

Regulatory Compliance: How Digital Data Protection Helps

Executive Summary

Organizations today face many compulsory regulatory requirements, among them:

- Gramm-Leach-Bliley (GLB) Act
- SEC Rule 17a
- Fair and Accurate Credit Transaction Act (FACTA)
- Sarbanes-Oxley Act (SOX)
- Rules 26 and 37 of the Federal Rules of Civil Procedure (FRCP)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Penalties for enterprises that do not comply with such requirements are severe.

Digital data protection solutions provide several ways to satisfy these requirements:

- Backup services to store electronic data off-site in secure, underground vaults
- Protection against data loss from natural disasters, human error, or sabotage
- Easy and complete data recovery
- Encryption that ensures privacy for sensitive information
- Coverage for servers, desktops, laptops, and remote computers
- Defense against disastrous and embarrassing disclosure of data through a lost or stolen notebook computer
- Data retention for selectable lengths of time (typically seven years)
- Rapid access and retrieval of information required for legal discovery
- Automatic and dependable processing
- Professional and experienced design and support services personnel

Organizations must leverage digital data protection to meet the challenges of regulatory requirements.

Introduction

Digital data protection — including backup and recovery, automatic digital shredding of compromised files, encryption, and digital archiving — is valuable to many enterprises, not only for providing data protection and business continuity, but also for helping enterprises comply with new regulations.

This white paper presents vital information about the regulatory requirements that enterprises must satisfy and how digital data protection helps enterprises to satisfy these requirements.

The Regulatory Challenges

Many enterprises must comply with an increasing number of regulatory requirements affecting their business — or face stiff penalties for non-compliance. The new requirements include these mandates:

- Protect business, financial, patient, employee, and customer information regardless of its format or medium – as required in HIPAA, Gramm-Leach-Bliley, and FACTA.

Contents

| | |
|--|----|
| <i>Executive Summary</i> | 1 |
| <i>Introduction</i> | 1 |
| <i>The Regulatory Challenges</i> | 1 |
| <i>The Role of Digital Data Protection in Compliance</i> | 3 |
| <i>Gramm-Leach-Bliley (GLB) Act</i> | 5 |
| <i>SEC Rule 17a</i> | 7 |
| <i>FACTA</i> | 8 |
| <i>Sarbanes-Oxley Act (SOX)</i> | 9 |
| <i>FRCP Rule 26</i> | 10 |
| <i>HIPAA</i> | 12 |
| <i>SysTrust™ Certification</i> | 14 |
| <i>PCI Compliance</i> | 14 |
| <i>Conclusion</i> | 15 |

- Ensure the privacy of individuals – as required by HIPAA, Gramm-Leach-Bliley, and FACTA.
- Disclose corporate information for the government during compliance audits and for the courts during litigation – as required by the Sarbanes-Oxley Act of 2002 (SOX), SEC Rule 17a-3 and 17a-4, and Rule 26 of the Federal Rules of Civil Procedure.
- Verify financial and business integrity for investors – as required by SOX.
- Demonstrate the security, availability, processing integrity, and confidentiality of the IT infrastructure environment – as required for SysTrust certification.

These mandates cover the growing volume of electronic documents, digital images, audio and video media, email, and instant messages, as well as paper and other physical records. In many cases, no paper records exist: only electronic records exist. Such electronically stored information (ESI) is admissible in court.

Specific regulatory requirements for electronic records also address the following issues:

- **TAMPER-PROOF RECORDS.** SOX Section 802 prescribes penalties for altering or deleting key business documents, including electronic documents. In addition, SOX Section 404 requires enterprises to conduct a management assessment of internal controls, which would include an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse.
- **RECORDS RETENTION.** Public companies must retain records within the SEC's legally specified time period, or for the period defined by their industry-specific regulations or other applicable laws and regulations.
- **RECORDS DISPOSAL.** U.S. Department of Defense directive 5015.2 and its statutory references require deleting data in such a manner that it cannot be recovered using disk-scanning tools. This directive, which pertains to records management products acquired by the Department of Defense, is becoming a best practice for enterprises.
- **DUPLICATE STORAGE.** It has become a best practice for enterprises to store duplicate records separately from the originals in a tamper-proof format that they transmit electronically to a remote location.
- **LEGAL STATUS OF ELECTRONIC RECORDS.** Storing business records digitally does not affect their admissibility. ESI is admissible in court.

