HEALTHCARE

The HIPAA Primer

WHAT YOU SHOULD KNOW ABOUT THE NEW REGULATIONS

Contents

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal regulation governing the protection of patient information, has been a part of the healthcare landscape for years. Now that same landscape is changing rapidly with the growing adoption of Electronic Health Records (EHR) and the American Recovery and Reinvestment Act of 2009 (ARRA).

The ARRA legislation makes billions of dollars available to accelerate the adoption of electronic records. In addition, it establishes new requirements for privacy and security, as well as more aggressive enforcement and increased penalties for violations. It is important to note that this legislation extends HIPAA requirements to third-party partners and vendors.

Understanding these new requirements is a critical challenge for every institution. Iron Mountain has prepared this primer to help you navigate the changes in HIPAA, clarify the role of vendors and other third parties, and heighten your awareness of best practices that will aid in compliance and improve the management of both paper and electronic health records.

More information can be found at www.ironmountain.com/hipaaprimer

What is Protected Health Information (PHI)?

PHI includes any information about health status, type of care, or payment related to 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'S NEW WITH HIPAA

HIPAA AND THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

In February 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA), designed to spur the national economy. Two provisions of the legislation have a direct impact on health information and HIPAA.

First, ARRA enacts strict time limits for adopting Electronic Health Records (EHR), and provides $19.2 billion in funding towards this goal. By 2015, healthcare providers must show meaningful use of electronic records or be subject to lower Medicare and Medicaid reimbursement payments. Second, ARRA includes the Health Information Technology for Economic and Clinical Health (HITECH) Act, which expands existing requirements to protect the privacy and security of health information, as well as other provisions related to health information technology.

The legislation is extensive and detailed, and should be studied at length by appropriate healthcare professionals. This section explains the major highlights of the rules and how they have changed.

KEY CONCEPTS:

- The American Recovery and Reinvestment Act of 2009, designed to spur the national economy, includes provisions for funding EHR adoption.
- The Act also includes specific revisions to the original HIPAA regulations passed in 1996.
- HIPAA rules have been tightened and penalties for violations have increased.
- Regulations have been extended to most third-party vendors ("business associates") who are now directly responsible for their own HIPAA compliance and are subject to penalties.

WHAT DOES IT MEAN TO BE HIPAA COMPLIANT?

HIPAA regulations establish what must be accomplished to protect patient privacy, but do not provide specific guidance for how to do this. In general, being HIPAA compliant means:

- Reasonable and appropriate policies and procedures must be in place that satisfy the detailed requirements of the Privacy and Security Rules.
- These policies and procedures should address the use, disclosure and security of PHI.
- Procedures should be documented, employees trained, the process should be audited and compliance tracked.

YOU ARE LIABLE FOR COMPLIANCE – AND SO ARE YOUR VENDORS

One of the important changes in HIPAA is to whom it applies. In the past, HIPAA rules were aimed primarily at "covered entities" – hospitals and other care providers. The third parties you do business with ("business associates") had to comply by contract but faced no direct enforcement.

Now that has changed. Under the new law, business associates are fully subject to HIPAA's privacy and security regulations. What's more, healthcare providers and other covered entities have certain responsibilities for making sure their business associates meet their HIPAA privacy and security obligations. If you know of a breach or violation by a business associate, you are required to take reasonable steps to correct it. If such steps are unsuccessful, you must terminate your business associate agreement. And, while you are not directly liable for HIPAA violations committed by your vendors, terminating your agreement may be disruptive and your reputation and image could be tarnished in the process.

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 privacy and security incidents to you
- Hold their agents and subcontractors to the same restrictions and conditions that they face
- Make arrangements to handle patient requests for PHI
- 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

Now let's look at the most important changes the HITECH Act made to the HIPAA rules themselves.

SECURITY RULE HAS BEEN BEEFED UP

The Security Rule has been considerably strengthened and applies to your business associates as well as to your organization. The Security Rule requires you to protect the confidentiality, integrity and availability of electronic protected health information (ePHI) in three broad ways:

- **Administrative Safeguards.** Operational processes and procedures, such as training, how people work, and processes for releasing information must be documented.
- **Physical Safeguards.** Physical controls such as locks, access to keys, restricted areas, and supervision ensure electronic information systems and ePHI are protected from unauthorized physical access.
- **Technical Safeguards.** Data-related information systems and associated controls, such as database security, network protection and user authorizations and passwords, that protect ePHI and control access to it.

