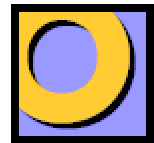


The Impact of Regulations on Email Archiving Requirements



an Osterman Research white paper
sponsored by



Why You Should Read This Report

Email is now just as admissible in court, and just as critical for an enterprise to maintain, as are its paper-based records.

Email has become the lifeblood of the modern enterprise: it has supplanted paper-based and verbal communications as the most critical single element of the corporate communications infrastructure. The vast majority of organizations now consider email a viable and trusted medium for taking orders, giving approvals, formalizing contracts and discussing sensitive personnel issues. Consequently, the corporate email system now contains a great deal of sensitive information that once was stored only on paper.

As dependence on email and its use have grown, so has the governmental and legal scrutiny regarding email. Email is now just as admissible in court, and just as critical for an enterprise to maintain, as are its paper-based records.

Complicating the issue is the rapidly increasing volume of email communications and other information contained with the messaging infrastructure. Osterman Research has found that approximately 60% of the critical business information that the typical email user requires for his or her job is stored within the email system. Further, email system storage growth increases by 40% or more each year because of the growing use of email, increasing use of attachments, and increased user reliance on email, among other factors.

Poor records retention practices expose the enterprise to a host of legal problems, potentially heavy fines imposed by regulatory agencies, a loss of reputation and other problems.

Every Enterprise is at Risk

All enterprises must retain the data within their email systems. Although enterprises in the financial services and healthcare industries face the most difficult data retention requirements, *all* enterprises in *all* industries are required to maintain records in email and other electronic media. Complicating the issue is that there are literally thousands of data retention requirements in the United States and elsewhere.

Poor records retention practices expose the enterprise to a host of legal problems, potentially heavy fines imposed by regulatory agencies, a loss of reputation and other problems. Because an archiving system can prevent the vast majority of these problems from occurring in the first place, the wisest strategy for any enterprise is to deploy an archiving system so that it can get control of its email before it becomes a problem.

Overview

Most of the regulations regarding document retention focus on records retention, not on the specific medium that is used to transmit or house records. In other words, these regulations focus on content and do not distinguish between records that are transmitted on paper or those that are transmitted electronically, such as through email.

The distinction between email and paper-based media with regard to its admissibility as a "record" in court has essentially disappeared.

Email has been recognized as an acceptable means of transmitting and documenting statements of public policy, and so the distinction between email and paper-based media with regard to its admissibility as a "record" in court has essentially disappeared. For example, according to the *Federal Rules of Civil Procedure*, electronic documents are now treated no differently than paper-based documents. At the state level, the Illinois Supreme Court, for example, ruled in 1995 that the definition of "documents" includes "all retrievable information in computer storage".

Email, in and of itself, is a transmission medium for content that may or may not be valuable. An email that contains information about an upcoming lunch date between co-workers, for example, is more or less useless after the date has taken place and typically does not need to be archived. An email that contains a broker's official comments on the financial health of a company, on the other hand, probably will need to be kept for many years because its content constitutes a record of a corporate viewpoint. Therefore, it is critical for any archiving system to be able to separate the "wheat" from the "chaff" and to store only that information that is critical for the enterprise to maintain on a long term basis. Doing so allows an enterprise to maintain control over its archiving storage requirements and it speeds the compliance process in the event that email-based information is required to satisfy a regulatory or legal requirement at some future date.

Most Businesses Are Not Archiving Properly

Osterman Research surveys have demonstrated that fewer than one-half of enterprises keep their critical email-based data for long periods. Some organizations simply delete all old emails after a set period regardless of statutory or contractual requirements, although they do so at their peril. For example, Federal regulations require that some types of critical information about employees be maintained for one

year, some require retention for six years, some for 30 years and some indefinitely.

Another problem is that some jurisdictions require the recipient, and not the sender, to handle email properly. For example, the North Carolina Public Records Act makes the recipient of an email the legal guardian of the message and the person responsible for ensuring that any content within the email that constitutes a record is handled properly. This further increases the liability of an organization that is governed by such a statute, since the recipient becomes the legal guardian of the emails that it receives, as well as those that it generates.

The Role of Archiving

Email has now become a critical part of the record-keeping requirements for the enterprise, simply because email is now used to transmit and house *records* – information that is critical to the enterprise because it contains information that must be retained on a long-term basis because of statute, legal necessity or some other reason. Consequently, the ability to archive this information has become a critical component of the records-keeping practices of any organization that uses email to conduct business or transmit important business information.

All industries face email archiving requirements, some more stringent than others – consequently, there is no industry that is truly “unregulated” with regard to record retention requirements.

Industries Impacted

All industries face email archiving requirements, some more stringent than others – consequently, there is no industry that is truly “unregulated” with regard to record retention requirements; rather, some industries are simply more regulated than others. A summary of the major regulatory requirements as they apply to document retention is shown in the following table.

