IRON MOUNTAIN®

BEST PRACTICES GUIDE

HEALTHCARE

The HIPAA Primer

WHAT YOU SHOULD KNOW ABOUT HIPAA AND THE OMNIBUS FINAL RULE

Contents

3 What's New With HIPAA?

8 Five Questions To Ask Your Vendors

12 Best Practices: Beyond Compliance

17 Iron Mountain's HIPAA Compliant Solutions

22 Conclusion

23 Appendix A: HIPAA Security Rule Requirements

24 Appendix B: Best Practices Checklist

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal statute governing the protection of patient information, has been a part of the evolving healthcare landscape for years. In 2009, the adoption of the American Recovery and Reinvestment Act (ARRA) made billions of dollars available to accelerate the adoption of electronic medical records (EMR). In addition, it established new requirements for privacy and security, as well as more aggressive enforcement and increased penalties for violations that extended beyond providers to third-party vendors. As a result, sweeping changes permeated throughout the healthcare industry including the widespread adoption of EMR technology and a renewed emphasis on privacy and security.

Most recently, the U.S. Department of Health and Human Services (HHS) released the HIPAA Omnibus Final Rule. The Rule replaces the various HHS Interim Rules and conforms HIPAA regulations to the HITECH Act to strengthen privacy and security in today's increasingly electronic times. While industry insiders place the HIPAA Omnibus Rule somewhere between "a regulatory tweak and a sweeping reform," clearly, a working understanding of these requirements is critical to the success of healthcare institutions.[1]

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.

[1] Source: http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

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?

THE HIPAA OMNIBUS FINAL RULE AND THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

In February 2009, President Obama signed into law the American Recovery and Reinvestment Act (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 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 as it clearly communicates the regulatory requirements today and lays framework for iterative requirements in the future. HSS and other regulatory bodies are continually working to clarify and strengthen its components as was most recently demonstrated with the release of the HIPAA Omnibus Final Rule.[2]

The HIPAA Omnibus Final Rule implements, among other things, a number of provisions from the HITECH Act to enhance privacy protections, extend individuals new rights to their personal health information, and strengthen enforcement provisions.[3] The Rule became effective on March 26, 2013, at which time all covered entities and third party vendors were granted 180 days from the effective date to achieve compliance with its final provisions.

[2] http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

[3] http://www.hitechanswers.net/hipaa-omnibus-effective-today/

At a high level, the Omnibus Rule modifications to the Privacy and Security Rules:

- Expand the definition of business associates to include any vendor that creates, receives, maintains or transmits PHI (which will for instance capture cloud service providers)
- Require business associates to enter into a written and comprehensive contract that contains specific provisions required by HIPAA
- Identify new and expanded individual rights
- Update the factors that determine the amount of civil monetary penalties and incorporate the increased and tiered civil money penalty structure
- Replace the Breach Notification Rules' "harm threshold" with a more objective standard
- Require a response to a patient's written request for copies of their PHI within 30 days (eliminating the 60-day timeframe for records maintained offsite)
- Enable patients to request information about care to be withheld if the patient paid for these services out-of-pocket

YOU ARE LIABLE FOR COMPLIANCE – AND SO ARE YOUR VENDORS

In the past, HIPAA rules were aimed primarily at "covered entities" — hospitals and other care providers. The third parties who handle or process PHI on your behalf ("business associates") had to comply by contract but faced no direct enforcement. In today's environment, all business associates are subject to HIPAA's privacy and security regulations.

Covered entities are responsible to enter into a compliant HIPAA agreement with business associates. Furthermore, 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 may not be directly liable for HIPAA violations committed by your vendors unless they are acting as your agent, terminating your agreement may be disruptive and could tarnish your reputation.

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
- Enter into business associate agreements with their vendors
- 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 respond to 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

Omnibus Defines Business Associate

The Omnibus Rule goes to great lengths to clearly identify the criteria for defining a business associate. It's important to understand the nuances of the business associate definition under the Omnibus Rule.

