HEALTHCARE

HIPAA PRIMER SERIES

Iron Mountain Data Protection Services

PROVEN, TRUSTED AND HIPAA-COMPLIANT MEDIA MANAGEMENT

Contents

Increasing awareness and requirements surrounding the protection of health information forces you to continually re-evaluate and modify traditional tape backup and archiving practices. To help keep up with ever-evolving regulations, leading healthcare organizations rely on Iron Mountain for secure and compliant media management.

Iron Mountain is the trusted partner for protecting your tapes and helping you recover quickly in the event of a disaster. Our workflows and facilities incorporate the latest in technology, best practices and regulatory compliance. We make sure our tape backup and archiving is compliant, to help you be compliant too.

We protect all of your data as if it were our own, meeting and often exceeding HIPAA standards. That's why Iron Mountain is the healthcare industry's partner of choice for data protection and compliant media management.

To meet the ever-evolving regulatory requirements of today's healthcare environment, you must not only have solid media management practices in place across your institution, but also obtain satisfactory assurances that your third-party partners are HIPAA compliant as well.

MEDIA BACKUP AND ARCHIVING

ARE YOU KEEPING PACE WITH REGULATIONS?

Increasing regulatory demands are placing renewed focus on your approach to tape management. More visibility and accountability than ever before is required across your entire tape program.

Backup tapes and other archived media must be moved, stored, and accessed throughout their lifecycle in compliance with HIPAA privacy and security regulations. These regulations have been made even more stringent under the American Recovery and Reinvestment Act of 2009 (ARRA).

In addition, HIPAA rules now require all of your vendors who handle Protected Health Information (PHI) to be compliant as well. This includes your tape backup and archiving partners.

In other words, in order for you to maintain compliance, you must also obtain assurances that your media management partners are HIPAA compliant as well.

WHAT THE LAW REQUIRES

The HIPAA Privacy Rule requires establishing and implementing measures to ensure the confidentiality, integrity, and availability of all PHI, while the Security Rule addresses safeguards specific to the security of electronic Protected Health Information (ePHI).

Who Must Comply. Health plans, healthcare clearinghouses, healthcare providers (also known as "Covered Entities"), and their business associates, including those that transport or store health information.

What It Covers. PHI includes any information about health status, type of care, or payment for care that can be related to an individual. The term is a broad one, and generally includes all information contained in a patient's medical record and payment history.

What the Penalties Are. The government has ramped up enforcement and penalties related to the protection of patient information. Penalties can reach a maximum of $1.5 million annually per type of violation. On the enforcement side, state attorneys general, in addition to the Department of Health and Human Services (HHS), have been given authority to prosecute HIPAA violations. There has already been an increase in enforcement compared to pre-HITECH Act, and we can expect this to continue with the following:

1. Any civil monetary penalties recovered by HHS will be used for their future enforcement efforts.
2. Individuals harmed by a violation may receive a percentage of the penalties, thus encouraging both patients and authorities to report violations.

By working with a partner who understands the latest regulations and has proven best-practice programs in place, you ensure that your patient information is handled according to the highest standards of security and reliability.

YOU NEED A PARTNER YOU CAN TRUST

Partnering with a specialist in media backup and archiving can reduce both your costs and risks. You benefit from their experience and technology investments, while freeing up your resources to focus on your core mission of delivering outstanding patient care. And, you ensure that your PHI is safe but accessible in the event of a disaster.

What Your Partner Should Provide. Beyond basic backup and recovery, your partner should offer technology to help you better manage your media. Automation provides access to tools, such as email alerts and validation statistics, which help streamline the discrepancy reconciliation process. In addition, automated procedures create comprehensive audit trails you can use to further ensure the security of your backup data.

Is Your Partner Compliant? Finally, as required under the new regulations, you need to obtain assurances that your media management partner is HIPAA compliant. This means they must understand the latest regulations and have proven best-practice programs in place to ensure that your patient information is handled according to the highest standards of security and reliability.

By choosing a data protection provider with these capabilities, you can be confident that you and your partner are compliant, realize a high level of reliability for day-to-day operations, and further ensure timely recovery in the event of a disaster.