Summary of Email Archiving Requirements

Industry	Key Regulatory Bodies/Statutes	General Requirements
Financial services	Securities and Exchange Commission (SEC) National Association of Securities Dealers (NASD) New York Stock Exchange	Maintenance schedules for records How records are to be maintained How records of communications with clients are to be maintained and supervised
Healthcare and life sciences	Health Insurance Portability and Accountability Act (HIPAA) Medicare Conditions of Participation Food and Drug Administration	Maintenance schedules for records Disposition of records Standards for data centers that house records

**Summary of Email Archiving Requirements
(concluded)**

Industry	Key Regulatory Bodies/Statutes	General Requirements
Government agencies	General Records Schedules from the National Archives and Records Administration Wide range of statutes and other requirements	Each agency develops its own retention policy
Automotive	Auto Industry Action Group (QS-9000)	Maintenance of quality performance records, internal quality system audits, documents relating to tooling records
Lumber	American Lumber Standards Committee	Maintenance schedules for records
All commercial enterprises	Sarbanes-Oxley Act Gramm-Leach-Bliley Act Internal Revenue Service Fair Labor Standards Act Americans with Disabilities Act Occupational Safety and Health Act Title VII of the Civil Rights Act of 1964 Wide range of other statutes and requirements	Maintenance schedules for records How records are maintained

Regulated Industries

To some extent, and in many countries, there are records-retention requirements for all organizations that are applicable to email. However, financial services, healthcare and government organizations are more heavily regulated with regard to their record retention requirements.

There are records-retention requirements for all organizations that are applicable to email. However, financial services, healthcare and government organizations are more heavily regulated with regard to their record retention requirements.

In addition to the basic records-retention requirements imposed by the Internal Revenue Service, various employment-related statutes, and so forth, these industries face additional requirements that can be quite difficult to satisfy. For example, brokerage houses must comply with a variety of SEC and NASD requirements that impose specific periods for retention of communications with customers, including requirements that dictate the ease of accessibility to these records for the first part of their storage period. There are also requirements that dictate the media on which these records can and cannot be stored.

Complicating the issue is that the SEC, for example, can impose significant fines for non-compliance with these regulations. Because some of the requirements are open to interpretation, regulated companies in this space face significant financial risk of either not complying with the regulations or falling short of their requirements. In short, organizations that are heavily regulated have a critical need for email archiving technology that can satisfy the myriad and changing regulations imposed upon them.

“Non-Regulated” Industries

Among enterprises whose industry-specific data retention requirements are less stringent, there is currently a debate regarding the archiving of emails and other electronic documents. For example, some IT managers within these enterprises believe that all content should be archived so that corporate knowledge held in email is retained. Other managers believe that email should be deleted regularly in order to reduce the liability that may arise in the event of a lawsuit or government inquiry. Essentially, there are three basic views on the issue of archiving email:

- **Delete all email regularly.** One group believes that all email should be deleted on a regular schedule, typically kept no longer than 90 days, so that potentially incriminating evidence will not be available during the discovery phase of a legal action or during a government inquiry. Those in this camp find justification for their position in cases in which archived emails have

harmed the organizations that kept them, such as the several internal emails written by Microsoft's Bill Gates that were presented as evidence against Microsoft in the US government's legal action against the company. Arguing against this position is that courts can instruct juries that if a party to a legal action destroys documents, there is a presumption that the documents were damaging to the destroying party.

- **Keep all email for long periods.** Another group believes that all emails should be kept for long periods, that they should be made accessible via archiving and tracking tools that permit an audit trail to be maintained, and that access to archived content should be permitted to employees and others for long periods of time. This view is held by those who are a) averse to risk and believe that it is better to know about damaging evidence so that its harm can be minimized through the application of appropriate legal or other strategies; and b) those who desire to extract corporate knowledge from the information stored in messaging systems.
- **Keep only important email.** A third group believes that emails should be categorized with regard to their importance, and that some of this information should be kept long term, while unimportant information should be deleted regularly. Here, too, this view is held by those who are averse to risk for legal or other reasons, as well as those who want to extract corporate knowledge from the messaging system.

Legal Considerations

Regardless of whether or not an industry is more or less heavily regulated with regard to its records retention requirements, there are several factors for any enterprise to consider with regard to the importance of email retention¹:

- **Electronic documents are now valid and have legal effect.** The legal and regulatory developments prevent the courts from denying legal effect or validity to electronic documents simply because they are in an electronic form. The legal and regulatory controls that apply to paper documents now apply to electronic documents. Parties who rely on or use electronic documents can be liable for their actions and omissions.

¹ Source: Dr. Lars Davies, CEO of Kalypton Limited and Senior Visiting Fellow at the University of London's Centre for Commercial Law Studies.

Without an appropriate archiving system from which emails can be methodically searched and extracted, a court can order that all servers and backup tapes be seized for analysis.

