

Regulation Overview

Retention by Data Type and Business Unit



Regulatory rules related to data retention have evolved into a central part of many IT shops data management practices. Current rules related to SEC filings, HIPAA and insurance claims affect virtually all organizations in their financial, HR, Environmental or direct business activities. On the horizon are a fresh group of regulatory requirements related to consumer information and customer contact.

The management of the process has changed dramatically from being a minor nuisance to requiring the attention of a full-blown organization, responsible for data retention oversight, audit and monitoring with a similar escalation in associated costs.

DATA TYPE	REGULATION	RETENTION REQUIREMENT	PENALTY
FINANCIAL INDUSTRY			
Broker-dealer	NASD 3010, 3110 SEC 17a-4	Broker data retention for between 3 and 6 years. Some require longer retention	Up to \$500,000 and 10 years in prison
Registered Investment Advisor	Investment Advisor's Act, SEC Rule 204-2	Advisors must maintain copies of certain books and records relating to their advisory business for not less than 5 years	Up to \$500,000 and 10 years in prison
Internal Auditor	Sarbanes-Oxley (SOX) section 802	Auditors must retain relevant data for at least 7 years	Penalties range from fines of up to \$1,000,000 to prison sentences of not more than 20 years
Bank	Gramm-Leach Bliley Act (GLBA)	Ensure confidentiality of customer financial information	Non-compliance of GLBA can result in a variety of fines and up to 5 years imprisonment for each violation
Hedge Fund	SEC Rule 203(b)(3)-2	Advisors must maintain copies of certain books and records relating to their advisory business for not less than 5 years	Up to \$500,000 and 10 years in prison
HEALTHCARE INDUSTRY			
Health Insurances	HIPAA	Retain patient data for 6 years	For Civil Penalties, up to \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated. For Criminal Penalties, up to \$50,000 and 10 years in prison.
Hospitals			

NOTE: HIPAA does not just affect the medical profession; it covers all entities that handle, maintain, store, or exchange private health or patient related information, regardless of size. This includes, but is not limited to:

- Healthcare organizations, health service providers, employers maintaining health records, public health authorities, health plans, life insurers, blood, sperm, organ donation banks, pharmacies, long-term care facilities, billing agencies, clearing houses, clinics, physician offices, etc. These cover:
 - o Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other healthcare providers
 - o Health insurance companies, HMOs, most employer group health plans
 - o Certain government programs that pay for health care, such as Medicare and Medicaid

LESS IS MORE

In data retention risk management, less is more. Reduction in the total volume of data under management is a key ingredient. Atomic level, lower value data that has been summarized and integrated for analysis purposes needs to be disposed of as early as possible. This elimination does not impact analytics having already been summarized or harvested for business-intelligence-related information. Storage optimization also reduces the time frame of disaster recovery, backup and recovery and operational overhead.

SOLUTIONS

The solution to the data retention process implementation needs to focus on several key services:

1. A standard data retention lifecycle for at least all the data subject to the data retention policy of the organization.
2. A rules based engine that can determine the retention status of a piece of data based on the data lifecycle.
3. An audit service that retains information about the data retention regulated data as it transitions through its lifecycle.
4. An audit service that retains information about the data retention rules enforced at a given time.
5. A reporting service that can leverage information from the audit service for analysis on a specific piece of data or a collection of data.

WHAT DOES ZL TECHNOLOGIES PROVIDE?

ZL's compliance platform provides a comprehensive set of tools for small and large businesses to comply with today's regulations governing electronic communications, including:

- Email archiving and WORM storage
- Email retention policy management
- Email search and discovery
- Email storage management
- Email attachment management
- Instant messaging archival

ZL provides an all-in-one solution, which stores data on virtually any non-rewritable device library, jukebox, etc. (CD-R, DVD-R, and magneto optical disc, et al). ZL automatically generates a comprehensive and hierarchically searchable index for headers, message body, size, and attachments. ZL's advanced search with proximity and context sensitivity matching allows companies greater granularity of searches according to use within sentences, paragraphs, and whole documents. Simultaneous cross-alias searching easily prevents multiple searches of the same user, reducing time and resources spent in the event of a pressing audit. ZL also provides a full auditor application, which enables internal or external auditors to capture specific mails and generate an annotated thread for tracking the entire review lifecycle. The quick summary for lexical analysis and compliance Analysis for reviewers provides easy summarization of compliance review logs, frequency and occurrences. Additional advantages with ZL are optional performance enhancements, data compression, data encryption, attachment staging and management, and a parallel mail system for disaster response.

ZL's platform also provides a full suite of integrated modules for securing customer data during storage and communication through methods such as:

- Secure email
- Secure document delivery
- Secure file collaboration
- Secure large file transfers
- Secure instant messaging

To protect the private information of consumers, ZL uses FIPS 140-2 compliant cryptographic algorithms such as AES and 3DES for data encryption. ZL is modular as well, giving our clients the ability to choose and select their encryption settings, key lengths, and algorithms. Consequently, all ZL platform based security modules take advantage of the most advanced and strongest encryption technologies available today to protect data. Also, with its powerful key escrow capability, a company will always have access to its vital encrypted data whenever needed.

While ensuring the highest levels of security is a primary consideration, the day-to-day practicality and usability of our solution is also at the forefront of our design considerations.

To address this requirement, ZL's solution is completely gateway and server based making it transparent to senders. Since there is no change in user experience, no training is necessary. In addition, ZL does not require recipients to download or install any software, applets, or ActiveX components onto their system. While many other solutions might claim they do not require any downloads, they might require applets or other installed components to run properly, potentially interfering with network firewalls and certain operating systems. ZL truly requires no such downloads, transparent or otherwise.

Administrators benefit from a fully automated system, which can be set to manage the entire life-cycle of registering, maintaining, and renewing users. ZL's full suite of automated end-user registration and authentication technologies provide maximum flexibility by tying to existing standards such as SSO, SAML, LDAP, Active Directory, and other centralized authentication schemes. These can be stored on directory servers, databases, PIN servers, or other structures. ZL also enables self-administration by users of their passwords or keys depending upon which security module is deployed. The burden for administrators operating the system is dramatically reduced.

Deployed individually or in concert, ZL's modules act to complete an existing compliance initiative within a firm and can provide a complete, unified email management solution.

ABOUT ZL TECHNOLOGIES

Established in 1999, ZL Technologies, Inc. (ZL) provides cutting-edge enterprise software solutions for email archiving, regulatory compliance, litigation support, corporate governance, content management, file archiving, and secure email. ZL's flagship product, the Unified Archive, offers comprehensive email and file archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Bloomberg, and others. The suite provides a highly flexible framework that is fully scalable, enabling organizations of all sizes to meet legal discovery, compliance, and storage management requirements. With a proven track record and an impressive list of clients, including Walgreens, Bank of New York Mellon, Pacific Life, and Morgan Keegan, among other top global institutions, ZL has emerged as the premier provider of email archiving and compliance solutions. For more information, please visit www.ZLTI.com

To learn more about how ZL Technologies can help you take control of your data, call us at 408.240.8989 or visit us online at www.ZLTI.com