WHAT TO LOOK FOR IN YOUR VENDOR'S COMPLIANCE

Among other things, your vendors must:

- ☑ Comply with their contracts to secure PHI, and control its use and disclosure.
- ☑ Have appropriate safeguards in place that satisfy the requirements of the Privacy and Security Rules.
- ☑ Report all HIPAA privacy and security incidents to you.
- ☑ Hold their agents and subcontractors to the same restrictions and conditions that they face.
- ☑ Provide you with the necessary information to respond to patient requests to "account for all disclosures."
- ☑ Be able to make their records related to PHI available if you are audited.
- ☑ Return or destroy all PHI if your contract has expired or is terminated.

Iron Mountain's proprietary InControl® security platform offers an end-to-end approach to managing, controlling and auditing media in transit. Combined with our high-security storage facilities, this creates a compliant media management solution that not only meets but exceeds HIPAA regulations.

IRON MOUNTAIN

A PROVEN MEDIA MANAGEMENT SOLUTION

Iron Mountain is the leader in offsite data protection and recovery, with more than 19,000 professionals and facilities worldwide. We operate our own secure transportation services with rigorous chain-of-custody control for media in transit. While in storage, your tapes are protected in secure, environmentally optimized vaults, yet available to you 24/7/365. With Iron Mountain Offsite Tape Vaulting, you reduce the possibility of data losses, theft and business interruptions, while enabling rapid recovery in the event of a disaster or other disruption.

We offer:

- Enhanced processes and workflows for greater efficiencies.
- Highly secure facilities and vehicles.
- Advanced Web-based tape inventory management tool.
- Real-time reporting and alerts to notify you of potential inventory discrepancies.
- Evolved best practices for compliant media management.

OFFSITE TAPE VAULTING

Access Backup Data in a Timely and Efficient Manner. Iron Mountain Offsite Tape Vaulting service is a proven, reliable solution for cost-effectively protecting your data and recovering efficiently in the event of a disaster. We protect your backup data securely, getting it offsite, offline and out of reach. And, we make tracking and managing your offsite data easy with SecureSync®. This Web-based tape inventory management system offers you complete visibility and control of all your backup, vaulting, and recovery activities.

INCONTROL PROTECTS YOUR TAPES IN TRANSIT

Security is especially critical when your backup tapes are in transit. That's why every Iron Mountain vehicle is equipped with InControl, the advanced transportation platform that ensures the protection of your sensitive information in transit in three key ways:

1 PREVENTION

Secure vehicles featuring patented locking mechanisms, vehicle alarm systems, and other innovative technologies.

2 EARLY DETECTION AND CORRECTION

Wireless scanning validates pickups and deliveries and maintains chain of custody. This allows us to identify and reconcile inventory discrepancies immediately, at the point of origination. Similarly, real-time authorization verification ensures that media exchanges occur only between an authorized employee and the courier.

3 PROOF

A real-time audit trail that documents every transaction. For increased visibility, you may opt to receive proof of service via email.

We offer:

- 24/7/365 emergency response.
- Rigorous chain of custody and audit trail for clear accountability.
- Proven best-practice processes that support your ability to conduct business in a HIPAA-compliant way.
- Consistent vaulting practices across all of your sites for enhanced compliance.

Our proven processes and stringent controls increase safe, secure handling. From the time your data is in our possession until the time it is returned to you, access is restricted exclusively to authorized personnel — yours and ours. At key points in transport and handling, tapes are scanned both for tracking and to document chain of custody. While vaulted, tapes are protected by card-key access, video surveillance, and highly trained security personnel. Prior to release, and at your option, we use Personal Identification Number (PIN) verification to validate the authorization level of individuals involved in media exchange (see page 9 for more information).

Archive Your Vital Data for Improved Business Continuity and Disaster Recovery. Iron Mountain Offsite Tape Vaulting also provides healthcare providers a highly compliant and reliable solution for long-term backup and disaster recovery. Our vaulting facilities are strategically placed within reach of major commercial centers and hot sites, yet removed from high-risk areas such as flood plains and fault zones. Backup tapes can be quickly delivered to any recovery location you choose via our secure fleet of vehicles or the third-party carrier of your choice.

