From Information Systems Security

82-02-54

DATA SECURITY MANAGEMENT

Records Retention and Security Regulations... Think about It!

Rebecca Herold, CISSP, CISA, FLMI

INSIDE

Security; Regulations; Health Insurance Portability and Accountability Act (HIPAA); Gramm–Leach–Bliley Act (GLB); U.S. PATRIOT Act; FDA Good Manufacturing Standards; FDA Good Laboratory Practice; White House's Proposed National Strategy to Secure Cyberspace; Paperwork Reduction Act; EU Data Protection Directive; Proposed EU Directive on Telecommunications Privacy

BACKGROUND

Executive management, such as the CEO and President, is increasingly legally accountable for ensuring the security and availability of their organizations' information. Over the past several years, various agencies and governments worldwide have been pushing for the adoption of data security and retention requirements in one form or another. Many have been successful, with retention requirements being incorporated into multiple, recently enacted legal regulations. In addition to data retention, many of these same laws, in addition to others, have some strict requirements for securing the access to data in storage that many organizations with their current technology network and configurations are having a challenge to meet.

Effectively managing business documents is crucial to any organization's bottom line. In addition to effectively managing the information received in electronic form, printing and mailing costs can be dramatically reduced by converting paper documents to searchable digital formats, at the same time making information more accessible to authorized decision makers throughout the organization.

PAYOFF IDEA

Every organization needs to have a records management plan and procedure in place for determining the security of the information it stores, and also for determining how long it must retain specific types of information. Archiving systems in which policies can be established is a relatively simple way to comply with the myriad regulations concerning record retention.

SECURITY

There are very clear requirements by internationally accepted security standards, such as ISO 17799, that specify that networks and organizational records must be securely maintained to meet statutory requirements, as well as support essential business activities. Information must be readily available to those who need access to perform business functions, but must be secured to prevent unauthorized access. The potential impact to an organization from both legal and operating perspectives could be devastating if inappropriate access occurs, to the level of putting an organization out of business.

REGULATIONS

The growing trend for requiring businesses to ensure the security and retention of certain types of information is apparent through the increasing use of electronic records in court cases and during the legal discovery process, and by reviewing some of the current laws. For example, U.S. federal regulations require that some employee records be maintained for one year, some require retention for five years, some for 30 years, and some indefinitely. And, there is a very wide range of penalties associated with destroying protected records. Additionally, many regulatory bodies, such as the U.S. FDA, have stringent records retention security requirements. Disaster plans must include details for protecting this vital information.

Some of the industries most noticeably hit by new security and retention regulations include, but are not limited to, the following:

- Financial
- Healthcare
- Internet service providers
- Telecommunications
- Government

Penalties for noncompliance with these regulations range all the way from warning letters to multi-million-dollar fines, prison time, and business closure. Following are some of the U.S. laws that have very specific security and retention requirements.

Health Insurance Portability and Accountability Act (HIPAA)

Covered entities 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. Additionally, such information must be maintained for six years from the date of its creation or six 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 (GLB Act)

Financial organizations with customers and consumers who are U.S. citizens must implement security to ensure the privacy of non-public personally identifiable (NPPI) information, and must also establish formal information security programs governing the security and retention of NPPI information. Both the organizations and individuals responsible for regulatory compliance within the organizations face potentially huge fines and/or prison time for noncompliance.

21 CFR Part 11

21 CFR Part 11 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.

U.S. PATRIOT Act

The U.S. PATRIOT Act requries 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). The Act 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 record keeping, reporting, verifying customer identification, and responding to law-enforcement requests. Additionally, money services businesses that have computerized data processing systems must integrate into their systems compliance procedures, such as record keeping and monitoring transactions, subject to reporting requirements. No specific retention period is mandated; however, the Act specifies that the government has the right to review what electronic information is available.

FDA Good Manufacturing Standards

The FDA Good Manufacturing Standards require that procedures be created and implemented for retaining all appropriate critical documents (e.g., 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 one year after the expiry date of the corresponding batch. For APIs with retest dates, records must be retained for at least three years after the batch is completely distributed.