Table 1. Industries Affected by Regulatory Compliance

| | Financial Services | Healthcare | Manufacturing/ Commercial | Energy | Retail | Government |
|--------------------------|--------------------|------------|---------------------------|--------|--------|------------|
| GLB Act | X | | | | | X |
| SEC Rule 17a-3 and 17a-4 | X | | | | | |
| FACTA | X | X | X | X | X | X |
| SOX | X | X | X | X | X | |
| FRCP Rule 26 | X | X | X | X | X | X |
| HIPAA | X | X | X | X | X | |

Clearly, many regulatory requirements involve digital data protection. What role, then, do solutions that provide digital data protection have in a comprehensive Compliant Records Management (CRM) program? How does digital data protection support your compliance needs?

The Role of Digital Data Protection in Compliance

Digital data protection includes these technologies, products, and services:

- Backup and recovery of servers and PCs
- Shredding files automatically on compromised computers, such as stolen laptops
- Data encryption
- Digital archiving of electronic documents

What safeguards do such digital data protection solutions provide to ensure compliance, given the requirements that electronic records must be tamper-free, duplicated, retained for specified periods, readily accessible for legal discovery, and managed to provide privacy and information protection? Here is a closer look at the important roles that digital data protection can play in compliance – and some of its limitations.

Storage vs. Backup

For many, no distinction exists between storage and backup. However, electronic records storage and backup have important differences:

- STORAGE SOLUTIONS alone cannot satisfy regulations for tamper-free, private, and protected records. Certainly, many options on the market can store large amounts of data and make it available — online and offline — for business uses. However, these systems focus only on data availability, not on data protection. In the event of accidents, system failures, natural disasters, and hostile human activities, they cannot ensure that data will remain free from tampering, and they cannot protect data from a wide variety of threats.
- BACKUP SOLUTIONS are not only for data storage and retrieval, but also for data protection, providing backup or duplicate files for disaster recovery purposes. The focus of backup solutions is to ensure that data is retained and available when ordinary storage fails. They provide safeguards to keep data tamper-free, private, and protected from a variety of destructive natural and human events, ensuring data is ready for recovery.

Backup vs. Archiving

Enterprises must separate backup data from archived data. Backups are for disaster recovery purposes, containing a snapshot of the system to restore it to its last known state. Archiving meets a long-term need for storing data with a searchable index for easy retrieval, if the need arises. Enterprises must follow retention rules for different types of archived data.

Backup vs. Archiving and Retention Systems

Backup solutions alone don't prevent regulatory trouble. While backup solutions meet requirements for duplicate, tamper-free, and secure records, they are not sufficient for a fully Compliant Records Management program. The demands of compliance and legal discovery require quick access to specific records whenever necessary, and a secure audit trail of actions against every record. While backup and digital archiving solutions are both part of electronic storage, they address different needs:

- BACKUP SYSTEMS are for wholesale data recovery from the closest point in time if the computing environment suffers failure or disaster. However, backup processes are not suitable for quickly searching data and retrieving individual items of data needed for compliance. Backup data is not indexed, and, consequently, is not easy to search. The most efficient and effective way to respond to litigation requests involving backup data is with an experienced data restoration and digital archiving solution provider. Additionally, most traditional backup processes do not provide an audit trail of actions on a backed-up record, as required for compliance and legal discovery.
- TRUE DIGITAL ARCHIVING, RETENTION SYSTEMS, AND SERVICES ensure that enterprises can find and access any given record, whenever required. Solutions today offer secure, compliant, cost-effective, and long-term archiving of electronic records. These solutions and services consolidate electronic records – email, images, statements, and

more – into a unified, browser-accessible archive for fast and easy search, retrieval, and management. They also record any action taken on archived records, providing a secure audit trail to prove that the records are free from tampering. This trail is essential in compliance audits and in cases where records appear as legal evidence.

Backup solutions cannot provide such easy retrieval and audit trails. Using backed-up records as official legal documents for compliance and litigation leads to spending considerable time and money to restore backup tapes, search for legally relevant material, and subject enterprises to the legal difficulties of attempting to prove that records remain unchanged. Furthermore, keeping several generations of backup tapes as archives opens up

the possibility of someone requesting that data for litigation purposes. Yet, many enterprises today still keep several generations of backup tapes as archives to meet the challenges of compliance and eDiscovery, despite the escalating costs of data storage. Even so, these enterprises are still vulnerable to the high costs of audits and litigation.

