PATIENT PRIVACY AND DATA SECURITY:

UTILIZING IT VENDORS TO MEET HIPAA COMPLIANCE AND AVOID RISKS

TABLE OF CONTENTS

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, was enacted by Congress to protect sensitive patient data. The act contains a "Privacy Rule" and a "Security Rule," which in turn protect the privacy, and set standards for the security of electronic protected health information (e-PHI). Taken together, these rules establish national standards for how companies working with sensitive patient data must ensure that data's confidentiality, availability, and integrity. HIPAA threw a curve ball at the healthcare industry, with mandatory requirements that sent providers scrambling to ensure compliance under HIPAA's rules and regulations. Moreover, the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, brought a dramatic update to the HIPAA Security Rule that more clearly defined the guidelines for proper interaction with health information, expanded the liabilities of companies that are subject to oversight, increased fines for non-compliance, enabled more stringent enforcement and incentivized healthcare companies to move to the digitization of health records.

President Obama carried on the Bush Administration's goal of achieving 100 percent digitization of health records by 2014. While it's not a mandate, the benefits of Electronic Health Records (EHR) are clear and healthcare providers are adopting this technology to improve compliance, reduce medical errors, streamline the delivery of patient care and improve patient outcomes. Under the HITECH Act, healthcare providers are encouraged to adopt EHR, enabling them to collect Medicare and Medicaid incentive payments when they use certified EHR technology to achieve specific objectives. EHR must be used in a meaningful way – for enhancing the delivery, safety and quality of healthcare, as outlined in the Meaningful Use of Electronic Health Records Final Rule.

According to the HIPAA Privacy and Security rules, compliance is required of both Covered Entities (any healthcare provider, health plan or healthcare clearinghouse) and Business Associates (any company that comes in contact with e-PHI while performing services for a Covered Entity). Both have an obligation to keep that data secure.

An update to HIPAA, known as the Omnibus Rule, was adopted in early 2013. The Omnibus Rule includes some major changes, including increased direct liability for Business Associates and their subcontractors as well as a tiered penalty structure for non-compliance.

Penalties for non-compliance vary based on the violation, but range between $100 and $1.5 million with criminal penalties of up to 10 years in confinement. Privacy and security issues related to EHR are handled and administered by the Health and Human Services Office of Civil Rights (HHS-OCR).

WHAT IS THE HIPAA SECURITY RULE?

The HIPAA Security Rule specifically identifies required policies and procedures for ensuring the safety of sensitive patient data. The Security Rule requires Covered Entities to implement necessary administrative, technical, and physical safeguards for protecting e-PHI, sometimes referred to as patient health information.

The Security Rule applies to covered entities such as health insurers, healthcare providers, healthcare clearinghouses, and any Business Associate, such as EHR and EMR vendors or Data Centers, that come in contact with e-PHI by creating, receiving, maintaining, storing or transmitting patient information electronically. HIPAA responsibilities have a trickle-down effect, impacting subcontractors and Business Associates of third-party vendors that come in contact with e-PHI at any point. In fact, the Omnibus Rule explicitly states that third-party data storage providers are considered Business Associates of Covered Entities – whether they ever actually view the data they store or not.

In order to ensure the confidentiality (data is not accessible by unauthorized parties), availability (data is available with appropriate reliability), integrity (data is not altered or destroyed in an unauthorized manner) of e-PHI, Covered Entities and Business Associates must also:

+ Identify potential threats and protect against anticipated threats to the security or integrity of e-PHI
+ Protect against reasonably anticipated impermissible uses or disclosures of patient data
+ Ensure compliance from their workforce, including subcontractors

Compliance with the Security Rule means providers and other Covered Entities, along with third-party contractors, vendors, and Business Associates will implement specific safeguards including:

+ Conducting a risk analysis and documenting reasonably anticipated threats
+ Reviewing policies and procedures regarding the prevention and handling of data breaches, including ensuring staff are trained and knowledgeable in reporting practices
+ Ensuring that e-PHI data is appropriately encrypted
+ Enabling patients to have the ability to obtain a copy of, amend or gain an accounting of accesses to their e-PHI
+ Obtaining Business Associate Agreements and coordinating the protection of e-PHI with all subcontractors or other entities who come into contact with the e-PHI

Covered Entities and Business Associates that come in contact with e-PHI are expected to develop their own procedures and policies based on their size, complexity, capabilities, technical infrastructure, and the likelihood and potential impacts of risks to e-PHI that satisfy the specific Implementation Standards set out in the Security Rule.