- **During discovery, all emails are subject to review.** Without an appropriate archiving system from which emails can be methodically searched and extracted, a court can order that all servers and backup tapes be seized for analysis.
- **Courts no longer accept the argument of technical difficulty when dealing with the legal issues surrounding email use.** For example, if an email server runs out of storage capacity and an administrator must delete messages from the server to make room for new content, this is not considered an acceptable defense if a company is asked by a court to provide email messages during a lawsuit.
- **Legal admissibility is now irrelevant when it comes to determining the reliability of evidence.** The focus is now on the evidential weight of the evidence. The strength of the evidential weight directly determines the reliability of that evidence, and the weight that the Court will place on that evidence. Without evidential weight, any evidence is of little real use in any dispute. The side with the greater evidential weight for material matters generally wins. The legal dispute resolution process works with the evidence put before it. The better one side's evidence, the more likely that side is to win the dispute.
- **Regulatory controls on the retention of documents and information are the main driver for electronic evidential weight.** Every commercial or governmental activity requires the production and retention of a record. The regulatory developments simply mean that the electronic versions must be retained for as long as their paper-based versions.
- **Electronic archiving imposes additional demands not required in traditional record-keeping.** In the paper-based world, parties can easily point to a particular copy of a document as the 'master' document, or the original. Evidential weight often begins with this particular copy. In the electronic world, however, this is far more difficult to do. Copies are not sent but are copied from system to system, and the original that existed on a particular laptop or desktop system is not the 'same' copy as that in the archive. Not only must archive systems comply with regulatory controls and retention requirements, but they must also be able to identify the original or 'master'

Electronic archiving imposes additional demands not required in traditional record-keeping.

copy, or at least prove that the copy on the system is identical to the original copy when that copy was in existence and that this copy has not been altered since.

- **Information must be tamper proof.** The problem with electronic information is that it is easy to alter, delete, or even lose; far easier in fact than with paper-based information, as any change or loss can occur without leaving any trace. The problem then is to ensure that information is correctly captured and stored in order to minimize any uncertainty over its integrity and existence so far as is possible.
- **Evidential weight is more than document retention.** Evidential weight requires that all aspects of a message or data are retained; the existence or occurrence, the message itself, any access to the message contents, any attempt to edit or delete the message, and ensuring that the message or document received or created is the message or document that is stored. Just storing a backup or snapshot of a message system is insufficient as is a system that provides a policy for storing messages after a period of time.
- **If a user cannot prove that every document or record has been retained for the correct period, they have not satisfied the evidential weight requirements.** Document and email retention requirements specify the retention period and storage mechanism. They do not affect evidential rules which are quite separate and which apply in addition to these requirements.
- **Archiving emails is the smartest course of action for any organization, even if archived emails are damaging to the company's defense during a legal action.** An organization is better served by understanding the extent of its liability and opting to settle out-of-court rather than have another source produce archived emails that are damaging to the organization.

An inability to satisfy compliance requirements – whether or not this compliance is imposed by a government regulatory agency or a legal action – can be damaging to an organization, both financially and otherwise.

The Risks of Non-Compliance

An inability to satisfy compliance requirements – whether or not this compliance is imposed by a government regulatory agency or a legal action – can be damaging to an organization, both financially and otherwise. For example:

- Five Wall Street brokerage houses – Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney

and US Bancorp – were fined a total of more than \$8 million by the SEC in December 2002 because these firms did not retain certain emails for SEC-mandated retention periods and for other infractions of SEC rules. The SEC investigation that culminated in these fines arose as part of a larger investigation into potential conflicts of interest between the research and investment banking operations at various brokerage firms.

- In *Proctor & Gamble Company v. Haugen* (an independent distributor of Amway products), Proctor & Gamble was fined for destroying email-based records. Proctor & Gamble did not preserve or search for emails relevant to this case that were written by five individuals and was fined \$10,000 for their failure to do so.
- In *Applied Telematics, Inc. v. Sprint*, Sprint was charged with destroying evidence because it continued to recycle its backup tapes even after the legal proceeding brought by Applied Telematics had commenced. The data that Applied Telematics had asked Sprint to produce included routing plans that were housed in Sprint's internal databases. Although there was no allegation that Sprint had intentionally destroyed this data, the Court found that Sprint should have modified its normal backup procedures in order to preserve the data after Applied Telematics had requested it.
- In *Anti-Monopoly, Inc. v. Hasbro, Inc.*, the Court ruled that a defendant that is required to produce documents during the discovery phase of a legal action can also be compelled to bear the costs of designing a mechanism for extracting the information from its computer-based files.
- Related to the above case is *Zubulake v. UBS Warburg*, in which the judge in the case has ruled that a new standard should be established for evaluating whether the plaintiff or the defendant bears the cost of electronic discovery. The judge in this case has taken a decidedly pro-plaintiff approach, meaning that organizations may be more likely to be charged for the costs of electronic discovery where the plaintiff can demonstrate that this discovery would yield information of sufficient importance to a case.