LiveVault and Connected Backup for PC

Customers can be sure their data is protected — off-site, offline, and out-of-reach — with Iron Mountain's LiveVault and Connected Backup for PC services. Available for servers and PCs, these services and software provide backup and recovery solutions for all of a company's distributed data, no matter where it's currently located or managed. Iron Mountain products and services ensure that backups happen automatically, consistently, and securely, while reducing the costs and burdens of backup and recovery.

In short, backup cannot replace archiving. Conversely, archiving cannot replace backup. Digital archiving solutions address the necessity for quick retrieval, audit trails, and retention periods that satisfy regulation and litigation needs. Disaster recovery and business continuity demand the ability to fully protect and recover all data to the most recent point in time after a failure. Enterprises need both solutions as part of their compliant records and data protection programs.

Clear policies are necessary for destroying information after it passes its defined retention period in a compliant records management program and exceeds its useful life for disaster recovery purposes in a data

protection program. By adhering to retention policies for compliant records management and data protection programs, customers avoid extra storage costs, excessive discovery and research fees, and possible legal headaches, while satisfying regulations and business continuity requirements.

Backup with Data Protection as One Component of a CRM Program

Given growing regulatory laws, enterprises face serious obstacles to comply with a multiplicity of requirements. Backup solutions that provide data protection, such as Iron Mountain's LiveVault® and Connected® Backup for PC solutions, help enterprises meet their compliance objectives.

At the same time, Iron Mountain's Digital Archives solution offers simple and quick search, retrieval, and management of all types and sizes of electronic records on an enterprise level. Digital Archives retains electronic records in a highly secure, auditable format on a scalable platform with no footprint on the customer site.

Iron Mountain's optional Consulting Services assists with designing and implementing comprehensive and legally credible Compliant Records Management (CRM) programs that proactively administer eDiscovery requests, while leveraging your existing technology infrastructure. Using eRecords consulting and strategy improves access to records, and makes it easier and more economical to find information for both discovery and operations. Establishing properly designed retention policies for physical and electronic records ensures that obsolete records are destroyed with confidence and that retention programs stand up in court. Customized data privacy programs protect confidential data.

Gramm-Leach-Bliley (GLB) Act

The Gramm-Leach-Bliley (GLB) Act requires that financial institutions ensure the security and confidentiality of their customers' non-public personal information. Identity theft has led the Federal government to create mandates to prevent even accidental disclosure of private information.

- **WHO MUST COMPLY:** Financial institutions have a continuing obligation to respect customers' privacy.
- **WHAT IT COVERS:** Customers' non-public personal information, such as Social Security numbers, credit records, and payment history.
- **PERTINENT REQUIREMENTS:** Administrative, technical, and physical safeguards:
 - Ensure the security and confidentiality of customer records and information.
 - Protect against any anticipated threats or hazards to those records.
 - Protect records against unauthorized access or use, which could result in substantial harm or inconvenience to any customer.
 - Ensure data recovery for operations.
- **PENALTIES FOR NON-COMPLIANCE:** Up to 10-year prison sentences and/or a maximum \$1 million fine.

In addition, the Treasury Department, the Office of the Comptroller, the Office of Thrift Supervision, the Federal Reserve Board, and the FDIC have issued a joint final rule, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (the Guidelines). The Guidelines require an enterprise to involve its board of directors in assessing the risk, managing and controlling risk, and overseeing service provider arrangements.

The Guidelines include the following Objectives:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect information against unauthorized use or access, which could result in substantial harm or inconvenience to any customer.

The Guidelines for management and control of risk include:

- Access restrictions at physical locations.
- Encryption, including while in transit or in storage on networks or systems to which unauthorized individuals might have access.
- Dual control procedures.
- Monitoring to detect actual or attempted attacks.
- Measures to protect against destruction, loss, or damage due to hazards such as fire, water damage, or technological failure.

The section on oversight of service provider arrangements requires:

- Due diligence in selecting service providers.
- Service providers by contract to implement appropriate measures designed to meet the Objectives of the Guidelines.
- Where indicated, monitoring service providers, including review audits and test results.

