Data Retention Compliance

White Paper

June 2007

Contents

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Many laws and regulations exist throughout the world that require specific retention time periods and associated safeguards for a wide range of data types. Organizations need to be aware of these data retention requirements and plan to meet the compliance challenges.

> According to Network Appliance "Regulated Data—Headache or Opportunity?" (October/November 2003), more than 10,000 United States federal, state, and local laws and regulations address records retention requirements.

Violations Have Significant Business Impact

Organizations that do not address data retention requirements face significant fines and penalties that can cripple business or even put an organization out of business. On December 3, 2002, the Securities and Exchange Commission (SEC), the New York Stock Exchange (NYSE), and NASD announced joint actions against Deutsche Bank Securities, Inc.; Goldman, Sachs & Co.; Morgan Stanley & Co., Incorporated; Salomon Smith Barney, Inc.; and U.S. Bancorp Piper Jaffray, Inc. for violations of recordkeeping requirements concerning email communications. The firms received fines totaling $8.25 million ($1.65 million each), along with a requirement to review their procedures to ensure compliance with recordkeeping statutes and rules. The regulatory agencies determined each of the five organizations:

- Violated Section 17(a) of the Securities Exchange Act of 1934, Rule 17a-4 under the Exchange Act, NYSE Rule 440 and NASD Rule 3110 by failing to preserve for a period of three years, and/or preserve in an accessible place for two years, electronic communications relating to the business of the firm, including interoffice memoranda and communications.
- Violated NYSE Rule 342 and NASD Rule 3010 by failing to establish, maintain, and enforce a supervisory system to assure compliance with NASD and NYSE rules and the federal securities laws relating to retention of electronic communications.

Organizations need to have a records retention and management plan, policy, and procedure in place to govern the security of the information they store, how long specific types of information must be retained, and how to securely and irreversibly dispose of the data when the retention periods have been met. In addition, they must know the data retention and management requirements within the laws and regulations applicable to their organizations.

> 🕮 A useful resource to help with establishing data and records retention policies and practices is *BS ISO 15489-1:2001 Information and Documentation*, which provides guidance on managing records of originating organizations, public or private, for internal and external clients.

Organizations need to discuss data retention laws and regulation with their legal counsel to obtain an interpretation of the applicable requirements based upon their own unique enterprise circumstances.

International Laws and Regulations

The following list highlights a sample of international laws and regulations (outside the United States) that specify data retention requirements.

1997 EU Directive on Privacy in Telecommunications:

- Article 6 requires traffic and billing data to be erased or made anonymous at the end of the period during which the bill may lawfully be challenged or payment may be pursued.

EU Data Protection Directive

- Personal data must be accurate and up to date.
- Organizations must not maintain data in a form that identifies specific individuals any longer than necessary for the purposes for which the information was collected or processed.

UK Anti-Terrorism, Crime and Security Act (ATCS) 2001

- Part 11 covers retention of communications data.
- Section 103 makes provision for a code of practice on data retention regulated under UK's RIPA part 1 chapter 2.

Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

- Part 1 maps to the data-retention principle under the EU Data Protection Directive.
- Principle 4.5 requires personal information not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.

United States Laws and Regulations

A sample of some U.S. laws and regulations with data retention requirements includes the following.

Sarbanes-Oxley Act of 2002:

- Fines and imprisonment of up to 20 years are proscribed for any person who corruptly alters, destroys, or conceals any records or documents to impair the use of them in any investigation.
- Failure to maintain audit/review work papers for at least 5 years can result in fines or imprisonment for up to 5 years.
- All audit and review information must be retained in a readily accessible and indelible format for 7 years.

Health Insurance Portability and Accountability Act (HIPAA):

- Covered entities (CEs) must not only ensure the security and appropriate access to health information while in transit through networks but also while the information is in storage.
- Such information must be maintained for 6 years from the date of its creation or 6 years from the date for which it was last in effect, whichever is later.
- Penalties include not only civil, but also potentially large fines and/or prison time.

Gramm–Leach–Bliley Act (GLBA):

- Financial organizations with customers and consumers who are United States citizens must implement security programs governing the security and retention of non-public personal information (NPPI).

21 CFR Part 11 (Electronic Records; Electronic Signatures):

- Requires all FDA-regulated program areas to follow technical and procedural standards for the processing, storage, security, and retention of electronic records and electronic signatures.
- Noncompliance can result in a range of FDA actions, including publicly available statements to closing the organization.

USA PATRIOT Act:

- Requires trades and businesses to record and report cash transactions of more than $10,000 (or two or more related transactions involving more than $10,000) and certain transactions involving monetary instruments to Treasury's Financial Crimes Enforcement Network (FinCEN).
- Requires that a program be established to prevent money laundering through the use of policies, procedures, and internal access and security controls. Included in the requirements are specifications for recordkeeping, reporting, verifying customer identification, and responding to law-enforcement requests.
- Money services businesses that have computerized data processing systems must integrate into their systems compliance procedures, such as recordkeeping and monitoring transactions, subject to reporting requirements.