Most of the fines imposed by regulatory agencies and the decisions by the courts have been relatively insignificant as a percentage of the revenues generated by the offending firms. However, these actions, we believe, are “a shot across the bow”.

To date, most of the fines imposed by regulatory agencies and the decisions by the courts have been relatively insignificant as a percentage of the revenues generated by the offending firms. However, these actions, we believe, are “a shot across the bow” and are intended to serve as a warning for firms to more carefully archive their email and other electronic content.

The ultimate intent of Congress and the Courts with regard to records retention requirements may be signaled by legislation like the Sarbanes-Oxley Act, discussed in the Appendix to this document. This Act imposes major criminal penalties for failure to properly maintain records of all types, including email. The passage of the Act was prompted by the failure of several high profile accounting firms and their clients to adequately maintain proper records and the subsequent crisis in investor confidence that these failures created. Sarbanes-Oxley imposes new federal oversight provisions on public companies and those who maintain their accounting records, including the creation of an oversight board, restrictions on the types of services that firms can provide and stringent processes governing internal corporate controls – including enhanced records management.

Sarbanes-Oxley follows the passage of the Gramm-Leach-Bliley Act of 1999, which also imposes stricter records management requirements on organizations.

What Do You Need in an Archiving System?

The wisest decision for any organization that relies on a messaging system as a key part of its communications infrastructure is to deploy a messaging archiving system.

Simple tape backups, the traditional method for backing up an email system, are not an effective method for ensuring that regulatory or legal requirements can be met, nor are these backups an effective method for gaining access to the wealth of content housed in the typical enterprise's messaging system. Further, backups are much more difficult to manage than a properly implemented archiving system, they require more IT involvement, and they can create much longer email downtime in the event of a server crash or other technical problem.

The wisest decision for any organization that relies on a messaging system as a key part of its communications infrastructure is to deploy a messaging archiving system. Such a system will ideally have all of the following characteristics:

- **No requirement for user involvement.** The primary benefit of such a capability is that the archiving process requires little or no user involvement, thereby increasing productivity for end users and completely eliminating human error.
- **Indexing of all content.** This is particularly useful in meeting the demands that are often imposed by a regulatory audit or court action.
- **End user access to the archive.** Because IT staff members sometimes cannot satisfy all of the requests to recover old content from backup tapes, allowing end users, such as compliance officers or corporate counsel, to access this information themselves can significantly reduce the workload for IT staff and can make archived information more easily available by end users.
- **Protection of archived data from tampering.** A key requirement of many of the content management regulations imposed by government is that data in the archive must be tamper-proof. Also, if content from the archive is accessed, the system will ideally provide an audit trail of who accessed the content and when it was accessed.
- **Flexible storage media options.** Because different regulations may require the use of different types of

storage media, it is important for any archiving solution to provide flexibility in the type of media in which the archive is stored, including magnetic, tape and optical.

- **Enforcement of corporate data retention policies.** A key provision of many data retention requirements is that content must be retained for a minimum period, but that it must not be kept for longer than a maximum period proscribed by statute. An archiving system will ideally permit all data to be kept as long as is necessary, but no longer, allowing data to be removed from the archive easily and in accordance with corporate and/or legal policies.
- **Archiving only required email.** Many organizations are interested only in archiving specific mailboxes, messages from specific domains, or messages from specific email addresses. This limits the content of the archive only to messages and other content that the organization deems necessary, rather than creating an archive of unnecessary content, which might include spam, informal employee communications, employee newsletters, and the like.

About Information Management Research, Inc.

Founded in 1992, IMR is a software company based in Englewood, Colorado. IMR is the developer of Alchemy MailStore, an email records retention and compliance management solution. The Alchemy family of document and record management solutions is trusted by thousands of organizations around the world to manage documents for regulatory compliance and records retention, and to provide business processes with fast access to archived documents. For more information visit our website at www.imrgold.com, call 303-689-0022, or send email to info@imrgold.com.

Appendix

This section provides details on some of the specific statutes and other provisions mentioned in this document.

US Financial Services

There are a variety of US federal government and other regulations that apply to document retention by financial institutions, among which are:

- SEC Rule 17a-3 and Rule 17a-4
- Amendments to Rules 31a-2 and 204-2
- NASD 3110
- NTM 98-11 (Amendments to Rules 3010 and 3110)
- NASD 2860 (b) (17) and 2210 (b) (2)
- NYSE Rule 342

These rules focus on records retention requirements for communications between broker-dealers and their customers, how retained data is to be stored, the ease of its accessibility, how sampling is to be performed to ensure that communications with clients is supervised, and so forth.

In short, these requirements more or less dictate that organizations in the financial services industry implement a set of archiving procedures and policies that will make compliance with the regulations possible, and that will facilitate regulators' demands for compliance.

SEC Rule 17a-3

Every member of a national securities exchange, including all brokers and dealers, must keep current a variety of books and records that relate to his or her business.