How LiveVault and Connected Backup Solutions Can Help

LiveVault (for servers) and Connected Backup (for PCs, Macs, and servers) solutions, used together with best practices, protect sensitive customer information by getting the data off-site, off-line, and out-of-reach. Storing backup data off-site in secure, state-of-the-art vaulting facilities ensures security and protects data against threats or hazards including natural disasters, human error, or sabotage. Both solutions eliminate unnecessary

Connected® Backup for PC

Delivered as an outsourced backup service or as licensed software, the Connected Backup for PC solution provides regular, secure, and automatic backups for desktop and laptop PCs, Macs, and servers, even over a dial-up connection. Data is vaulted safely offsite – without any intervention by company IT staff. Users can restore lost data quickly and easily, without incurring help desk support costs. Administrators gain online, secure, and centralized management and control of data and backups. This service ensures consistent desktop and laptop PC data protection without user- or IT-initiated backup routines. Data is vaulted off-site to a mirrored data center. This reduces the risk of lost business-critical data due to accidental file deletions, viruses, and other sources of data corruption. This service also decreases help desk costs by eliminating attempted data restores from unprotected PCs. Ensures consistent data backup processes and IT control of data residing on individual PCs.

exposure of information to human threats and natural disasters, while ensuring data security and privacy.

Encrypting backup data containing sensitive customer information is an advisable precaution to prevent unauthorized access. For these protection requirements, LiveVault and Connected Backup solutions offer unmatched capabilities, including 256-bit AES encryption (LiveVault) of all data in transit or at rest in storage. Only the customer has the password.

LiveVault and Connected Backup solutions ensure that data protection happens regularly and automatically, which is critical for the many sources of sensitive data distributed throughout an enterprise. Many go unprotected because of their remote location or poor resources for manual backup. LiveVault and Connected Backup solutions can ensure that secure backup and protection extend to the sensitive data from all areas of the business.

LiveVault and Connected Backup best practices offer increased security using strong physical security in the form of hardened vault locations. Because they can back up and safeguard distributed data, LiveVault and Connected Backup solutions meet requirements for operational data recovery. In the event of small-scale data losses, users can quickly recover data over the Internet.

Iron Mountain's DataDefense™ solution can automatically delete and overwrite data that administrators specify. It can prevent potentially disastrous and embarrassing disclosure of data because of a lost or stolen notebook computer, tampering with passwords, and unauthorized access.

SEC Rule 17a

In 1934, to protect investors from fraudulent or misleading claims, the SEC enacted the Securities Exchange Act, a set of laws that required keeping records for reviewing and auditing securities transactions. SEC Rule 17a amends that law to allow broker-dealers to store records electronically, including electronic communications such as email and instant messages.

- **WHO MUST COMPLY:** Broker-dealers and those individuals who trade securities or act as brokers for traders, including enterprises such as banks, securities firms, stock brokerage firms, any financial institutions that trade any type of security governed by the SEC, and any entities under the jurisdiction of the National Association of Securities Dealers (NASD).
- **WHAT IT COVERS:** Electronic records and communications relating to traded securities governed by the SEC.
- **PERTINENT REQUIREMENTS:**
 - Records retention on compliant media from the time of creation to final disposition.
 - Written and enforceable retention policies.
 - Storage of data on indelible, non-rewriteable media.
 - Readily retrievable and viewable data.
- **PENALTIES FOR NON-COMPLIANCE:** Suspension and potential fines up to \$1 million.

How LiveVault and Connected Backup Solutions Can Help

Although SEC Rule 17a does not explicitly require storing data off-site, off-site storage complies with the rule, and makes good business sense because it ensures that both copies of a record cannot be destroyed in the same disaster. LiveVault (for servers) and Connected Backup (for PCs, Macs, and servers) solutions provide effective, efficient solutions for keeping critical information off-site and protected. The data is encrypted, making it unreadable to unauthorized people, yet easily accessible when needed.

Protection of data should continue as long as regulations or litigation requires, or until deliberate destruction as part of an end-of-life cycle. LiveVault and Connected Backup solutions can retain stored data for as long as the customer requires (typically seven years).

Backup and archiving are different processes and should remain distinct. Digital archiving solutions address the necessity for quick retrieval and provide audit trails of inactive data stored for specified retention periods for regulations and litigation.

LiveVault and Connected Backup solutions ensure that the task of data protection happens automatically. It is critical to deal with the many sources of sensitive data distributed throughout an enterprise. Otherwise, this data might be unprotected because of its remote location or lack of manual backup resources. LiveVault and Connected Backup solutions ensure that secure backup and protection include all areas of the business and all sensitive data.