The problem lies in the fact that most Covered Entities – and particularly third-party vendors that do business with Covered Entities, i.e. Business Associates -- don't have internal administrative, technical and physical safeguards to implement this level of protection. Most enterprises choose to outsource data storage to a Data Center or Managed Services Firm.

Contracting with a Data Center for storing e-PHI eliminates many of the challenges associated with ensuring data availability, integrity and patient privacy, as Data Centers by definition operate with the highest levels of security, reliability and redundancy. Data Centers offer 24/7/365 management and monitoring of a company's online operations with an onsite, dedicated support team – allowing for immediate detection of potential risks and data breaches for rapid response.

Many Covered Entities don't have the budget needed for the equipment, systems, technology, personnel, and other overhead costs associated with maintaining an on-site Data Center. Outsourcing data storage to a third-party Data Center or Managed Services Firm that can collaboratively manage and monitor the security and integrity of your data is a valuable and cost-effective alternative, but there are many considerations that come into play. Not all Data Centers are created equal, nor do they have appropriate systems in place for handling sensitive e-PHI.

WHAT REQUIREMENTS SHOULD YOU LOOK FOR WHEN OUTSOURCING THE STORAGE OF e-PHI TO A THIRD-PARTY PROVIDER?

Outsourcing the storage of e-PHI makes a lot of sense for many healthcare providers, health IT vendors and other Covered Entities and Business Associates, but choosing a third-party provider with adequate systems and security in place isn't a matter of simply choosing any Data Center. Not all are designed for HIPAA Privacy and Security compliance. The following measures are critical for Data Centers demonstrating the ability to provide your enterprise with services for collaboratively maintaining HIPAA compliance, including confidentiality, availability, and integrity of sensitive e-PHI.

1 EXTENSIVE KNOWLEDGE OF HIPAA AND HITECH RULES AND REGULATIONS

First and foremost, any Data Center you consider for your enterprise should have extensive knowledge of HIPAA and HITECH rules and regulations. You should see extensive information on how a Data Center's systems are set up for compliance on the company's website and/or literature. If not, it's worth inquiring if a Data Center offers the services your enterprise requires, and has the in-depth knowledge and experience to deal with e-PHI.

IDEALLY, DATA CENTERS AND MANAGED SERVICES FIRMS DEMONSTRATING KNOWLEDGE OF HIPAA AND HITECH RULES AND REGULATIONS OFFER:

+ An in-depth understanding of the policies and protocols set forth by HIPAA, the Omnibus Rule and HITECH Act
+ Resources for customers outlining how their organization protects sensitive patient data
+ Regular audits and compliance checks to identify potential threats to e-PHI
+ Response systems in place to quickly respond to potential data breaches
+ Methods to ensure that the customer and Data Center collaboratively protect for the confidentiality, availability and integrity of e-PHI
+ The ability to negotiate and execute a meaningful Business Associate Agreement that defines the relationship and division of responsibilities between the customer and the Data Center in protecting e-PHI

Data Centers that demonstrate comprehensive knowledge and have policies in place to support HIPAA typically provide this detailed information to customers before a contract is signed. With the increasing number of Covered Entities requiring compliant data storage, HIPAA compliance is becoming a major selling point – even a gold standard – for Data Centers and Managed Services Firms.

2 ABILITY TO HELP YOU CHOOSE PRODUCTS AND SOLUTIONS TO MEET HIPAA COMPLIANCE REQUIREMENTS

You should also look for a Data Center that's not trying to sell you a "one-size-fits-all" solution. Organizations that deal with e-PHI run the gamut: Covered Entities range from hands-on health practitioners to health insurers, ancillary health services firms requiring access to third-party patient data, Business Associates of both Covered Entities and their subcontractors, and a variety of other entities. When it comes to dealing with e-PHI, each Covered Entity or Business Associate requires a unique set of data services, including the amount of storage required, the average number of authorized information requests generated within a given time frame, reporting requirements, and other needs.

A credible Data Center provider will walk you through your existing infrastructure to diagnose, assess and manage any threats, vulnerabilities and risks to the e-PHI whether at rest or in motion. These top providers will offer customized solutions based on this individual analysis and assessment, providing a solution that collaboratively meets the requirements under HIPAA.

Standard and Additional Services

The following are standard and additional services offered by HIPAA compliant data centers and managed services firms.

RISK ASSESSMENT TOOL: A risk assessment tool allows Covered Entities and Business Associates to conduct the necessary and required audits and analyses to predict and respond to threats to data integrity, confidentiality and availability of critical patient information. Risks come in many forms, including employee error, unencrypted data, lapses in notification, data stored on mobile devices, and a variety of other situations.