21 CFR 58.195: FDA Good Laboratory Practice

In general, documentation records, raw data, and specimens pertaining to a nonclinical 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:

- A period of at least two years following the date on which an application for a research or marketing permit, in support of which the results of the nonclinical laboratory study were submitted, is approved by the Food and Drug Administration (FDA). This requirement does not apply to studies supporting investigational new drug (INDs) applications or applications for investigational device exemptions (IDEs), records of which shall be governed by the provisions of paragraph (b)(2) of this section.
- A period of at least five years following the date on which the results of the nonclinical laboratory study are submitted to the FDA in support of an application for a research or marketing permit.
- In other situations (e.g., where the nonclinical 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 two years following the date on which the study is completed, terminated, or discontinued.

White House's Proposed National Strategy to Secure Cyberspace (as of June 19, 2002)

An early draft of the White House's National Strategy to Secure Cyberspace details the same kind of mandatory customer data collection and retention by U.S. Internet service providers as was recently enacted in Europe. However, a U.S. Justice Department source indicates the data retention issue is mentioned in the strategy only as an industry concern, not as a requirement. Until the "Strategy" is finalized and passed, affected organizations (e.g., ISPs and telecom companies) need to determine their data retention practices for e-mail headers (from, to, cc, and subject lines) of each e-mail every customer sends or receives, and every ISP customer's complete Web browsing history. The period of time the data will have to be retained is unknown at this time; however, specific legislative proposals range from twelve months to seven years.

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

Certain records must be preserved for either three or six years, depending on the particular record.

Commodity Futures Trading Commission (CFTC) Rule 1.31

This rule requires that all books and records required to be kept by a Futures Commission Merchant (FCM) must be kept for a period of five years from the date thereof, and that the required books and records can 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.

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

In general, financial records, supporting documents, statistical records, and all other records pertinent to an award must be retained for a period of three 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

Title 26 carries a penalty of up to $500,000 and three years in prison for destroying records. Records must be retained based on the type of organization; but in general, keeping records for at least seven years to address this code is considered a good business practice.

Americans with Disabilities Act

Information about persons whose employment was involuntarily terminated must be kept for at least one 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 one year from the date of personnel action.

Employee Retirement Income Security Act of 1974

Any e-mail, notes, or other correspondence related to employee benefit plans must be kept indefinitely, as required by the Employee Retirement Income Security Act of 1974.

Occupational Safety and Health Act

All documents that include information about the monitoring of 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 five 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 health care provider, or to the patient herself.

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

Some documents may never be destroyed in accordance with this act. 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 six 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 three 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 three 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.

In addition to the plethora of U.S. laws, there are many more security and retention laws worldwide. For example, just a few of these include the following from the European Union (EU):

EU Data Protection Directive

Personal data must be accurate and up-to-date. To comply with this requirement, organizations must take reasonable steps to ensure that personal data maintained

by the organization meets these requirements. Additionally, 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.

Proposed EU Directive on Telecommunications Privacy

The European parliament passed the Communications Data Protection Directive on May 30, 2002. This directive lists the minimum and optional data that must be retained by Internet service providers and telephone companies. This data includes:

- User-id and password
- Assigned IP address
- Number of bytes transmitted and received
- Specified "Optional" information, including: credit card number or bank account for subscription payments

For e-mail servers, service providers must retain the following data:

- IP address
- Message ID
- Sender
- Receiver
- User ID

Providers of "file upload and download servers" must retain the following data:

- ftp log
- IP address
- User-id and password
- Path and filename of data objects uploaded or downloaded

Providers and managers of Web servers must retain the following data:

- IP source address
- Operations performed, such as GET command, etc.
- Path of the operation (to retrieve html page or image file); basically all the details of Web pages visited have to be kept

For normal phone lines, telephone companies will have to keep the following information:

- Numbers called (whether connected or not)
- Date

- Time
- Length
- Name
- Date of birth
- Address
- Bank account of the subscriber
- Types of connection the user has, such as phone, ISDN, ADSL, etc.

For mobile and satellite users, providers must retain generally the same information as telephone companies in addition to the identification and geographical location of the user.

RECOMMENDATIONS

All organizations need to have a records management plan and procedure in place for determining the security of the information they store, and also for determining how long they must retain specific types of information. Archiving systems in which policies can be established is a relatively simple way to comply with the myriad regulations concerning record retention.

Rebecca Herold, CISSP, CISA, FLMI, is Vice President, Privacy Services, and Chief Privacy Officer for DelCreo, Inc. She is the editor of *Privacy Papers: Managing Technology, Consumer, Employee, and Legislative Actions* (Auerbach Publications, 2002). She can be reached at rebecca@delcreo.com.