Our highly trained professionals can also assist with testing your disaster recovery plan. We have participated in over 43,000 disaster recovery tests and are uniquely qualified to help you validate your plan.

Compliant Media Destruction. Secure destruction is an important part of any compliant media management program. Tape backups should not be archived longer than needed or required by law. Iron Mountain offers proven media destruction services with multiple authorizations and sign-offs to ensure that the right media is being destroyed. This process generates an auditable chain of custody for increased compliance, as well as a certificate of destruction to verify completion.

Workflows that Work

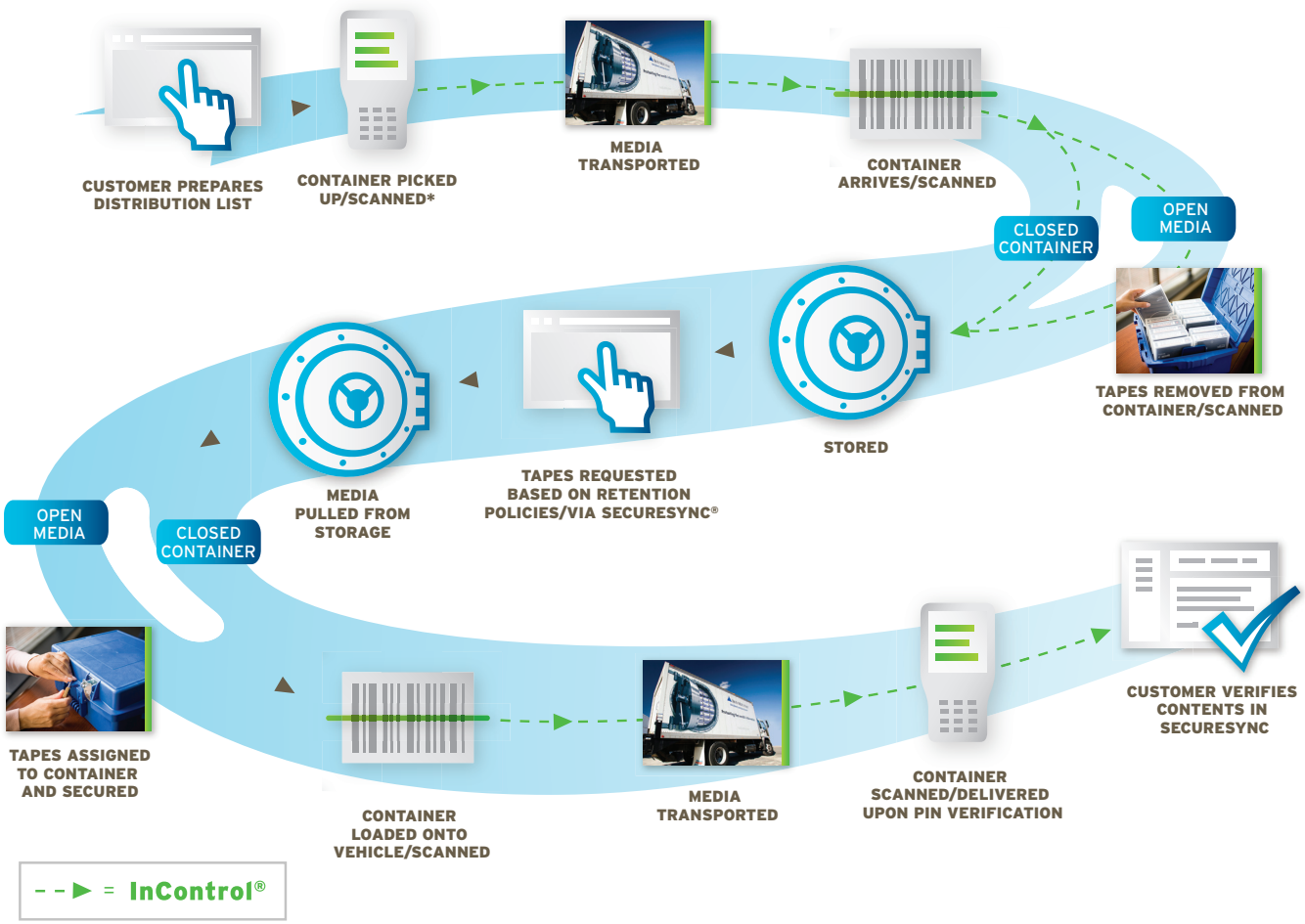
Iron Mountain's proven, highly evolved workflows protect your media at every stage of pickup and delivery. Our stringent procedures for authorization, exchange, storage, and transport allow your media to be preserved over time yet readily available should you need it.