LiveVault for Servers

An outsourced backup service provided by Iron Mountain, the LiveVault solution provides fully managed backup and monitoring of customer server data, securely, automatically, and consistently, 24x7x365. Data is encrypted, sent off-site and off-line, without any intervention by enterprise IT staff. With the on-site backup appliance option, users can recover larger amounts of data quickly, while still moving it off-site for complete disaster recoverability. The service provides a fast, easy way to restore data – from a single file to an entire server – to ensure business continuity. The LiveVault solution gives enterprise authorized personnel online, secure, centralized management and control of data backup and restoration – any time, any place – for all servers.

FACTA

The Fair and Accurate Credit Transaction Act (FACTA) makes permanent the national standards originally set by the Fair Credit Reporting Act (FCRA) of 1996. Originally, these consumer protections were to expire in 2003. FACTA also creates new provisions to combat identity theft and help its victims.

- **WHO MUST COMPLY:** Broker-dealers and those individuals who trade securities or act as brokers for traders, including enterprises such as banks, securities firms, stock brokerage firms, any financial institutions that trade any type of security governed by the SEC, and any entities under the jurisdiction of the National Association of Securities Dealers (NASD).
- **WHAT IT COVERS:** Information from creditors regarding fraudulent applications and transactions. It also covers any record about an individual, whether in paper, electronic, or other form, which is in a consumer report or is derived from a consumer report.
- **PERTINENT REQUIREMENTS:** Victims of identity fraud may now request and obtain information from creditors, which creditors must supply.
- **PENALTIES FOR NON-COMPLIANCE:** Statutory damages, actual damages, punitive damages, and attorney's fees.

How LiveVault and Connected Backup Solutions Can Help

LiveVault (for servers) and Connected Backup (for PCs, Macs, and servers) solutions supply creditors with a reliable way to get their transaction and application information off-site, off-line, and out-of-reach to protect such data from loss or inadvertent destruction. If people suspect they might be a victim of identity theft and rightfully request their transaction and application information, such safeguards protect the necessary data from unauthorized access, but allow ready access to appropriate parties.

Enterprises should encrypt backup data containing consumer information as a precaution against disclosure. Both LiveVault and Connected Backup solutions use high levels of AES digital encryption in data transmission and storage, supplemented by strong physical security that includes hardened underground vault locations.

The DataDefense solution can prevent potentially disastrous and embarrassing disclosure of data due to a lost or stolen notebook computer, tampering with passwords, or other unauthorized access. The solution can automatically delete and overwrite data that administrators specify.

Sarbanes-Oxley Act (SOX)

This Act implements multiple reforms to increase integrity in financial reporting. It prescribes:

- Federal oversight of public auditors
- A new set of auditor independence rules
- Protection for “whistleblowers” at publicly traded companies
- New disclosure and reporting requirements applicable to public companies and insiders
- Signed certifications of the integrity of financial reports from CEOs and CFOs

Severe civil and criminal penalties punish persons who are responsible for accounting or reporting violations.

- **WHO MUST COMPLY:** All U.S. and non-U.S. public companies that issue securities in the U.S. public markets, including their auditors, board members and lawyers.
- **WHAT IT COVERS:** Includes financial data and records, and related records and communications.
- **PERTINENT REQUIREMENTS:** An infrastructure designed to protect and preserve records and data from destruction, loss, unauthorized alterations, or other misuse.
- **PENALTIES FOR NON-COMPLIANCE:** Up to a 10-year prison sentence and potential \$15 million fine.

How LiveVault and Connected Backup Solutions Can Help

LiveVault (for servers) and Connected Backup (for PCs, Macs, and servers) solutions help establish the required infrastructure and controls to protect and store vital company financial records, satisfying key requirements for privacy, security, and confidentiality:

- Getting data off-site and off-line protects and preserves the records from destruction, loss, and viruses. It also maintains a duplicate copy stored separately from the original.
- Storing information at an off-site vaulting facility ensures that data is protected and available for business continuity and disaster recovery.
- Using a trusted third-party vendor with a global footprint ensures consistent execution and monitoring of best practices, as determined by internal control frameworks, across the entire enterprise.
- Encrypting backup data prevents unauthorized access.

The Committee of Sponsoring Organizations (COSO, a private sector trade group supporting SOX) Internal Controls Integrated Framework divides the overall problem of IT risk assessment and control into two parts. One part includes general IT processes, such as data management, disaster recovery, and data center operations. The LiveVault and Connected Backup services fall into this category. They comply with SOX requirements and provide strong controls for the data management functions. They also preserve the completeness and accuracy of backup data, so that processing following restoration is reliable. Access is restricted properly, assuring that data is not altered or deleted through the backup process. Only the LiveVault solution provides guaranteed data recoverability through its limited warranty.