FDA Good Manufacturing Standards:

- Requires retaining all appropriate critical documents, such as development history reports, scale-up reports, technical transfer reports, process validation reports, training records, production records, control records, and distribution records.
- The retention periods for these documents must be specified within the procedures.
- All production, control, and distribution records must be retained for at least 1 year after the expiry date of the corresponding batch.
- For APIs with retest dates, records must be retained for at least 3 years after the batch is completely distributed.

21 CFR 58.195: Food and Drug Administration (FDA) Good Laboratory Practice:

- In general, documentation records, raw data, and specimens pertaining to a non-clinical laboratory study and required to be made by this part must be retained in the archive(s) for whichever of the following periods is shortest:
  - At least 2 years following the date on which an application for a research or marketing permit, in support of which the results of the non-clinical laboratory study were submitted, is approved by the FDA. This does not apply to studies supporting investigational new drug (IND) applications or applications for investigational device exemptions (IDEs), records of which are governed by the provisions of paragraph (b)(2) of this section.
  - At least 5 years following the date on which the results of the non-clinical laboratory study are submitted to the FDA in support of an application for a research or marketing permit.
- In other situations (such as where the non-clinical laboratory study does not result in the submission of the study in support of an application for a research or marketing permit), a period of at least 2 years following the date on which the study is completed, terminated, or discontinued.

Securities Exchange Act Rules 17a-3 and 17a-4:

- Certain records must be preserved for either 3 or 6 years, depending on the particular record.

Commodity Futures Trading Commission (CFTC): 17 CFR Part 1 Regulation 31.1:

- Requires all books and records required to be kept by a Futures Commission Merchant (FCM) for a period of 5 years from the date thereof, and that the required books and records be stored on micrographic or electronic storage media unless the documents are trading cards or other documents on which trade information is originally recorded in writing.
- Organizations in the futures and commodities industry that do not have automated recordkeeping must:
  - Show that recordkeeping meets pertinent regulatory requirements before converting it to electronic records.
  - Create a duplicate of both required records and an index of those records, and maintain the duplicate at a separate location.
  - Have an auditable system for transferring records to electronic media.
  - Ensure the commission has the information needed to access electronic records.
  - Provide an independent source for downloading records that are kept solely on electronic media.

Federal Energy Regulatory Commission (FERC): Part 125:

- Specifies regulations regarding protection from fire, floods, and other hazards and in the selection of storage space.
- Safeguard the records from unnecessary exposure to deterioration from various specified conditions.
- Software and hardware that is required for the retrieval of stored data must be maintained for the retention periods specified in Section 125.3—Retention Periods; examples include:
  - Annual reports—5 years
  - Meeting minutes related to stockholders—5 years (with conditions)
  - Titles, franchises, licenses—6 years (with conditions)
  - Procurement agreements—6 years
  - General accounting ledgers—10years
  - Plant ledgers—25 years
- This ruling applies to all forms of records, including unstructured forms, such as email.

Department of Energy (DOE) 10 CFR 600.153: Retention and Access Requirements for Records:

- Financial records, supporting documents, statistical records, and all other records pertinent to an award must generally be retained for a period of 3 years from the date of submission of the final expenditure report or, for awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, as authorized by the DOE.

Internal Revenue Code Title 26:

- Carries a penalty of up to $500,000 and 3 years in prison for destroying records.
- Records must be retained based on the type of organization; in general, keeping records for at least 7 years to address this code is considered a good business practice.

Internal Revenue Service (IRS): Rev Proc 97-22:

- Part 03 Section 1.6001-l (e) states "…the books or records required by Section 6001 must be kept available at all times for inspection by authorized Internal Revenue Service officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law."
- The electronic storage system used must meet the following requirements:
  - Ensure the integrity, accuracy, and reliability of information stored
  - Prevent any type of alteration to the records as well as deletion or deterioration of stored electronic records

Americans with Disabilities Act (ADA):

- Information about persons whose employment was involuntarily terminated must be kept for at least 1 year from the date of the termination.

Age Discrimination in Employment Act:

- Any information containing advertisements or public notices for open job positions must be kept for 1 year from the date of personnel action.

Employee Retirement Income Security Act of 1974:

- Any email, notes, or other correspondence related to employee benefit plans must be kept indefinitely.

Occupational Safety and Health Act (OSHA):

- All documents that include information about monitoring employee exposure to hazardous substances must be retained for 30 years.

Toxic Substances Control Act:

- Documentation of any employee's allegation of ill health effects or occupational injury must be retained for 30 years.

Mammography Quality Standards Act of 1992 (MQSA):

- Medical records related to actual original mammograms (films) and mammography reports must be maintained for:
  - A period of not less than 5 years, or
  - Not less than 10 years if no additional mammograms of the patient are performed at the facility, or
  - Longer if mandated by state or local law, or
  - Until a request is made by or on behalf of the patient, that her records be permanently or temporarily transferred to a medical institution, her physician or healthcare provider, or to the patient herself.