STRENGTHEN THE CHAIN OF CUSTODY WITH PERSONAL IDENTIFICATION NUMBER (PIN) VERIFICATION

Once enabled, PIN verification requires users to enter a unique code before they can send or receive media. This feature helps you tighten the media management process and reduce risk by:

- ☑ Documenting all transfers and receipts.
- ☑ Ensuring media is only released to authorized parties at your location.
- ☑ Registering activity in your SecureSync account and allowing you to view the individuals associated with a specific handoff.

OFFSITE TAPE VAULTING WORKFLOW



*Each scan point allows us to identify and reconcile inventory discrepancies immediately, at the point of origination.

Iron Mountain has invested years in developing a proven, comprehensive approach to compliant media backup and archiving. And, we continue to invest in keeping our systems up to date with the latest HIPAA regulations. As a result, we are able to provide you the expertise and resources you need to reduce risk across your organization and realize timely recovery in the event of a disaster.

HIPAA COMPLIANCE AND BEYOND

Since tapes and other physical backup media must be handled and transported frequently, they pose a special compliance challenge. Iron Mountain has taken the lead in meeting that challenge with our InControl platform, an end-to-end approach to managing, controlling and auditing media transportation. Combined with our high-security storage facilities, this allows Iron Mountain to meet or exceed HIPAA regulations.

And, we enforce stringent operational processes and procedures to ensure the protection and preservation of your sensitive information at all of our facilities across the country. The bottom line is, we make sure our tape backup and archiving is compliant, to help you be compliant too.

KEY REQUIREMENTS OF THE HIPAA PRIVACY AND SECURITY RULES

The HIPAA Privacy Rule is intended to ensure that PHI is not used or disclosed inappropriately or without the patient's permission. The Security Rule is specifically designed to protect PHI that is used and stored electronically. Both aspects of the rule apply to data protection. HIPAA rules cover three broad areas of activities:

Administrative Safeguards. Operational processes and procedures, such as training, access restrictions, and workflow, to enforce that information is always handled according to policy. Additionally, this section of HIPAA requires a contingency plan, also known as a disaster recovery plan.

Physical Safeguards. Physical controls such as locks, access to keys, and supervision, to protect against unauthorized physical access.

Technical Safeguards. Data-related information systems and associated controls, such as database security, network protection, and user authorizations and passwords, to protect data from software intrusions and attacks.

INCREASE CONTROL, VISIBILITY, AND COMPLIANCE WITH SECURESYNC

SecureSync provides you complete visibility and control of your backup, vaulting, and recovery activities.

- ☑ Rapidly search your inventory to locate tapes needed for disaster recovery, patient treatment, or any other purpose.
- ☑ Authorize and track how your employees access and use PHI.
- ☑ Consistently document and manage retention policies.
- ☑ Easily request schedule changes, access reports, and track exceptions.
- ☑ Create and maintain your latest disaster recovery plan.

MEDIA MANAGEMENT COMPLIANCE CHECKLIST

HIPAA regulations now require your business associates, as well as your own institution, to be compliant. Iron Mountain maintains the following policies and procedures to promote compliance.

ADMINISTRATIVE

- ☑ Dedicated resources to monitor protection systems
- ☑ Employee screening and background checks
- ☑ Employee training for the appropriate handling of PHI
- ☑ Standardized workflows to ensure best practices
- ☑ Multiple scans/signatures when information is shipped or destroyed
- ☑ Personal Identification Number verification to limit access only to authorized personnel
- ☑ Web interface to help you manage and track records-related activities
- ☑ An adequate and reasonable disaster recovery plan that addresses risk
- ☑ "Full deployment" testing at least once a year, covering disaster recovery plans, processes, people and infrastructure

ADMINISTRATIVE SAFEGUARDS

HIPAA requires documented procedures for operational processes, such as training, workflow, and a disaster recovery plan, be put in place to reinforce that information is always handled according to policy. Iron Mountain meets this requirement, and helps *you* meet it, in several ways.