IN-DEPTH, ONGOING RISK MANAGEMENT: A one-time analysis isn't adequate for keeping up with ever-emerging and ever-changing threats to data security. Covered Entities, along with any Business Associate that may come into contact with e-PHI to any degree, must continuously monitor and manage the threat landscape to provide sufficient protection of protected data.

CONTINGENCY PLANNING: What happens in the event of a breach? Rapid response plans are critical to minimize data compromise, especially in the event of a large-scale attack that impacts an entire Data Center. Managed Services Firms and Data Centers must be equipped with backup and contingency plans to minimize impacts and maintain security post-breach.

HIPAA RISK ASSESSMENT SUPPORT: Some Data Centers offer support for Covered Entities and Business Associates to ensure compliance with the HIPAA Security Rule through risk assessments. Risk assessments identify deficiencies related to organizational infrastructure, policies and procedures, documentation, security, and administrative safeguards. The most comprehensive assessments not only identify deficiencies, but offer tips for remediation to ensure strict compliance.

HIPAA AUDIT SUPPORT: A HIPAA audit is stressful for any Covered Entity, with the threat of fines looming as disciplinary actions. When Covered Entities and Business Associates use third-party resources for data storage and management, they typically rely on those third-party providers to maintain necessary security. When an audit rolls around, Data Center support is critical for providing the documentation and evidence needed to prove ongoing compliance.

HIPAA TRAINING FOR DATA CENTER TECHNICAL PERSONNEL: Data Center employees with access to e-PHI are required to undergo training in HIPAA Security requirements and other protocols. This includes any employee working for the Data Center who discusses protocols and policies with Covered Entities or Business Associates, and even those without direct involvement in the service agreement who could potentially access e-PHI. All Data Center personnel must attend periodic training on HIPAA rules and requirements, and Data Centers must ensure that every employee within the organization has an adequate understanding of HIPAA rules, policies, procedures, and processes to support HIPAA compliance.

OMNIBUS COMPLIANT BUSINESS ASSOCIATE AGREEMENT: A comprehensive Business Associate Agreement outlining the protections, compliance, ongoing reporting and risk assessment that's compliant with the recent HIPAA Omnibus Rule.

INTRUSION DETECTION SERVICES: Rapid detection of intrusions to e-PHI.

INTRUSION PROTECTION SERVICES: Comprehensive protection against potential intrusions and risks to e-PHI.

VULNERABILITY DETECTION AND REPORTING: Ongoing analysis and alerts to potential vulnerabilities and rapid reporting to enable sufficient response to risks.

MANAGED ANTIVIRUS PROTECTION: Viruses can expose otherwise secured data, so managed antivirus protection is critical when outsourcing e-PHI storage and management to third-party providers.

The following features make it possible to store, access, and transfer data through secure, encrypted connections and encrypted data files that make it difficult or impossible to access data even if a breach occurs. This includes proper encryption of both data at rest and data in motion. Encryption converts plain text into ciphertext, which appears to third-parties as nothing more than a random set of characters. Data is decrypted only when a transfer is complete or data at rest is being accessed by an authorized person. Encryption makes it impossible for unauthorized third parties to decipher text and obtain sensitive e-PHI.

Encryption represents one of the most effective practices for maintaining confidentiality. All data leaving, coming in to,

or stored within the Data Center should be encrypted for maximum protection. Data in motion is commonly encrypted even by business entities that don't handle e-PHI as a general sound security measure.

However, most attacks occur at end points where data is at rest, not when it's in motion - making proper encryption of stored data equally important. Data at rest is encrypted either by encrypting the entire database or only specific columns and rows. Encrypting the entire database sometimes creates performance issues, while encrypting partial databases may restrict sensitive data from authorized users.

Availability of e-PHI is especially important within the healthcare industry, in some cases more critical than others. A surgeon, for instance, prepping to perform emergency surgery on a critically ill patient requires immediate access to the patient's data. If e-PHI is inaccessible at a critical time of need, the data would be unavailable, possibly putting a patient at greater risk. Likewise, a last-minute insurance pre-authorization for a potentially

These features, when combined, create a comprehensive layer of security with maximum protection for the confidentiality and integrity of e-PHI and ensured availability for authorized access

MANAGED TRANSMISSION ENCRYPTION SERVICES: Managed transmission encryption services protect and obscure data while in transit, reducing the likelihood of interception and interpretation by unauthorized persons.

IPSEC VPNS: Internet Protocol Security (IPSec) Virtual Private Networks (VPNs) allow remote access to e-PHI while maintaining security standards.