It's worth noting that many of the security requirements involve the training and supervision of people, and an investment in technology. Therefore, these requirements can be difficult and costly to implement and verify, especially for smaller outside vendors with limited resources.

For more details on the Security Rule, please see Appendix A.

PRIVACY RULE REMAINS STRONG

In general, the HIPAA Privacy Rule remains unchanged under the new legislation. As before, HIPAA sets national standards for protecting personal health information, and limits the use or disclosure of that information without specific patient authorization. The Rule requires that appropriate safeguards be in place and also gives patients the right to obtain a copy of their health records and to request corrections.[1] What has changed is the addition of breach notification provisions, discussed below, and that business associates are now required by law to comply with certain provisions of the Privacy Rule and are subject to penalties for non-compliance.

MANDATORY NOTIFICATION OF PRIVACY AND SECURITY BREACHES

If PHI privacy or security breaches occur, you must report them to all affected individuals and to the Department of Health and Human Services (HHS). If the breach affects 500 or more individuals in one state, you must also report it immediately to HHS and to the media. Breaches affecting less than 500 individuals can be reported annually. Your business associates are required to report breaches to you, the covered entity. You should also know that HHS is required to publish reported breaches on its website[2] when more than 500 individuals are affected, including each covered entity involved in the breach.

What is considered a security breach?

A security breach is defined as any use or disclosure that "compromises the security or privacy" of protected health information. In addition, the breach must pose a significant risk of financial, reputational, or other harm to the individual to trigger the obligation to provide notice.

MORE AGGRESSIVE ENFORCEMENT AND INCREASED PENALTIES

The government has ramped up enforcement and penalties related to the protection of patient information. Penalties can now reach a maximum of $1.5 million annually per type of violation. On the enforcement side, State Attorneys General have been given authority to prosecute HIPAA violations, putting such cases squarely in the political arena and at the forefront of public awareness. And, in the future, individuals harmed by a violation may receive a percentage of the penalties, thus encouraging patients to report violations.

STRICTER ACCOUNTING OF DISCLOSURES

While individuals have always had the right to request a report detailing who their medical record was disclosed to, this requirement has been made stricter. As part of the effort to promote the adoption of the EHR, the HITECH section of ARRA has been amended to include the tracking of treatment, payment, or healthcare operations disclosures of PHI made through an EHR.

The Take-Away

Stricter regulations, larger penalties, stronger enforcement, the inclusion of business associates and greater public visibility all place an increased burden on healthcare entities and their partners to understand HIPAA regulations and take firm steps to bring policies, people, systems and procedures into compliance.

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

ASK THE VENDOR:

1. "Have you audited your solutions to ensure they are HIPAA-compliant?"
2. "Can you deliver against the provisions incorporated in our contract?"
3. "What policies and procedures have you put in place to monitor the use or disclosure of PHI?"
4. "Have your employees been properly trained?"
5. "Do your agents and subcontractors to whom you provide PHI agree to the same restrictions and conditions that you do?"

FIVE THINGS TO ASK YOUR VENDORS

WHAT TO ASK YOUR VENDORS TO VERIFY HIPAA COMPLIANCE

The previous section explained that business associates are now fully accountable for HIPAA compliance. If you contract with outside vendors, you are required to take reasonable steps to ensure they maintain secure procedures for handling PHI and are compliant with HIPAA regulations – up to and including canceling contracts and terminating relationships.

Of course, most vendors will say they are HIPAA compliant. However, as a healthcare entity, you need to be certain of compliance in order to avoid costly, disruptive changes to your organization.

To help you evaluate a vendor's HIPAA compliance and ensure that you have appropriately safeguarded patient information, this section provides five key questions you should ask every outside business associate.

KEY CONCEPTS:

- Vendors are now held to the same legal standard as providers for HIPAA compliance.
- Providers are responsible for holding vendors accountable to their contracts.
- Identifying compliant vendors may be difficult.
- To avoid having to cancel contracts or change vendors, providers should conduct "due diligence" regarding HIPAA compliance prior to engaging in a partnership arrangement.

As a provider, you should always have clear contracts with your vendors stating explicitly what your expectations are regarding protection of patient privacy. Then, you must hold your vendors accountable for living up to the contracts.

1 "HAVE YOU AUDITED YOUR SOLUTIONS TO ENSURE THEY ARE HIPAA-COMPLIANT?"

A formal risk assessment is necessary to verify any claims of compliance. As part of your vendor selection and due diligence, you should ask if your vendor has conducted a thorough gap analysis comparing their solution's privacy and security controls to HIPAA's privacy and security requirements. Can they demonstrate they have taken appropriate steps to identify and mitigate risks and achieve compliance?