Access and Use. Iron Mountain has tight controls so that information in our care is used or disclosed *only* for the purpose of delivering our services. Using advanced security measures, such as InControl technology, employee identification badges, and 24/7 surveillance, we physically restrict and monitor access to your backup tapes during transit, storage, and disposal. What's more, we provide you with the tools necessary to manage and monitor your employees' authorization and access.

Privacy Policies and Procedures. Iron Mountain employs a comprehensive approach to protect your sensitive information. This includes dedicated security resources, safety and security policies, regular audits, and effective employee training and management oversight. We also strictly enforce processes governing access to our buildings, and maintain a highly secure chain of custody for all patient information under our care.

Workforce Training and Management. Since backup tapes must be handled and transported, workforce training and management is a high priority for any compliance program. Iron Mountain boasts an exceptional screening and training program for all of our employees. Our training policies include:

- Comprehensive background checks for new hires.
- Screening of drivers.
- Employee training for the appropriate handling of PHI.
- Special safety and security screening for destruction specialists and equipment operators.

Mitigation. In order to achieve and maintain compliance, you must evaluate the security and compliance of your media management program on a regular basis. Iron Mountain has created a team dedicated to monitoring HIPAA requirements and evaluating our compliance. This team proactively tracks changes to industry regulations and works with Iron Mountain operations personnel on an ongoing basis to improve processes, mitigate risks, and reinforce continued compliance.

Data Safeguards. Safeguards should extend across all processes, such as securing media with lock and key, limiting access to keys or pass codes, and destroying tapes before discarding. Iron Mountain maintains data safeguards for tapes in our care across all operations and for all personnel. Safeguards include:

- Stringent controls for security, custody, transportation and delivery of your data.
- Personal Identification Number verification to limit access only to authorized personnel.
- HIPAA-compliant media destruction.
- Best-in-class storage facilities (see page 14).

Record Retention and Compliant Destruction. The proper, permanent destruction of all PHI in accordance with retention policies is necessary to reduce the risk of a security breach and maintain compliance.

Iron Mountain's secure media destruction facilities leverage consistent information disposal policies and processes. We obtain multiple authorizations and sign-offs to verify that only the right media is being destroyed. Upon approval, all tapes eligible for destruction are rendered permanently unreadable and then destroyed by incineration.

This highly compliant destruction process meets the requirements of the safe harbor to avoid breach notification by rendering the media PHI unusable, unreadable, or indecipherable by encryption or destruction.

Disaster Recovery Plan. We complement your disaster recovery plan with our best practices, compliant workflows, and strategically placed facilities for storing your backup data. Located near major hot sites but removed from high-risk areas such as flood plains and earthquake zones, our facilities provide optimal security. Additionally, our secure fleet of vehicles protect your backup tapes while in transit.

Audit Trail. Iron Mountain maintains a comprehensive approach to auditing and tracking your tapes throughout their lifecycle. Our solution offers:

- Tools and reports to help manage access, including unique employee identification, monitoring of facilities access, and scanning of tapes and tape containers whenever handled or moved.
- Complete audit trail for all media in our possession, from storage through transport and up to media exchange.
- Record of employee training, enforcement, and program monitoring and a Certificate of Destruction to verify completion of all media that has been destroyed.

Checks and Balances. Our workflows incorporate numerous redundant steps to validate the integrity of all tape pickups and deliveries, archiving, and ultimately destruction. At every stage of handling we validate the order's accuracy, comparing it against the previous step in the process.