LiveVault and Connected Backup solutions ensure that data protection for distributed data is automated and regular. This automated, consistent approach provides proof of a good-faith attempt on the part of enterprises to protect their vital business information for disaster recovery, business continuity, and general records compliance.

FRCP Rule 26

In Federal district courts, Rules 26 and 37 of the Federal Rules of Civil Procedure govern discovery and disclosure of information relevant to civil lawsuits. Recent amendments have altered these Rules significantly. The Rule changes bring about these practical results:

- The definition of discoverable evidence — including electronically stored information (ESI) — is now much broader;
- Litigants must produce requested information more rapidly;
- The penalties for non-compliance are more severe.

Enterprises must respond to these Rule changes to protect their businesses.

Five major rule changes pose risks to all enterprises:

- Rule 26(a) explicitly defines all electronically stored information (ESI) as discoverable, including email, records, documents, plans, schedules, images, and voice mail, regardless of the location or format of the data.
- Rule 26(f) requires that all parties involved in a lawsuit meet early in the process and confer to resolve discovery and, especially, eDiscovery, issues. This rule requires information about electronic data as soon as possible.
- Rule 26(b)(2) recognizes that certain ESI might not be producible because it is too difficult or too costly to do so. Locating this data is essential.
- Rule 26(b)(5) addresses the inadvertent production of privileged information during eDiscovery. Protecting the enterprise's privileged information is vital.
- Rule 37(f) allows for inadvertently destroying requested data, which is permissible only during routine records disposal.

Any enterprise can become involved in a civil lawsuit. These changes to Rules have created new challenges for enterprises to overcome when satisfying the compulsory legal discovery process.

- **WHO MUST COMPLY:** All enterprises that are, or might become, party to a lawsuit.
- **WHAT IT COVERS:** Enterprise information of all kinds, including proprietary information.
- **PERTINENT REQUIREMENTS:** Enterprises must produce requested information rapidly and completely. Enterprises must demonstrate good-faith efforts to retain and produce data, and that destruction of data is not deliberate but part of routine records disposal.
- **PENALTIES FOR NON-COMPLIANCE:** Fines, sanctions, and negative outcomes of lawsuits.

How Iron Mountain Solutions Can Help

While archiving is the preferred method of accessing information for eDiscovery, backup solutions can provide demanded electronic documents. With Iron Mountain's Connected Backup DiscoveryAssist™ solution, enterprises can gain access to and retrieve data across all repositories in Connected Backup Data Centers. DiscoveryAssist offers path and file name filtering to speed data collection, and maintains the file metadata necessary to support third-party search and review. DiscoveryAssist uses Iron Mountain's Connected Backup solution.

Connected Backup (for PCs, Macs, and servers) and LiveVault (for servers) solutions back up and recover documents, email, images, and any other files. These solutions reliably delete electronic records by date in accordance with retention schedules. Filtering recovered files by date simplifies meeting eDiscovery requirements. It also helps exclude privileged information during discovery. Iron Mountain stores all data in its ultra-secure underground facilities. Configurable retention policies — from seven days to seven years — deletes

unnecessary data on schedule, reducing the burden of data management for litigation discovery and demonstrating the enterprise's regular business operations.

The Connected Backup and LiveVault solutions encrypt all data in transit and in storage with AES encryption. Password-protected encryption keys maintain security even when key-holders leave the company.

Iron Mountain's eDiscovery & Litigation Support Services performs gap analysis to reveal weaknesses in existing electronic discovery procedures and to identify potential sources of discoverable electronic information. Gap analysis also helps maintain a defensible chain of custody. Such analysis also streamlines effort and improves workflow to reduce time and expenses for rapid response to discovery requests and investigations. This service also indexes all managed files and securely stores them in our highly scalable digital archives, optionally encrypting them for additional security. Detailed and company-specific litigation hold processes satisfy legal standards.

Iron Mountain's DataDefense solution encrypts sensitive information on computers, including laptops, so that no one can view or use it without the decryption key. With the DataDefense solution, even if privileged information is disclosed to a party during eDiscovery, they cannot view or use that information. Knowing that sensitive enterprise information is protected can speed the production of requested ESI. The Connected Backup solution also offers this capability.