SEC Rule 17a-4

Some of the records that must be retained by brokers and dealers must be preserved for at least six years, the first two years "in an easily accessible place"; while other records must be retained for at least three years, the first two years "in an easily accessible place". Examples of the types of records that must be retained for at least three years are the originals of all communications that pertain to the business of the broker or dealer, including memos, emails and other correspondence; financial statements; internal audit working papers; all written agreements; and a variety of other information. All information related to the opening or

maintenance of a customer account must be kept for at least six years.

Further, if records are to be stored on electronic media, the “examining authority” must be notified by the broker or dealer prior to storing records on electronic media. If non-optical disk technology is to be used for this storage, the notification occur at least 90 days before this media is used, and proof must be provided either by the user of the storage system or by its manufacturer that the applicable SEC requirements for document storage will be met by the storage system that is employed. SEC Rule 17a-4 also specifies various requirements for the electronic storage system used to archive relevant records.

Amendments to Rules 31a-2 and 204-2

These amendments permit funds and advisers to maintain all of their records in an electronic format, even if the original records were not created or received in this format, as long as procedures are put in place to protect records from “loss, alteration or destruction”; that access to these records is limited only to authorized personnel; and that “electronic copies of non-electronic originals are complete, true, and legible”.

NASD 3110

The National Association of Securities Dealers requires under this rule that, “each member shall make and preserve books, accounts, records, memoranda, and correspondence in conformity with all applicable laws, rules, regulations, and statements of policy promulgated thereunder and with the Rules of this Association and as prescribed by SEC Rule 17a-3. The record keeping format, medium, and retention period shall comply with SEC Rule 17a-4.” Other provisions of this rule require that each member maintain a record of written complaints from customers or their representatives, and that all records maintained under this rule are subject to the time and accessibility requirements specified under SEC Rule 17a-4(b).

NTM 98-11 (Amendments to Rules 3010 and 3110)

This Notice to Members specifies supervisory procedures for the review of correspondence between individual representatives and the public, and it specifies that each member develop written policies and procedures for the review of such correspondence.

NASD 2860 (b) (17)

This rule requires that “every member shall maintain and keep current a separate central log, index or other file for all options-related complaints, through which these complaints can easily be identified and retrieved.” Further, “background and financial information of customers who have been approved for options trading shall be maintained at both the branch office servicing the customer’s account and the principal supervisory office having jurisdiction over that branch office.”

NASD 2210 (b) (2)

This rule requires that each member retain for at least three years a file of all sales literature and advertisements that have been used by the member firm, including the identification of the individual(s) that either prepared these documents or approved their use.

NYSE Rule 342

This New York Stock Exchange rule requires that “procedures be designed for review of communications between members of the NYSE and the public so that reasonable supervision can be exercised over members’ representatives”. This rule also requires members to create written procedures and policies regarding their communications with the public.

Other Provisions

Sarbanes-Oxley Act of 2002

The Public Company Accounting Reform and Investor Protection Act, also known as Sarbanes-Oxley, proscribes a number of penalties for altering or destroying corporate data. Key provisions of the Act include:

- Anyone who knowingly alters, falsifies, destroys or otherwise tampers with a document or record can be imprisoned for up to 10 years and/or fined.
- Any accountant or accounting firm that audits a firm governed by the SEC must retain all relevant audit-related documentation for five years following the end of the fiscal period during which the audit or review was finalized.

Sarbanes-Oxley represents a turning point in government’s oversight of corporate accounting procedures and records retention policies. While government has always imposed

certain requirements on regulated and unregulated enterprises to retain critical data, Sarbanes-Oxley has major implications for enterprises in two ways:

- First, it raises the bar for records retention by imposing massive penalties for the intentional alteration or destruction of records.
- Secondly, the Act radically expands the records-keeping requirements for public (and even private) companies. For example, while the Act explicitly focuses only on accounting and related procedures, analysts suggest that it may require firms to bolster record-keeping procedures in a variety of other areas, including operations, IT and human resources.

What this means for an enterprise governed by Sarbanes-Oxley is that the maintenance of records is now more critical than it ever has been. Further, because specific interpretations of the Act are still being defined, enterprises governed by it are going to be subject to changing interpretations of specific provisions of the Act for some time.

Government Agencies

All US federal agencies are required to maintain a comprehensive records schedule that specifies each agency's policy regarding the retention and disposal of records. Each agency develops its own retention policy by combining the General Records Schedules from the National Archives and Records Administration, as well as specific policies that it has created. Among the data retention rules that apply to government agencies are the following:

- Electronic Signatures Act
- 36 CFR 1220.34
- 36 CFR 1220.38
- 44 USC 3101
- 44 USC 3106
- US Department of Defense Directive 5015.2
- NPG 1441.1C
- NARA General Records Schedule 20

Electronic Signatures Act

The Electronic Signatures in Global and National Commerce Act, which was signed into law in 2000, allows electronically-created contracts to have the same force of law as contracts that are written on paper. According to the Act,

any government agency's record-keeping obligations may be met solely through the maintenance of electronic records if those records accurately "reflect the information set forth in the record, and remain accessible to all persons who are entitled to access, in a format that can be accurately reproduced".

