upon both political and corporate governance; however, the success of a company in this endeavor will also rely on the independent ability of employees to properly interpret the more vague aspects of document retention policy.

When it comes to financial companies as well as other companies who handle sensitive information from clients, it is very important that a business follow the Federal Rules of Silver goal Procedure, as those procedures have recently been modified to include electronic data inside of its discovery rules along with its governance over paper documents. It is also up to these companies to communicate their policies and how the company will interpret federal policies to their customers so that potential clients will understand exactly what kind of company they are doing business with before any documentation that would be better served under other interpretations of a federal document retention policy would be appropriate.

In-house counsel should be an expert on the more important aspects of federal documentation retention policy. Meet and confer requirements, schedule agreements, any negotiation of easily accessible electronic and paper data, issues of privilege, good faith safe harbors and good faith loss should be all within the wheelhouse of any attorney who claims to represent a financial institution with a reputation.

Typical Document Retention Policy

Document retention and destruction policy for smaller companies that do not have to undergo the full brunt of scrutiny from the federal government may be simpler than some larger companies. In the simpler cases, the typical document retention policy will be divided into two major categories. The first category will be comprised of records that can be discarded immediately after being viewed. The second group of documents are known as "designated retention" documents. These documents will need to be retained either permanently or for specified periods, depending on the appropriate nature of each individual document.

Of course the retention of documents, even electronic documents, is much more expensive than immediate discarding. It is also more time-consuming for company. This will naturally lead most companies to want to discard any documents that do not need to be maintained. However, even smaller companies will need to understand the emotional ramifications of any document retention policy, as even a general destruction policy that does not take into account the nuances of recent political events will raise the ire of certain inferences in different types of litigation.

It should always be policy that document retention policies are to be reviewed as well as approved by senior management. Documents retention policy should also be changed according to federal mandate. When a policy is reviewed, approved or changed, it should be communicated to all relevant employees and enforced with a steady hand across all divisions of the company. Any violation of a document retention policy should be treated quite seriously, even if there are no immediate outside ramifications. If a company has an in-house counsel, it should take the lead in becoming proactive concerning the approval of document retention policies as well as changes to internal policy based upon federal mandate. In-house counsel should also take an active role in training employees in learning new aspects of a document retention and destruction policy.

All document retention policies should adhere to the Sarbanes-Oxley Act of 2002. This act requires all auditors of US companies that are public to retain audit workpapers as well as all related information for at least seven years after the conclusion of the audit. If a company is audited, all care should be taken to adhere to this policy. Sarbanes-Oxley is actually quite strict in its punishments of anyone who is in violation of this policy - destroying a document that is relevant to an audit before the seven year period is a criminal offense. Employees of all companies, including public and private companies, are subject to this punishment, and there are many cases of employees in many different types of companies having undergone federal scrutiny because of a liberal interpretation of a document destruction policy. The moral of the story: Err on the side of caution when dealing with the federal government, no matter what size company you may be.

Document Retention Policy When it Comes to Electronic Records

The destruction of electronic records should raise no more concern than that of a paper record; however, because of the changes in procedure in many federally regulated industries such as medicine, electronic records have actually become more important to keep. Many companies are actually opening entirely new divisions solely for the upkeep and maintenance of electronic records. Although these records are easily created and destroyed, they are still able to cause a great deal of trouble for any company that is under federal audit.

At the instant that any type of regulatory proceeding or litigation becomes foreseeable, it is usually the best practice of a company to place an immediate hold on all sources and documents that may be relevant to the proceedings.

Best practices usually does not include any sort of automatically destruction policy, especially in the instance that any type of regulatory proceeding or litigation is in the foreseeable future. There is a real risk of sanctions when it comes to the destruction of electronic documents to the same extent that there is with text documents. There are many cases in which companies have been sanctioned by the federal government for failure to produce emails that would have otherwise been considered rather innocuous; however, simply because they were not able to be produced, the company underwent the full brunt of sanctions that the federal government could offer.

Litigation holds are an aspect of the law that all companies should consider in their document retention and destruction policies. Litigation holds should be triggered at the same time that any type of litigation is in the foreseeable future.

Additional Policy Considerations for Large Companies

Larger companies that have the potential to do business with the federal government directly should make it a point to adhere very closely to the Sarbanes-Oxley Act as well as write in cautionary procedures to retain all records that have to do with any type of interaction with the federal government.

Large company should make it a point to store all emails that have to do with audience and internal procedures that are performed in conjunction with those audits.

In order to make room for more relevant emails, personal communication on company hardware should be limited, if not outright banned. If personal communication is found on company machines, best practices dictate that this electronic communication is usually archived permanently. Instant message communications that are found to be personal should undergo the same scrutiny as emails. Punishment should be swift and decisive even if there is no immediate external reaction.

Best practices usually always dictate that employees will have no expectation of privacy when using company machines. This will help to deter personal communications. It will also provide legal cover when an email that is deemed to be personal and outside of the realm of the business must be used in conjunction with any litigation that does have to do with the business.

Best practices also usually dictate that all emails that are sent to the audit committee of the company that are related to complaints on frauds, internal controls, accounting or auditing should be retained permanently.

Best practices usually dictate that any correspondence that is made between a company and third parties such as auditors or consultants should be kept permanently, or at least archived, regardless of the content that is contained in those emails. Instant messages should take the same kind of prevalence as emails in this situation.

Finally, any emails that are sent inside the company that relate to audit workpapers or any type of financial controls should be kept, at minimum, for seven years. These are the types of documents that are most likely to be called upon in litigation.