In addition, ask them to verify that they have policies and procedures in place to protect the privacy and security of PHI and determine if they are focused on continuous improvement. This is important because compliance is not a "one and done" proposition, but rather a continuous process.

2 "CAN YOU DELIVER AGAINST THE PROVISIONS INCORPORATED IN OUR CONTRACT?"

As a provider, you should always have clear contracts with your vendors stating explicitly what your expectations are regarding the protection of patient privacy. Then, you must hold your vendors accountable for compliance with those terms.

Ask each vendor to review and verify the terms of the contract. Insist on satisfactory assurances that they can comply. Any vendor you do business with, if they receive or disclose PHI, should have a robust program of compliance.

3 "WHAT POLICIES AND PROCEDURES HAVE YOU PUT IN PLACE TO MONITOR THE USE OR DISCLOSURE OF PHI?"

Promises and policies are not enough to ensure compliance. Ask your vendor how they will track and monitor the use and disclosure of PHI. Do they have regular reviews of procedures? Do they track disclosures and verify that they were done correctly?

Also, make sure your vendor has clear processes for notifying you in the event of a security breach, which they are required to do under the law.

4 "HAVE YOUR EMPLOYEES BEEN PROPERLY TRAINED?"

Even the best policies and procedures rely on the people who implement them. Ask your vendor to provide documentation of their procedures regarding employee hiring, training, attendance and performance. Employee training and documented processes help ensure that everyone understands how to handle records appropriately.

Among the questions you should ask: Do they conduct background checks on new hires? Do they monitor and track attendance and performance? Do they provide specific training on what incidents need to be reported?

Even the best policies and procedures rely on the people who implement them.

5 "DO YOUR AGENTS AND SUBCONTRACTORS TO WHOM YOU PROVIDE PHI AGREE TO THE SAME RESTRICTIONS AND CONDITIONS THAT YOU DO?"

HIPAA regulations require that your vendors hold their agents and subcontractors to the same conditions that you require of yourself and your vendors. Make sure your vendors have signed contracts with their agents that explicitly state expectations regarding privacy and security compliance. Also ask for specifics about how your vendor audits subcontractors to validate compliance. Just as you require validation from your vendors, make sure your vendors require the same of their agents.

The Take-Away

While you as a provider are not liable for vendor violations under HIPAA, you are required to take reasonable steps to correct problems and breaches, including canceling contracts and terminating relationships if necessary. To avoid such disruptive steps and to protect your organization, it pays to ask hard questions of your vendors before you engage them to handle patient information.

Best practices go beyond compliance. They ensure that all reasonable measures are taken to protect PHI, to remain in good standing with the law and the public, and promote a positive and responsible image in the community.

BEST PRACTICES: BEYOND COMPLIANCE

BEST PRACTICES GO BEYOND COMPLIANCE TO MITIGATE RISKS

When most healthcare professionals think of HIPAA regulations, they think in terms of compliance. Indeed, compliance is absolutely necessary, but aiming only for compliance may not fully mitigate risks. Today, public reputation and standing in the community depend on securely protecting patient information – and avoiding negative headlines.

Iron Mountain is helping healthcare organizations to raise the bar by employing best practices gained from experience at leading hospitals and other health-care institutions around the country. This best-practice approach goes beyond compliance. It 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. These are goals that most organizations can readily agree with.

This section examines the best practices in use at leading healthcare organizations nationwide, based on Iron Mountain's direct experience.

For a detailed checklist of best practices, please see Appendix B.

KEY CONCEPTS:

- Best practices provide the details needed to create and maintain appropriate processes and training.
- Best practices go beyond compliance to establish high levels of security and protection.
- Areas of concern include stored records, information in transit, access, employee training and contingency planning.
- Addressing these issues helps to ensure compliance and maintain your standing in the community.

WHEN INFORMATION IS AT REST: STORAGE BEST PRACTICES

Since patient information is "at rest" – stored somewhere in your system – the vast majority of the time, it's important that best practices are used for storing PHI. These practices and requirements include:

- Physical access controls, such as locked facilities and visual monitoring
- Intrusion detection and alarm systems
- Environmental controls, fire detection and suppression systems
- Appropriate security for electronic data, such as encryption, authentication and passwords
- Redundant infrastructure for data centers
- Duplicate copies of data for disaster recovery purposes
- Data integrity checks to detect file corruption
- Dedicated resources to monitor protection systems
- Special management of archived data and disaster recovery (see Contingency Planning)

Physical to digital migration. As you migrate from hard copy to electronic records, a best practice is to centralize the storage of physical records and document conversion services into as few locations as practical or with a single vendor, in order to minimize transportation of PHI and the inherent risks associated with information in transit. The location, or locations, should have appropriate technology, access controls and encryption protocols in place. Also, you should limit the number of people that have access to this information.