BUSINESS ASSOCIATE: Any organization that creates, receives, maintains, or transmits PHI on behalf of a provider or another business associate is a HIPAA business associate and, therefore, required to maintain compliance with the privacy and security rules.

NOT A BUSINESS ASSOCIATE: Any organization that transmits PHI but does not maintain or store it is considered a "conduit exception" and, therefore, does not require a business associate agreement.

THE HIPAA SECURITY RULE HAS BEEN STRENGTHENED

With the release of the Omnibus Rule, 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.** This definition is a broad one and includes 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 third-party vendors with limited resources.

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

PRIVACY RULE REMAINS STRONG

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. The Omnibus Rule further clarifies the breach notification provisions, penalties, and business associate requirements; these changes are discussed below.[4]

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) within 60 days from the time your organization knew or should have known of the violation. If the breach affects 500 or more individuals in one state, you must also report it 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 if more than 500 individuals are affected, HHS is required to publish reported breaches on its website including each covered entity involved in the breach.

THE AGGRESSIVE ENFORCEMENT AND SUBSTANTIAL PENALTIES CONTINUE

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. Keep in mind, that the $1.5 maximum is per type of violation, not per year. Therefore, the maximum penalties in totality are dependent on how many kinds of violations are found and can vary based on the discretion of HHS.[5]

On the enforcement side, state attorneys general, in addition to the Department of Health and Human Services, have been given authority to prosecute HIPAA violations. In the future, we can expect the following: 1) Any civil money penalties recovered by HHS will be used for their future enforcement efforts; and 2) Individuals harmed by a violation may receive a percentage of the penalties, thus encouraging both patients and authorities to report violations.

EXPANDING THE PATIENT'S ACCESS RIGHTS

While individuals have always had the right to access their records, the Omnibus Rule requires – where feasible – the provision of access to an electronic copy of all ePHI in a designated record set.

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.

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

[5] For example, one healthcare provider was fined $4.3M for failing to provide 41 patients copies of their medical records upon request and subsequently failing to cooperate with an investigation.

A security breach is defined as the acquisition, access, use, or disclosure of (unsecured) protected health information which compromises the security or privacy of the protected health information. A breach is presumed to have occurred unless it is demonstrated that there is a low probability that the protected health information has been compromised based on a risk assessment of the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure of PHI was made
- Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired
- The extent to which the risk to the PHI has been mitigated

FIVE QUESTIONS TO ASK YOUR VENDORS

WHAT TO ASK YOUR VENDORS TO VERIFY HIPAA COMPLIANCE

The previous section of this guide 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 potential business associate.

OVERVIEW OF THE QUESTIONS:

1 "Have you audited your solutions to ensure they are HIPAA-compliant?"

2 "Can you deliver against the provisions incorporated into our contract?"

3 "What policies and procedures have you put in place to monitor the use of 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?"

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.

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?

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

With respect to the use and disclosure of PHI, 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.

Omnibus' Chain of Assurances and Liability"

Providers and covered entities are required to obtain "satisfactory assurances" that PHI will be protected as required by the Privacy and Security Rules from their business associates. **However, the Omnibus Rule now requires business associates to obtain the same assurances from their sub-contractors.**

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.

THE HIPAA PRIMER

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 healthcare 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.

Best practices based on Iron Mountain's 60+ years of experience – in use at leading healthcare organizations nationwide – are profiled here.

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
- Management of archival and disaster recovery data to meet RTO and RPO requirements

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 nonrecoverable 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, you should:

- 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
- Ensure each person has their own, unique login credentials and that user names and passwords are not shared among employees or with vendors
- 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:

- Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that meet service level and budget considerations for your organization
- 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

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 provide the necessary resources to recover from 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, are able to meet the requirements of your contract, and are able to sign a Business Associate Agreement.