Further, this Act applies not only to government entities, but to all organizations that do business electronically. A fundamental advantage of the Electronic Signatures Act is that it supersedes all state laws and provides a uniform method for conducting business electronically.

36 CFR 1220.34

"Agencies must institute adequate records management controls over the maintenance and use of records wherever they are located to ensure that all records, regardless of format or medium, are organized, classified, and described to promote their accessibility, and make them available for use by all appropriate agency staff for their authorized retention period. Agencies must also maintain permanent records in a format that will permit transfer to the National Archives of the United States."

36 CFR 1220.38

"Agencies must ensure the proper, authorized disposition of their records, regardless of format or medium, so that permanent records are preserved and temporary records no longer of use to an agency are promptly deleted or disposed of in accordance with the approved records schedule when their required retention period expires. As an intermediate step when records are not needed for current day-to-day reference, they may be transferred to a records storage facility."

44 USC 3101

"The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."

44 USC 3106

"The head of each Federal agency shall notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, or destruction of records in the custody

of the agency of which he is the head that shall come to his attention."

US Department of Defense Directive 5015.2

"Create, maintain, and preserve information as records, in any media, that document the transaction of business and mission in wartime and peacetime to provide evidence of DoD Component organization, functions, policies, procedures, decisions."

NPG 1441.1C

NASA Procedures and Guidelines define a variety of retention requirements for both electronic and non-electronic records, including guidelines for retiring records. This document also includes a section dealing specifically with electronic records and requirements specifically aimed at these record types.

NARA General Records Schedule 20

This schedule provides disposal authorization for certain electronic records and specified hard-copy (paper) or microform records that are integrally related to the electronic records. This schedule applies to disposable electronic records created or received by Federal agencies including those managed for agencies by contractors. It covers records created by computer operators, programmers, analysts, systems administrators, and all personnel with access to a computer.

Healthcare and Life Sciences

The most important healthcare-related legislation dealing with content retention requirements is HIPAA, although there are a number of healthcare-related document retention requirements imposed by the US federal government. Among these regulations are the following:

- HIPAA requires that a wide range of documents, including email messages, be kept for six years. Among the documents that must be maintained for six years are contracts with business associates, all documents related to policies and procedures, communications from patients who wish to modify the information held by a healthcare provider, authorizations and consumer complaints. Also, HIPAA requires that all records about a patient must be retained for two years after a patient's death.

- HIPAA also requires that retained content must be stored in a robust data center that provides minimum guaranteed uptime and very high security, among other requirements.
- HIPAA also imposes strict data disposal requirements, including overwriting or physically destroying all magnetic media that is no longer in use or that is given away or sold.
- The Medicare Conditions of Participation requires hospitals to retain medical records for five years. Medicare requires that medical records be retained for five years as they relate to radiological and nuclear medicine services, and inpatient and outpatient services, among others. Psychiatric hospitals must also retain a variety of medical records for five years. Further, Medicare and Medicaid reimbursement to rural health clinics requires that these clinics maintain medical records for six years.
- The Food and Drug Administration requires that drug makers maintain records of employees' contact, date of birth, compensation and other information for three years.

Canadian Financial Services

The *Universal Market Integrity Rules for Canadian Marketplaces* specify a number of content retention requirements that are similar to those specified for US financial services firms, including the following:

- Dealers and traders must retain information on each order they place, as well as the owner of each account, for at least seven years, the first two years in an easily accessible location.
- All dealers' and traders' firms must make such records available for review and copy to regulators at any time during normal business hours for at least seven years from the date of origination of each order.

The TSX Group, managers of the TSX Venture Exchange and the Toronto Stock Exchange, have also developed their own set of content retention requirements, including a requirement that all Due Diligence Reports and their supporting documentation must be retained for at least six years.

The Investment Dealers Association of Canada (IDAC) has published a *Guide to Record Retention Requirements* which requires that “any documents which would be necessary to defend an action against a Member or support an action by a Member should be kept at least until the appropriate limitation period has expired.” Some provinces, such as Ontario and Quebec, have differing legal requirements. IDAC recommends that its members err on the side of caution and use a seven-year retention period for certain types of documents. For example, IDAC recommends that correspondence with customers be retained for seven from the date that a customer’s account is closed, although health and safety records should be retained permanently.

Canadian Government Requirements

The Canadian Government specifies a variety of content retention requirements, selected portions of which are summarized in the following table.