Information destruction. Files that are no longer required by law nor needed for care should be properly destroyed. A secure, consistently implemented destruction program can protect your organization and patients by increasing control over records, and mitigating risk and potential liability. Best practices include:

- Retention schedules that encompass federal and state requirements
- Consistent information disposal policies and procedures
- Proof of employee training, ongoing communications, enforcement and program monitoring
- Secure shredding for paper and other hardcopy media
- Audit trail and documentation that both physical and electronic materials have been destroyed to a non-recoverable form
- Secure chain of custody if information is transported for destruction
- Secure destruction of electronic records in accordance with retention policies

WHEN INFORMATION IS IN MOTION: TRANSPORTATION/TRANSMISSION BEST PRACTICES

Information is inherently at greater risk when being moved. Best practices require ongoing and vigilant tracking, monitoring and reviewing of transit events and procedures.

Physical security. When transporting records physically between locations, you should:

- Secure information before transport
- Ensure no damage occurs during transport
- Package loose materials and fragile items in a secure manner
- Use opaque wrapping when transporting medical records to protect PHI

Removable media, such as tapes, should be encrypted prior to transport. Load and lock tapes in a container before an exchange takes place. If combination locks are used, avoid using obvious combinations such as '000' or '123'.

Vehicle security. State-of-the-art vehicle security, vehicle process controls, driver screening and background checks and standard operating procedures provide a foundational defense against potential information loss and prevent common vehicle-related errors.

Chain of custody. It is essential to have a fully documented chain of custody for all patient information, whenever it is moved. The chain of custody should capture the entire handling process, from packing and shipping, to receiving, filing and storage. Leverage real-time scanning capabilities to systematically track and validate information in transit.

Transmission security. When transmitting electronic patient information, these best practices are recommended:

- Use public key encryption for mutual authentication
- To avoid breach notification requirements, implement encryption according to NIST Special Publication 800-111, including at least AES 128-bit algorithms
- Develop security procedures to protect your encryption keys

WHEN INFORMATION IS USED: ACCESS CONTROLS

The first step in controlling access to PHI is managing the integrity of your inventory – knowing what information you have. Best practices include accessing or retrieving only the minimum necessary information to perform a specific job or task, and implementing proper protocol for employees handling PHI.

For protecting electronic information, best practices include:

- Assign a person or department to authorize and supervise password assignments
- Require passwords that combine upper and lower case letters, special characters and numbers
- Change passwords frequently (at least every 90 days) and keep them in a secure location
- Utilize login timeouts to avoid leaving live screens unattended
- Lock user accounts after too many failed login attempts
- Deactivate login credentials for terminated employees

WHEN INFORMATION IS HANDLED: EMPLOYEE BEST PRACTICES

Always screen employees using comprehensive background checks, and train them to properly handle PHI. Reinforce and monitor workflows to ensure that employees access only the minimum information necessary to complete a specific job or task.

WHEN INFORMATION IS LOST OR DESTROYED: CONTINGENCY PLANNING

Contingency planning involves the ability to recover health records and restore services in the event of disaster or data loss. HIPAA regulations for securing digitally stored information require that you conduct a formal risk analysis, and then develop an adequate and reasonable disaster recovery plan that addresses your risks, with policies and procedures in place that cover backup, storage and recovery.

Beyond compliance, best practices demand that your disaster recovery plan lay the foundation for good business continuity. Some basic requirements are:

- Backup records should be securely stored offsite
- Backup data centers and your data and storage archives should be geographically separate from your primary IT infrastructure or computer room
- Backup data centers should not rely on the same infrastructure as the primary site
- Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that meet service level and budget considerations for your organization

In addition, you should regularly and frequently test your plans to ensure you can achieve continuity of business after a disaster. "Full deployment" tests should be performed at least once a year, covering your disaster recovery and business continuity plans, processes, people and infrastructure.

Be prepared through effective disaster planning.
Few if any healthcare facilities have the ability to nearly instantaneously scale resources to meet a disaster. This is one of the most compelling reasons for hiring an outside vendor to provide disaster recovery services – if you can verify that the vendor is truly qualified.