U.S. Code Title 44 (Paperwork Reduction Act):

- Some documents may never be destroyed; for example:
  - Certain presidential and presidential-related materials
  - Items as identified by the National Archivist
  - Agreements between states
- In general, federal computer systems must maintain travel-related records for 6 years, or until audit, whichever is sooner, then destroyed.
- For the Department of Labor, printed investigation forms generated by the WHISARD system must be retained in the investigative files of Wage and Hour District Offices. Database information must be captured on tape at the end of each fiscal year and retained for 25 years. The U.S. Forestry Service retains records indefinitely.

Social Security Administration (SSA) Records Retention:

- All SSA financial records and supporting documents must be retained for a period of 3 years as follows:
  - Financial records and supporting documents must be retained until resolution of federal audit findings and cost effectiveness measurement system (CEMS) compliance review findings.
  - Non-expendable property records must be retained until 3 years after the final disposition of the item.
  - Statistical records and records that pertain to the processing of disability claims must be retained for the length of time specified in accordance with the Department of Archival Records Administration schedule.

NASD Rule 3110:

- Securities firms must retain all correspondence of their representatives that are part of its securities or investment banking business. This rule spells out the requirements for maintaining recordkeeping, record formats, storage mediums, and records retention periods that comply with and support SEC Rule 17a-4.
- Affected firms must accomplish all of the following to be in compliance:
  - Thoroughly document and enforce records retention policies
  - Store data on indelible, non-rewriteable, and non-erasable media
  - Make a search/reference index available for of all stored data
  - Make data readily retrievable and viewable
  - Store data off-site

NASD 3010 (3) Retention of Correspondence:

- Each member must retain correspondence of registered representatives relating to its investment banking or securities business in accordance with Rule 3110.
- The names of the persons who prepared outgoing correspondence and who reviewed the correspondence must be ascertainable from the retained records and the retained records must be readily available to the Association, upon request.

New York Stock Exchange (NYSE) Rule 440:

- Broker and dealer firms must properly manage, search, and retain emails relating to the business while controlling the costs resulting from managing emails.

National Archives and Records Administration (NARA): Part 1234 and GA Schedule 24

- There are many retention and storage requirements found within the following sections:
  - Section 1234.22—Creation and Use of Text Documents
  - Section 1234.30—Selection and Maintenance of Electronic Records Storage Media
  - Section 1234.32—Retention and Disposition of Electronic Records
  - Section 6—User Identification, Profiles, Authorizations, and Password Files
  - Section 11—IT Infrastructure Design and Implementation Files

Department of Defense: DoD 5015.2:

- Section C2.2.9—Systems Management Requirement has several retention requirements within the regulation requiring:
  - Backup of Stored Records (C2.2.9.1)
  - Storage of Backup Copies (C2.2.9.2)
  - Rebuild Capability (C2.2.9.4)
  - Storage Availability and Monitoring (C2.2.9.5)
  - External Email Management and Retention (C2.2.10.2)

About the Author

Rebecca Herold has more than 16 years of experience in information security, privacy and compliance. Rebecca is an independent consultant, author and instructor and assists organizations of all sizes with their information privacy, security and regulatory compliance programs.

Rebecca has a B.S. in Math and Computer Science and an M.A. in Computer Science and Education. Rebecca is a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA), a Certified Information Systems Manager (CISM), and a Fellow of the Life Management Institute (FLMI). Rebecca has been a member of the Information Systems Audit and Control Association (ISACA) since 1990 and has held all board positions throughout her membership in the Iowa chapter. She was Vice President, Privacy Services and Chief Privacy Officer at DelCreo, Inc., Chief Privacy Officer and Senior Security Architect for QinetiQ Trusted Information Management, Inc., and Senior Systems Security Consultant at Principal Financial Group. Rebecca was instrumental in building the information security and privacy program while at Principal Financial Group which was awarded the CSI Outstanding Security Program of the Year Award in 1997. Rebecca is also an adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program.

Rebecca authored The Privacy Papers (Auerbach) in 2001, The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach) in 2003, The Business Executive Practical Guides to Compliance and Security Risks book series (Realtime Publishers) in 2004, Managing an Information Security and Privacy Awareness and Training Program (Auerbach) in 2005, The Definitive Guide to Security Inside the Perimeter (Realtime Publishers) in 2005 and The Privacy Management Toolkit (Information Shield) in 2006. Rebecca lives in the country near Des Moines, Iowa. She is the community leader at http://www.realtime-itcompliance.com, and she can be reached at rebeccaherold@rebeccaherold.com.

About NetIQ Corporation

NetIQ, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. NetIQ's best-of-breed solutions help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes Systems Management, Security Management, Configuration Control and Change Administration. For more information, please visit www.netiq.com.