**Selected Canadian Government
Content Retention Requirements**

Type of Information	Retention Period
Routine activities related to correspondence management	Two years
Monthly, weekly, status, etc. reports and statistics regarding real property management	Three years
Policies and procedures related to motor vehicle and equipment accidents	Five years after superseded (active for two years, dormant for three years)
Information regarding cancelled building projects	Two years after cancellation
Policies and procedures regarding the purchase and issue of medical supplies and drugs	Five years after superseded (active for two years, dormant for three years)
Policies and procedures regarding accounts payable	Six years after superseded (active for two years, dormant for four years)
Routine information regarding accounts payable	Two fiscal years
Reports of minor building fires	Two years after report is made to Dominion Fire Commissioner
Invoices and vouchers from commercial firms, hospitals, suppliers, etc.	Six years after superseded (active for two years, dormant for four years)

**Selected Canadian Government
Content Retention Requirements
(concluded)**

Type of Information	Retention Period
Information regarding bonding of employees	Two fiscal years
Accident and occupational injury or illness investigation reports not related to exposure to a hazardous substance, including related correspondence and the supervisor's Hazardous Occurrence Investigation Report	Ten years
Accident and occupational injury or illness investigation reports related to exposure to a hazardous substance, including related correspondence and the supervisor's Hazardous Occurrence Investigation Report	Thirty years

The National Archives of Canada has published *Retention Guidelines for the Common Administrative Records of the Government of Canada*, which applies to various functions within Canadian institutions. These guidelines are intended for organizations' internal records, but are not truly a mandate from the Government of Canada. Instead, each institution within the Canadian federal government is responsible for the creation and implementation of its own retention periods.

In addition, Canada's Privacy Act also specifies retention periods for various types of government information. For example, if a government institution uses personal information, it is required to retain that information for a regulated period of time so that the subject of that information is provided with an opportunity to access the information that was used. The Privacy Act also requires government institutions to dispose of personal information in compliance with regulations that are issued by the minister in charge of that institution.

The Department of National Defence and the Canadian Forces have also specified retention periods for various types of information. For example, all supporting documentation regarding a payment, such as receipts or contracts, must be retained for at least six years.

The Canadian Income Tax Act, Proceeds of Crime Act and the Canada Business Corporations Act also specify various content retention requirements.

Outside North America

Outside of North America, there are a variety of regulations that govern content retention:

- In the United Kingdom, the Data Protection Act and Freedom of Information Act impose requirements for specific data retention practices. For example, the Data Protection Act 1998 permits any person about whom a UK-based organization holds personal information to have access to that information for a nominal fee. This Act also requires "data controllers", such as employers, to establish procedures to protect personal data. The Data Protection Act, which was originally passed in 1984, was amended in 1998 in order to make UK law consistent with Directive 95/46/EC of the European Union.
- France's Conseil des Marchés Financiers' Decision 99-05, "Keeping of data relating to transactions in financial instruments admitted to trading on a regulated market", requires that documents relating to orders for financial transactions be retained for varying periods from six months to five years.
- In June 2002, in keeping with proposed European Union guidelines on data retention, the Spanish parliament imposed a requirement on Internet service providers (ISPs) to keep data on their clients for a minimum of one year. This followed a May 2002 decision by the European Parliament that permits member states to force telecommunications companies and ISPs to retain data for periods longer than would be necessary simply for billing or other administrative purposes.
- Ireland has imposed a data retention requirement since early 2002 that requires telecommunications companies to maintain records of its customers' telecommunications traffic for a minimum of three years.

For additional information on European guidelines for email retention, contact IMR to request a copy of the article *Email Archiving: An Update From Europe*.

Other Regulations That Apply to All Employers

Although financial services and healthcare firms, as well as government agencies, are subject to strict regulations regarding the retention of messaging system and other content, virtually all firms are subject to content retention requirements. For example, in the United States there are a

wide variety of government-mandated requirements for content retention that apply to employers, while the Internal Revenue Service requires that virtually all firms retain key tax-related records for specified periods. In most cases, these regulations do not call out retention requirements specifically for email or messaging systems, but these regulations instead specify the content that must be retained, regardless of the medium in which the content was transmitted or saved. Because messaging systems are housing an increasing proportion of this content because of the growing use of messaging, these regulations will continue to apply increasingly to messaging as the de facto repository for much of this content.

Data Retention Requirements for Employers

A summary of regulations that apply to most employers is shown below.

Selected US Government Content Retention Requirements for Employers²

Type of Information	Retention Period	Applicable Statute(s)
Written training agreements, summaries of applicants' qualifications, job criteria, interview records and identification of minority and female applicants.	Duration of training program plus three years	Fair Labor Standards Act, National Labor Relations Act
Hiring documents, including job applications, resumes, job inquiries, and records of refusals to hire.	One year from date of personnel action	Age Discrimination in Employment Act
Promotion, demotion, transfer, selection for training, layoff, recall or discharge.	One year from date of personnel action	Age Discrimination in Employment Act
Payroll records, collective bargaining agreements, including any changes, individual contracts, written agreements under the FLSA, sales and purchase records, and certificates and notices of the Wage and Hour Administrator	Three years	Fair Labor Standards Act and National Labor Relations Act
Personnel records of an individual whose employment has been involuntarily terminated	One year from the date of the termination	Americans with Disabilities Act

² Information provided by Jennifer Suich Frank, Esq., Lindquist & Vennum P.L.L.P.