WHEN BUSINESS ASSOCIATES ARE INVOLVED: THIRD-PARTY VENDORS

As noted above, third-party vendors can provide the variable resources you need to supplement your staff. However, be sure your vendors meet the criteria for HIPAA compliance and are able to meet the requirements of your contract.

The Take-Away

Many healthcare organizations are moving beyond compliance and raising the bar through the use of best practices gained from the experience of leading hospitals and other healthcare institutions around the nation. Best practices allow you to maintain a strong defense against HIPAA violations across the full lifecycle of patient records, remain in good standing with the law and the public, and promote a positive and responsible image in your community.

Iron Mountain is a trusted partner to healthcare providers across North America. We safeguard valuable patient information and provide the most rigorous compliance policies and procedures in the industry.

IRON MOUNTAIN'S STORY

IRON MOUNTAIN'S HIPAA-COMPLIANT SOLUTIONS

Iron Mountain has maintained a proactive HIPAA compliance program since the regulations were introduced, to appropriately protect the privacy and security of individually identifiable health information in our possession. We have updated, and continue to update, our policies and procedures to meet the latest government regulations and the needs of our customers. As a general practice we use the most rigorous standards in the industry.

This section reviews the highlights of Iron Mountain's HIPAA compliance program.

KEY CONCEPTS:

- HIPAA has been a focus for Iron Mountain since the regulations were introduced.
- We maintain continuous reviews of our programs to ensure best practices and compliance.
- Iron Mountain works with each individual customer to meet their service level needs.
- Our standards for compliance are second to none in the industry.
- We provide industry-leading Tools for Transformation™ that include documented workflows, secure transport, facility standards, network security, audit trails and employee screening and training.

CURRENT HIPAA PRIVACY AND SECURITY COMPLIANCE PROGRAM

Iron Mountain's compliance program incorporates the physical, organizational, and technical security controls required of business associates by our customer contracts and the Security Rule (see Appendix A).

Iron Mountain's security program is comprehensive and includes dedicated security resources, mandatory safety and security policies, regular audits, and effective employee training and management oversight. Our facilities meet privacy regulation requirements and include physical access controls, intrusion detection systems and advanced fire suppression controls. 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.

In addition, we carefully control and monitor all uses and disclosures of protected health information in our possession, and restrict access to that information to those necessary to deliver our services. These restrictions are reinforced through our policies, procedures, and training.

WHAT YOU CAN EXPECT WHEN PARTNERING WITH IRON MOUNTAIN

While Iron Mountain works with each individual customer to determine their service levels, in general you may expect Iron Mountain's HIPAA-compliant services to follow these guidelines:

- Iron Mountain only uses and discloses customer PHI for the purpose of delivering our services.
- We physically restrict access to customer PHI during transit, storage, and disposal. Digitally stored patient information receives the additional benefit of strong technical controls over access.
- Iron Mountain maintains a regular dialogue with our customers regarding the privacy and security of their protected health information.

A SAMPLING OF OUR HIPAA COMPLIANCE MEASURES

In response to the new regulations, Iron Mountain undertook and completed an extensive compliance assessment of each of our service lines regarding HIPAA's Privacy and Security Rule requirements. We also performed an enterprise-wide risk management analysis and have used this data to drive additional investments in our business operations.

These measures resulted in a number of new operating procedures as part of our HIPAA enforcement, including:

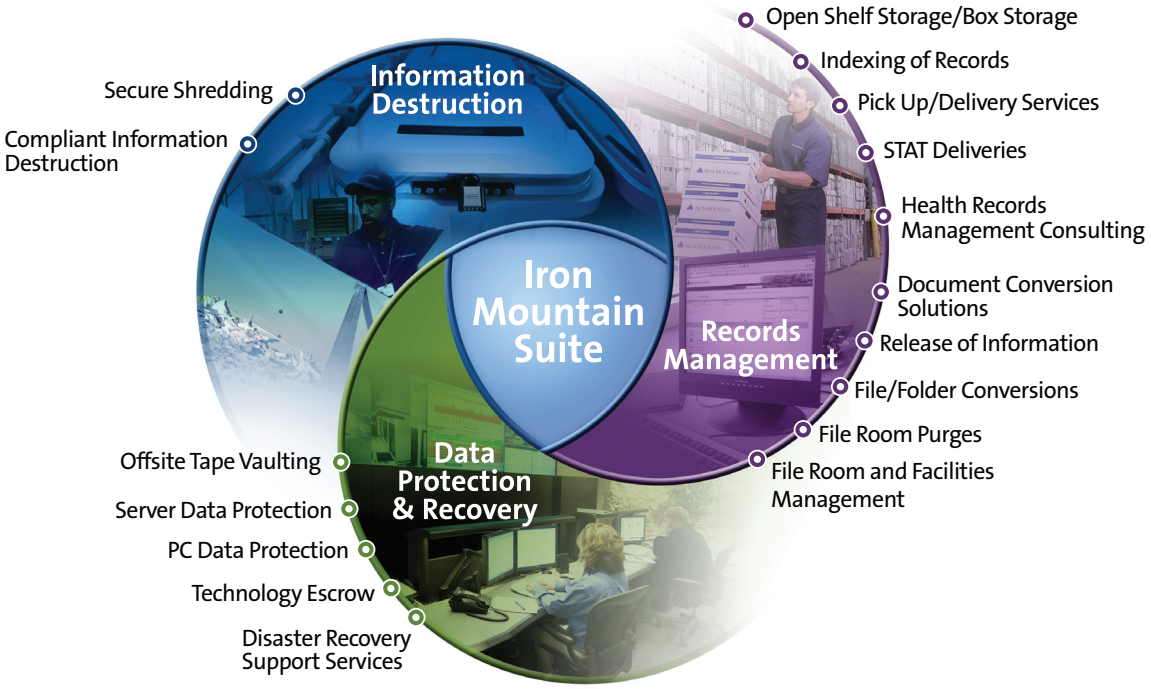
- HIPAA-compliant Business Associate Agreements with all of our 3rd party vendors who handle PHI.
- Redesigned methods and procedures to reduce risk.
- Documented procedures and workflows.
- Updated HIPAA training for all Iron Mountain employees.

In addition, as new rules and guidelines are issued under the HITECH Act's requirements and new provisions come into effect, Iron Mountain is committed to taking whatever steps are necessary to comply.

TOOLS FOR TRANSFORMATION™ – THE IRON MOUNTAIN DIFFERENCE

Healthcare providers are faced with daunting information challenges: Meeting the new HIPAA regulations, achieving best practices, and moving forward with continuous improvement through the transition to the EHR and beyond. Meeting these challenges will require transformational approaches.

Iron Mountain is your partner for achieving transformation, while reducing costs and the risks associated with information protection and storage. More than two thousand hospitals and thousands of healthcare providers rely on Iron Mountain to deliver HIPAA-compliant solutions with proven best practices. Our comprehensive solutions address the complex health information challenges of today and tomorrow, including transitioning to electronic records, regulatory compliance, data protection, image archiving and disaster recovery.



At Iron Mountain, we have the tools to transform the way you manage health information and processes, so you can achieve more than compliance. You can achieve peace of mind.

Documented Workflows/Processes. We've invested millions of dollars in our chain of custody systems, providing unmatched accountability for your patient information. Our industry-leading enhancements include:

- **InControl**®, a comprehensive set of processes that protect information while in transit with fully patented, industry-leading alarms, real-time tracking, and an auditable chain of custody.
- Installation of carton strapping machines in all North American markets.
- Standardization of workflow procedures across all Iron Mountain Record Centers.
- Multi-check process to ensure that every incoming carton is scanned at your location, at the Iron Mountain dock, at the inbound station and at the shelf location, with each scan validated to ensure accuracy and to protect chain of custody. Plus, discrepancy reporting along the way allows us to validate compliance with our processes.

Facility Standards. At Iron Mountain, we've developed what we believe are the highest standards for facility security in the industry. Your records are safe, secure and fully protected. Our facility standards include:

- 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 that include both ceiling and in-rack sprinkler systems.
- Intrusion detection systems, monitored by a central station.
- Strictly enforced process controls governing the admittance and monitoring of personnel entering and exiting facilities.
- Geographically separated, world-class underground data centers.
- Mandatory facility audits to enforce accountability and monitor compliance with standards.

The Numbers Tell the Story

The result of our focused approach to information storage and PHI protection has been nothing short of remarkable:

- More than 45,000 healthcare accounts, including 2,000 hospitals.
- Over 10 million linear feet of medical records and 2 million linear feet of x-ray films stored in our facilities.
- More than a quarter million analog films converted to digital images for delivery to a Picture Archiving and Communications System (PACS).
- Over 65 million data assets stored in highly secure data protection vaults.
- 6 petabytes of digital data under management.
- Over 2.5 million PCs backed up and 70 million digital files restored to date.
- 3,500+ vehicles making 18 million trips a year worldwide.