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 some of the most rigorous compliance policies and procedures in the industry.

IRON MOUNTAIN'S HIPAA COMPLIANT SOLUTIONS

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.
- ✓ We maintain rigorous compliance standards.
- ✓ We provide industry-leading services that include documented workflows, secure transport, facility standards, network security, audit trails and employee screening and training.

THE IRON MOUNTAIN HIPAA PRIVACY AND SECURITY COMPLIANCE PROGRAM

Iron Mountain's compliance program incorporates the physical, organizational, and technical security controls required by 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.

HIPAA COMPLIANCE MEASURES

In response to the new industry 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 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.

Likewise, as new rules and guidelines, including Omnibus, are issued under the HITECH Act's requirements, and new provisions come into effect, Iron Mountain will address and comply with these provisions.

EVOLVING WITH THE INDUSTRY AND THE ELECTRONIC MEDICAL RECORD

Healthcare providers are faced with daunting information challenges: Keeping up with ever-evolving regulatory requirements, 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 managing this 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.

Iron Mountain can help you transform the way you manage your health information and processes so you can achieve peace of mind.

Comprehensive Information Management Solutions

Records & Information Management

Records Management

Vital Records Protection

Consulting

E-Records Consulting

Project Management

Data Backup & Recovery

Server and Application Data Protection

Technology Escrow

Disaster Recovery

Offsite Tape Vaulting

Document Management

Document Imaging

Hosted Imaging Archive

Discovery Services

Secure Shredding

Onsite and Offsite Secure Shredding

Compliant Information Management Programs

Secure Media Destruction

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 capabilities 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.
- 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 is evidenced by:

- 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 79 million data assets stored in highly secure data protection vaults.
- 6 petabytes of digital data under management.
- 3,400 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 to verify materials have entered the destruction process.
- 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 provides an exceptional screening and training program for our employees, from records specialists and IT staff to those who drive our vehicles.

All members of our workforce responsible for handling PHI are 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 positions such as Release of Information associates we provide even more detailed HIPAA training. Our training policies include:

- Comprehensive training guides addressing specific 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 longstanding history of leadership in regulatory compliance, Iron Mountain took comprehensive steps when the HIPAA Omnibus Rule was passed to ensure that we continue to meet federal regulations regarding the protection of patient information — and we remain committed to this effort. We know healthcare partners rely on Iron Mountain for our best practice approach to the storage, backup, and availability of patient information, as well as our ability to protect their reputation from risk and harm.

CONCLUSION

The compliance challenges facing healthcare providers and other entities that handle medical information 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 maintained that leadership with the enactment of the ARRA legislation in 2009, and more recently with the release of the Omnibus Rule, 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. The bottom line? You can trust Iron Mountain to protect and secure your patient information.

HIPAA Security Rule Requirements

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 Arrangements.** 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

□ Management of archival and disaster recovery data to meet RTO and RPO requirements

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
- □ Wrapping medical records in opaque material when transporting to protect PHI
- □ Encrypting 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

PLANNING RESOURCES TO ADDRESS DISASTER

□ 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

□ All business associates must sign a BA or BAA agreement

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 lifecycle, you can access additional best practice guides in this series including:

CLOUD STORAGE SOLUTIONS

HIPAA-Compliant Solutions for Cloud-Based Storage

IRON MOUNTAIN DATA PROTECTION SERVICES

Proven, Trusted and HIPAA Compliant Media Management

IRON MOUNTAIN DOCUMENT CONVERSION SERVICES

The HIPAA Compliant Approach to Transitioning from Physical to Digital Records

IRON MOUNTAIN RECORDS MANAGEMENT SERVICES

Records Management Solutions That Keep *You* Compliant

Disclaimer: This document is meant to be a general guideline only based on health information management best practices. It is not intended to provide legal advice or guidance. If your institution needs legal help with HIPAA compliance, a suitable law firm should be engaged.