Digital Archives

Digital archiving, retention systems, and services ensure that enterprises have ready access to any given record, whenever it is needed. Solutions available today offer secure, compliant, and cost-effective long-term archiving of electronic records. These solutions and services consolidate electronic records – email, images, statements, and more – into a unified, browser-accessible archive for fast and easy search, retrieval, and management. They also record any action taken on any archived records, providing a secure audit trail to prove that records have not been tampered with, for compliance audits and for cases where litigants must submit legal evidence.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act of 1996) was enacted with a goal to support the protection of personally-identifiable health information (PHI). It limits using and disclosing information about the physical or mental health of an identifiable patient without his or her consent or authorization, as well as specifying the need for safeguards to protect PHI.

- **WHO MUST COMPLY:** Individuals and enterprises, such as doctors and other healthcare personnel, hospitals, pharmacies, medical billing services, healthcare plans, HMOs, and business associates of these enterprises, such as their accountants and attorneys.
- **WHAT IT COVERS:** All medical records and other health information that identifies the individual patient.
- **PERTINENT REQUIREMENTS:** Administrative, technical, and physical safeguards that protect the privacy of a patient's health information by preventing any intentional or unintentional use or disclosure. In addition, records must be recoverable in the event of a small-scale or large-scale disaster.
- **PENALTIES FOR NON-COMPLIANCE:** Up to 10-year prison sentence and fines of \$25,000 per year.

HIPAA has supplemental standards, in the form of "final rulings," which codify how health care providers and those who handle individually-identifiable patient health records must comply. The rulings include provisions that require compliant backup methodologies to ensure that individually identifiable health records remain private and secure. The security and privacy rulings require a backup plan, a disaster recovery plan, and an emergency mode operation plan (Section 164.308).

How LiveVault and Connected Backup Solutions Can Help

LiveVault (for servers) and Connected Backup (for PCs, Macs, and servers) solutions provide critical data security protection without compromising patient privacy. LiveVault and Connected Backup solutions help enterprises meet or exceed HIPAA regulations.

LiveVault and Connected Backup Solutions Meet Security Requirements

Health care providers must implement comprehensive security systems to ensure that they protect electronic patient records against data loss and unauthorized access. A HIPAA-compliant security system must include administrative procedures, physical safeguards, and technical measures to protect patient information while stored, and while transmitted across communications networks. The LiveVault and Connected Backup solutions implement security and availability features in the following areas:

- Preserves a retrievable, physically secure, off-site, exact copy of patient records with easy, frequent data backups. Encrypts all data before it leaves the customer's server and keeps it encrypted during transmission and storage. Only the customer has access to the decryption password.
- Protects backup transmissions further by using integrity controls, mutual authentication, access controls, alarms for abnormalities, auditing of failed logins, and event reporting.
- Simplifies disaster recovery with tools to restore lost data quickly.
- Reduces media control risks, compared to traditional disk or tape backup techniques, by eliminating insecure methods of data handling, especially transporting physical media offsite.
- Offers multiple point-in-time backups per day — as often as every 15 minutes — to ensure that recovery is possible with minimal data loss.
- Allows long retention periods — as long as seven years — to meet HIPAA requirements.

LiveVault and Connected Backup Solutions Meet Privacy Requirements

Under the HIPAA rules for the privacy of personal data, health care providers that engage in electronic transactions must observe privacy safeguards to restrict the use and disclosure of individually identifiable health information. As independent third-party service providers, Iron Mountain and its subcontractors are “business associates” under the HIPAA security and privacy rules. If needed, Iron Mountain will provide and sign a business associates agreement in conjunction with use of the LiveVault service. The LiveVault service and its agents do not receive data for any purpose except to provide data restoration after data loss. Because the data is encrypted before it leaves the customer’s server and only the customer has access to the password, the LiveVault service and its agents cannot access the data.

LiveVault and Connected Backup solutions are important parts of a HIPAA-compliant solution for preventing unauthorized access:

- *Secure Transmission and Storage:* Customer data is encrypted with 256-bit AES encryption (LiveVault), and then transmitted and stored as encrypted data at vaults that reside offsite at a secure remote facility. With the LiveVault solution, customer encrypted data may also optionally reside on an appliance at the customer’s site to facilitate rapid recovery.
- *Logical Access:* Strict controls limit logical access to the data; for example, a secure user interface prevents viewing the contents of data files. In addition, customers can restore data only to the computer where the data originated, or to a computer where the customer has installed the data encryption key. The user interface cannot specify, change, transport, or access data encryption keys.