With our stable customer base and nationwide presence, we are able to commit significant investments to developing new products, services and increased security that keep us at the forefront of protecting and storing sensitive information.

Network Security Features. Protecting the integrity of the corporate network and the privacy of sensitive data is of utmost concern to Iron Mountain. Our data security features are second to none and based on best practices gained from decades of experience. For example, we have implemented a robust network security infrastructure including firewalls, intrusion detection systems and product-level penetration testing by independent 3rd party organizations. We constantly review and update our network security to protect against the latest threats and to maintain accepted best practices.

Audit Trail/Documents. With Iron Mountain, you never have to guess what happened to a document. Our audit trails, monitoring and reporting are comprehensive and thorough and track your documents throughout their lifecycle. This information can be used both for reporting and for continuous improvement initiatives. For example:

- We provide a Certificate of Destruction that verifies service completion for all materials destroyed.
- Our Release of Information Solution includes a detailed accounting of all disclosures.
- We provide detailed tools and reporting to manage authorized system users.
- Iron Mountain creates an audit trail for all materials in our possession.

EMPLOYEE SCREENING/TRAINING:

Employees are the key to successful HIPAA compliance and best practices, and Iron Mountain boasts an exceptional screening and training program for our employees, from records specialists and IT staff to those who drive our vehicles.

Each member of our workforce is trained in HIPAA regulations. As part of this training and ongoing job performance, we reinforce that employees are never to access PHI unless their job requires them to do so. And, we educate every employee on the rules for identifying and reporting incidents. For those positions that handle PHI, such as Release of Information associates, we provide even more detailed HIPAA training.

Our training policies include:

- Comprehensive training guides specifically addressing HIPAA requirements.
- Comprehensive background checks as a standard component of our employee new hire process.
- Screening of drivers as part of standard operating procedures.
- Special safety and security screening for our destruction specialists and equipment operators.

The Take-Away

Building on our history of leadership in HIPAA compliance, Iron Mountain took comprehensive steps when the ARRA legislation was passed to ensure that we meet all federal regulations regarding protection of patient information. Our Tools for Transformation™ provide the capabilities needed by providers to meet the information challenges now and in the future. We are committed to maintaining rigorous compliance programs on behalf of the thousands of healthcare providers. Our healthcare partners rely on Iron Mountain for storage, backup, availability of patient information, destruction and our ability to protect their reputation from risk and harm.

CONCLUSION

The challenges presented to healthcare providers and other entities that handle medical information by HIPAA, combined with the transition to the EHR, require proven and trusted solutions. And, those solutions must be delivered efficiently and cost-effectively.

Iron Mountain has been a leader in providing HIPAA-compliant services since the regulations were first adopted. We have maintained that leadership with the enactment of the ARRA legislation in 2009, taking decisive steps to enhance our processes and training to ensure that our healthcare clients remain at the forefront of best practices in the secure protection of patient information.

With thousands of hospitals and other providers relying on Iron Mountain across the country, you can be assured that we have the resources and the commitment to continue our leadership in the years to come. You can trust Iron Mountain to protect and secure your patient information.

APPENDIX A

Key Elements of the Security Rule Requirements

The HIPAA Security Rule covers protection of electronic protected health information in the following areas:

ADMINISTRATIVE SAFEGUARDS:

- **Security Management Process.** Risk analysis, risk management, sanction policy and information system activity review
- **Assigned Security Responsibility.** Management and supervision of security measures and conduct
- **Workforce Security.** Authorization and/or supervision, workforce clearance procedures, termination procedures
- **Information Access Management.** Isolating healthcare clearinghouse function, access authorization and access establishment and modification
- **Security Awareness and Training.** Security reminders, protection from malicious software, login monitoring and password management
- **Contingency Plan.** Data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures and application and data criticality analysis
- **Evaluation.** Periodic evaluation of security safeguards
- **Business Associate Contracts and Other Arrangement.** Written contract or other arrangement for contingency operations

PHYSICAL SAFEGUARDS:

- **Facility Access Controls.** Facility security plan, access control and validation procedures and maintenance records
- **Workstation Use and Security.** Physical safeguards to restrict access to information
- **Device and Media Controls.** Disposal, media re-use, accountability and data backup and storage

TECHNICAL SAFEGUARDS:

- **Access Controls.** Unique user identification, automatic logoff and encryption/decryption
- **Audit Controls.** Mechanisms to record and examine system activity
- **Integrity.** Mechanism to authenticate ePHI
- **Person or Entity Authentication.** Corroboration that a person or entity is who they claim to be
- **Transmission Security.** Integrity controls and encryption