Selected US Government Content Retention Requirements for Employers (cont'd.)

Type of Information	Retention Period	Applicable Statute(s)
Consumer allegations of personal injury or harm to health, reports of occupational disease or injury and reports or complaints of injury to the environment submitted to the manufacturer, processor, or distributor from any source	Thirty years for employee claims of occupational disease or occupational health problems	Toxic Substances Control Act
Records of medical examinations required by law	Duration of employment plus thirty years, unless OSHA requirements provide otherwise	Occupational Safety and Health Act
Records concerning complaints of handicap discrimination, (in programs and activities receiving or benefiting from federal financial assistance) and relevant employment records of charging party and employees in similar positions.	Three years	Rehabilitation Act of 1973
Personnel records concerning any discrimination charge brought by any agency or individual (e.g., records about charging party and all other employees holding similar positions, application forms, or test papers completed by all applicants for same position)	Until final disposition	Title VII of the Civil Rights Act of 1964
Records of monitoring exposure to hazardous materials	Thirty years	Occupational Safety and Health Act
Manufacturers, processors, or distributors of any chemical substance must retain records of employees' "significant adverse reactions" to health or the environment.	Thirty years from date such adverse reaction first reported to or known by person maintaining record	Toxic Substances Control Act

Selected US Government Content Retention Requirements for Employers (concluded)

Type of Information	Retention Period	Applicable Statute(s)
Employee benefit plans (such as pension or insurance plans); seniority and merit systems which are in writing	Duration of plan and for at least one year after plans' termination	Age Discrimination in Employment Act
Any correspondence, inquiries or notes relating to individual eligibility determinations	Indefinitely	Employee Retirement Income Security Act of 1974
Wage and hour records for the purpose of determining retirement benefits.	Indefinitely; alternatively six years following date of lump sum distribution.	Employee Retirement Income Security Act of 1974 and the Fair Labor Standards Act
All personnel or employment records including application forms, resumes, other hiring records; records regarding promotion, demotion, transfer, layoff, discharge, pay rates, or other compensation terms	One year from date records made or personnel action taken, whichever is later	Title VII of the Civil Rights Act of 1964
Personnel records concerning a charge of discrimination filed or an action brought against an employer under Title VII or the ADA	Until final disposition of the charge or the action (the date of expiration of the statutory period within which the aggrieved person may bring an action in U.S. District Court or the date such litigation is terminated)	Americans with Disabilities Act

Internal Revenue Service Requirements

In addition, there are a variety of IRS data retention regulations that apply to virtually all employers, other organizations and individuals. These requirements demand that records be retained for varying periods ranging from two years to seven years, although some records, such as those that relate to the failure to file a return, have indefinite retention periods.

Exceptional Cases

There are also unusual circumstances in which content retention requirements may exceed those that are mandated by statute. For example, in 1999, the US Department of Justice asked the Office of Personnel Management to preserve a variety of records that were being held by insurance carriers under the Federal Employees Health Benefits Program, even though the requirement for retention of these documents was only three years. This request followed a court order to preserve all documentation related to the US Government's litigation against manufacturers of tobacco products.

Other Requirements

There are a wide variety of other requirements imposed by a variety of federal statutes, including the:

- Welfare and Pension Plans Disclosure Act
- Employers Retirement Security Act
- Civil Rights Act and Equal Pay Act
- Federal Employee's Compensation Act

There are also a variety of other content retention requirements that apply specifically to companies in certain industries, as discussed below.

Automotive Industry Requirements

General Motors, Ford and Daimler-Chrysler have sponsored the Auto Industry Action Group, which has issued a set of quality requirements that are specific to the automotive industry. These requirements, published as QS-9000, is a superset of ISO-9000; the latter is a universally applicable quality system that applies to manufacturers of all types.

The key provisions of QS-9000 include the following:

- Quality performance records must be retained for one calendar year after the year they were created.

- The records associated with internal quality system audits and the management review of these audits must be retained for three years.
- A variety of documents that relate to tooling records, production part approvals, purchase orders and amendments for any automotive part or part family must be retained as long as the part(s) is being produced or is used for the service of vehicles, plus one calendar year.

Exceptions to this may be specified by customers. For example, Robert Bosch Australia retains all records for 10 years after the last data entry for any part. Further, all of Bosch's essential quality performance records related to parts that are considered critical or related to safety requirements are retained for 15 years.

Other Requirements

The American Lumber Standard Committee specified minimum retention periods for documents, including emails. These requirements call for various retention periods for different types of documents.

© 2003 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed outside of the client organization that has purchased it, nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.