By preventing loss of data, LiveVault and Connected Backup solutions are also important for HIPAA-compliant strategies:

- *Physical Controls:* The data center is a hardened underground facility, meeting numerous physical criteria. The facility controls access through administrative procedures, physical safeguards, and technical security measures.
- *Redundant Vaults:* All backed-up data resides on two separate, redundant vaults. The data center has redundant bandwidth providers, power, and HVAC.
- *Retention for up to Seven Years:* Customers can retain historical backups for up to seven years.

Both the LiveVault and Connected Backup solutions complement physical safeguards to ensure that recent and vulnerable data receive protection automatically and regularly. This protection is critical, because sources of data are often distributed throughout an enterprise. Many of these sources rarely receive protection because of their remote location or poor resources for manual backup. LiveVault and Connected Backup solutions can ensure that backup and protection extend to all areas of the business and their sensitive data.

This automated, regular approach provides auditors with proof of a good-faith attempt on the part of enterprises to protect their vital business information for the purposes of disaster recovery and business continuity. It also ensures data recovery for operations.

Iron Mountain’s DataDefense™ solution deletes specified data — and can overwrite data locations to prevent recovery of deleted data — under conditions that administrators define. These conditions include a lost notebook computer, password tampering, and other evidence of unauthorized system access. The DataDefense solution can prevent potentially disastrous and embarrassing disclosure of data, for example, when notebook computers are lost or stolen.

Proactive Effort

In addition to meeting the challenges of externally imposed regulations, enterprises must also work proactively to improve their IT processes for security, confidentiality, and robustness. Such proactive enterprises choose business partners and vendors that can assist them to meet these internal goals. SysTrust™ Certification and PCI Compliance are two achievements that demonstrate a partner's commitment to best practices.

SysTrust™ Certification

SysTrust certification is a rigorous process that the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed to provide independent assurances that an enterprise's systems operate reliably and without material errors, faults, or failures. Iron Mountain has achieved SysTrust™ certification — an audit of IT systems by an outside, independent auditor to ensure appropriate internal controls for the security, availability, processing integrity, and confidentiality of the IT infrastructure environment.

Iron Mountain engaged auditor Ernst & Young to perform the most recent SysTrust audit. Certification completed on March 23, 2007. This certification process encompasses Iron Mountain's general IT infrastructure:

- production data center and network operations
- server configuration and database administration
- storage management systems
- disaster recovery processes
- system monitoring tools and processes
- system security (both logical and physical)
- change management and common support processes.

Iron Mountain intends to renew this certification annually.

PCI Compliance

The Payment Card Industry (PCI) Data Security Standard supports secure practices in credit card processing to combat the threat of credit card data loss or compromise. All entities storing, processing, or transmitting cardholder data must abide by the standard's requirements. Iron Mountain has achieved PCI compliant status - an audit of IT systems by an outside, independent auditor to ensure standards for secure networks, protecting data, vulnerability management, and access control. Compliance requirements include the following six areas:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Implementing strong access control measures
- Monitoring and testing networks regularly
- Maintaining an information security policy

PCI-compliant companies must conduct business only with other PCI-compliant members.

Iron Mountain engaged the services of CyberTrust as an independent auditor to ensure and certify that policies, systems, and technologies comply with the (PCI) Data Security Standard. CyberTrust performed an on-site audit, confirming compliance with the PCI Data Security Standard on March 31, 2007, for the records management, data protection, and shredding businesses. Iron Mountain's compliance within the program is defined as a Level 2 service provider. Iron Mountain is currently the only company in its industry validated as PCI compliant.

Conclusion

With the new regulations, the roles and values of digital data protection have expanded. The primary functions of these solutions are to provide disaster recovery and business continuity as part of a comprehensive data protection strategy. These functions, as well as privacy and security safeguards, are now an important component of a Compliant Records Management program.

However, the regulations also require fast recovery of specific data for compliance audits and litigation. Digital archiving of electronic records for audits and litigation requests helps enterprises subject to the regulations reviewed previously. By using the information in this white paper, enterprises can avoid the risk of non-compliance by employing the protections afforded by digital data protection to meet audit and litigation requests for specific records. Iron Mountain products and services support enterprises in their efforts to become compliant corporate citizens.

©2007 Iron Mountain Incorporated. All rights reserved. Iron Mountain, design of the mountain, LiveVault, and Connected are registered trademarks and Iron Mountain Digital, DataDefense, and Discovery Assist are trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America, and the Pacific Rim. For more information, visit our Web site at www.ironmountain.com.