APPENDIX B

Storage Best Practices

GENERAL

- ☐ Physical access controls, such as locked facilities and visual monitoring
- ☐ Intrusion detection and alarm systems
- ☐ Environmental controls, fire detection and suppression systems
- ☐ Appropriate security for electronic data, such as encryption, authentication and passwords
- ☐ Redundant infrastructure for data centers
- ☐ Duplicate copies of data for disaster recovery purposes
- ☐ Data integrity checks to detect file corruption
- ☐ Dedicated resources to monitor protection systems
- ☐ Special management of archived data and disaster recovery

MIGRATION TO EHR

- ☐ Centralized location or vendor for storage of physical records and conversion services
- ☐ Centralized location has appropriate technology, access controls and encryption protocols in place
- ☐ Full disaster recovery backup of all records at separate location

INFORMATION DESTRUCTION

- ☐ Retention schedules that encompass federal and state requirements
- ☐ Consistent information disposal policies and procedures
- ☐ Proof of employee training, ongoing communications, enforcement and program monitoring
- ☐ Secure shredding for paper and other hardcopy media
- ☐ Audit trail and documentation that both physical and electronic materials have been destroyed to a non-recoverable form
- ☐ Secure chain of custody if information is transported for destruction
- ☐ Secure destruction of electronic records in accordance with retention policies

Transportation/Transmission Best Practices

PHYSICAL SECURITY

- ☐ Securing information before transport
- ☐ Ensuring that no damage occurs during transport
- ☐ Packaging of loose materials and fragile items in a secure manner
- ☐ Use of opaque wrapping when transporting medical records to protect PHI
- ☐ Encryption of removable media, such as tapes, prior to transport
- ☐ Loading and locking of tapes in a container before an exchange takes place
- ☐ Avoiding use of obvious lock combinations such as '000' or '123'

VEHICLE SECURITY

- ☐ Vehicle security and vehicle process controls
- ☐ Driver screening and background checks
- ☐ Standard operating procedures to prevent common vehicle-related errors

CHAIN OF CUSTODY

- ☐ Fully documented chain of custody for all patient information that is moved
- ☐ Tracking of specific activities of handling, including who handles information and when
- ☐ Verifying condition of material at departure and arrival
- ☐ Audit trail maintained and available for review

TRANSMISSION OF ELECTRONIC PHI

- ☐ Public key encryption for mutual authentication
- ☐ To avoid breach notification requirements, implement encryption according to NIST Special Publication 800-111, including at least AES 128-bit algorithms
- ☐ Appropriate security procedures to protect your encryption keys

Access Controls

GENERAL

- [ ] Accurate inventory of PHI and who can access it
- [ ] Policy of accessing and retrieving only the minimum information needed to perform a specific job or task
- [ ] Written protocols, distributed to all relevant workers, for handling PHI

ELECTRONIC ACCESS

- [ ] Designate a person or department to authorize and supervise password assignments
- [ ] Passwords that combine upper and lower case letters, special characters and numbers
- [ ] Policy for changing passwords frequently (at least every 90 days) and keeping them in a secure location
- [ ] Use of login timeouts to avoid leaving live screens unattended
- [ ] Locking of user accounts after too many failed login attempts
- [ ] Deactivate login credentials for terminated employees

Employee Best Practices

- [ ] Screening of all employees using comprehensive background checks
- [ ] Training employees to properly handle PHI
- [ ] Documenting and monitoring workflows
- [ ] Ensuring that employees access only the minimum information necessary to complete a specific job or task

Contingency Planning

GENERAL

- [ ] A formal risk analysis for securing digitally stored information
- [ ] An adequate and reasonable disaster recovery plan that addresses the risks
- [ ] Policies and procedures for backup, storage and recovery
- [ ] Secure archiving of backup records offsite
- [ ] Separation of primary and backup data in geographically dispersed data centers
- [ ] Avoiding use of the same infrastructure for primary and backup sites
- [ ] Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that meet service level and budget considerations for your organization
- [ ] "Full deployment" testing at least once a year, covering disaster recovery plans, processes, people and infrastructure

VARIABLE RESOURCE LOADS

- [ ] Evaluation of the resource load required to meet various disaster recovery situations
- [ ] Planning for "worst-case" requirements
- [ ] Engagement of an outside vendor to manage disaster recovery if needed, to ensure resource availability

Third-Party Vendors

- [ ] All business associates meet HIPAA requirements