MEDIA MANAGEMENT COMPLIANCE CHECKLIST

PHYSICAL

- ☑ Secure archiving of backup records offsite
- ☑ Physical access controls, such as locked facilities and visual monitoring
- ☑ High-security storage facilities with guards, intrusion detection, and alarm systems
- ☑ Environmental controls, fire detection and suppression systems
- ☑ Loading and locking of tapes in a container before an exchange takes place
- ☑ High-security vehicles for transporting records
- ☑ HIPAA-compliant destruction with multiple sign-offs and an auditable chain of custody

TECHNICAL

- ☑ Strict regulations that prohibit employees from loading, reading, or using a tape in any way except as necessary to deliver the service

PHYSICAL SAFEGUARDS

Your backup and archived tapes are secure with Iron Mountain. We've developed what we believe are the highest standards for facility security in the industry including:

- Placement of facilities outside of high-risk areas, with comprehensive risk-assessment processes for all facilities, taking into account risk factors such as high crime, industrial railroad lines, and other hazards.
- Careful incorporation of physical access controls.
- Advanced fire suppression controls with ceiling and in-rack sprinkler systems.
- Intrusion detection systems, monitored by a central station.
- Strictly enforced process controls for admittance and monitoring of personnel entering and exiting facilities.
- Geographically separated, world-class underground media vaults.
- Mandatory facility audits to enforce accountability and monitor compliance.

Transportation Standards. Our utilization of secure fleet vehicles for the pickup and delivery of your sensitive information ensures information is protected while in transit. Our vehicles are equipped with dual-key ignition, driver proximity alarms, a high-security key-locking mechanism, and door-ajar ignition prevention. Additionally, our drivers use real-time wireless scanning technology and PIN verfication to maintain an auditable chain of custody and limit access to only authorized individuals. Our advanced vehicle security, vehicle process controls, driver screening and background checks, and auditable workflows provide a foundational defense against potential information loss and prevent common transportation-related errors.

TECHNICAL SAFEGUARDS

The technical requirements of HIPAA apply primarily to the security of electronic data and data-related systems and serve to protect data from software intrusions and attacks.

Iron Mountain prohibits its employees from loading, reading, or using a tape in any way except as necessary to deliver the service. We strictly enforce this policy, leveraging advanced security technologies to limit and track employees' access and monitor the location of your tapes at all times. Additionally, there is no equipment onsite that can be used to read or write data, meaning your tape data physically cannot be accessed while being stored at our facilities. As a result, you can feel confident that your data will remain safely vaulted and, in turn, unexposed to software intrusion and attacks.

BEYOND COMPLIANCE

HIPAA requires that your partners be HIPAA compliant. To further mitigate risk, however, Iron Mountain goes beyond compliance. We employ best practices we have developed and learned at leading hospitals and other healthcare institutions around the country. This best-practice approach ensures that all reasonable measures are taken to protect patient information, to remain in good standing with the law and the public, and to promote a positive and responsible image in the community.

CONCLUSION

With more than 30 years of data protection experience in healthcare, over 90 dedicated facilities, and 3400 highly secure vehicles, you can be confident that Iron Mountain has the resources and expertise necessary to support your compliant media management program. We have invested years in developing a proven, comprehensive approach to compliant media backup and archiving. And, we continue to invest in keeping our systems fully up to date with the latest HIPAA regulations.

By leveraging our compliant data protection solutions and extensive industry expertise, you can establish best practices across your organization to reduce risk — and bring peace of mind while improving audit preparation, reporting capabilities, and overall media program management.

That's why Iron Mountain is the trusted tape backup and archiving partner for healthcare providers nationwide.

To learn more about our HIPAA-compliant data protection solutions for healthcare, contact us today at 1-800-899-IRON.

HIPAA PRIMER SERIES

Our HIPAA Primer Series offers you in-depth insights into the proven best practice policies and procedures Iron Mountain employs to ensure that our solutions not only meet but exceed HIPAA requirements.

To learn more about how a specific solution can help you ensure your information remains highly secure yet accessible throughout its life cycle, check out additional best practice guides from this series, including:

IRON MOUNTAIN CLOUD STORAGE SOLUTIONS
HIPAA-Compliant Solutions for Health Information Challenges

IRON MOUNTAIN DATA PROTECTION SERVICES
Proven, Trusted and HIPAA Compliant Media Management

IRON MOUNTAIN DOCUMENT CONVERSION SERVICES
The HIPAA-Compliant Approach to EMR Transition

IRON MOUNTAIN RECORDS MANAGEMENT SERVICES
HIPAA-Compliant Solutions That Keep *You* Compliant

IRON MOUNTAIN RELEASE OF INFORMATION SERVICES
Coming Soon

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.