SSL/TLS SESSIONS: Secure Socket Layer (SSL) and Transport Layer Security (TLS) Sessions are additional security layers that allow secure access to, retrieval of and transmission of sensitive e-PHI.

SSH, SFTP: Secure Shell (SSH) and SFTP (SSH File Transfer Protocol) enable secure data access, transfer and management capabilities.

MANAGED STORAGE ENCRYPTION SERVICES: Managed Storage Encryption Services encrypt data stored on servers, preventing interpretation even if data is breached or accessed by an unauthorized party when it's not in transfer.

SELF-ENCRYPTING FILESYSTEMS: Self-Encrypting Filesystems are a valuable tool for encrypting files and folders both on local machines and devices and on remote servers, protecting e-PHI from unauthorized access.

MANAGED ENCRYPTED BACKUP: This feature allows Covered Entities and Business Associates to create a backup copy of data—essential for unanticipated data losses—while encrypting the data so that even IT support staff are unable to decipher the information.

APPLICATION LEVEL ENCRYPTION: This encryption layer protects data at the application level with precise control over access levels.

REDUNDANT FIREWALL PROTECTION: Firewalls are a standard security measure, but redundant firewalls add an extra layer of reliability. These are ideal for business-critical data infrastructures like those of Covered Entities and their Business Associates.

DMZ CONFIGURATION/DATABASE ISOLATION: A Demilitarized Zone (DMZ) configuration allows some data to be public-facing while private data, like e-PHI, remains private and secure. Likewise, Database Isolation restricts specific sensitive databases from access to unauthorized personnel, ensuring maximum security for e-PHI.

KEY SERVER ISOLATION: Key Server Isolation is a complex security protocol that isolates a full, specified set of keys based on actions, ensuring the integrity of data falling within those keys by locking editing capabilities.

DDOS MITIGATION SERVICES: Denial-of Service (DDOS) Mitigation Services are a recovery tactic used to minimize damage from a DDOS attack. DDOS Mitigation redirects traffic to a different location to protect the core network when an attack is detected.

AUTOMATED OS SECURITY PATCHES: This feature automatically implements operating system-based security patches, eliminating the need for Covered Entities to maintain in-house IT security personnel with the knowledge required to effectively implement these critical updates.

life-saving measure, delayed due to the unavailability of data could be catastrophic for patients, providers, and Business Associates. That's why a detailed risk assessment to evaluate the way in which e-PHI will be accessed, along with the proper safeguards such as backup systems to ensure availability, are an essential consideration when choosing a Data Center. Your Data Center should provide a combination of features and security measures that balance security with availability.

Clearly, there's more that goes into adequately securing e-PHI than a simple antivirus program and an encrypted database. When you consider outsourcing data storage to a Data Center or Managed Services Firm, these considerations are critical. Data Centers offering most or all of these features and safeguards will likely provide the most comprehensive services for HIPAA compliance.

CAPABILITY TO HELP YOU DESIGN YOUR COMPANY'S TECHNOLOGICAL STRATEGIES, POLICIES, AND PROCEDURES TO COOPERATIVELY MAINTAIN HIPAA COMPLIANCE

In addition to a series of comprehensive security safeguards and practices that maintain the confidentiality, availability and integrity of e-PHI that is stored, accessed or transmitted, a Data Center partner should be able to work with a Covered Entity or Business Associate to define the responsibilities of each party in the relationship.

Every entity involved in the access, storage or transmission of e-PHI shares responsibility for maintaining the confidentiality, availability and integrity of that sensitive patient information. Vendors and associates work more effectively when they work together to create strategies, policies, and procedures to collectively maintain HIPAA compliance.

ENSURING COMPLIANCE ACROSS ALL PARTNERS AND VENDORS

The HIPAA Security Rule specifies that Covered Entities, in order to maintain compliance, are required to review and modify their security policies and procedures on a regular basis. When organizations add new Entities – such as clinics or vendors – which have remote access to e-PHI through portable devices, external systems or hardware not owned or managed by the Covered Entity, this is a particularly relevant requirement. Because today's healthcare organizations are constantly evolving and changing, with new clinics and practices changing hands or opening every day, frequent reviews of policies and procedures are good practice.

Data Centers should address the characteristics of your organization's current environment as well as the potential impacts and safeguards necessary, should there be changes to that environment. This means preparing for the addition of service vendors or partners, new firms which coordinate or are involved in financial transactions related to patient care and any other organization with potential access to e-PHI as well as implementing policies and procedures which address the addition of any entity involved at any stage of the continuum of coordinating, delivering or documenting patient care or data in any way.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

Administrative Safeguards comprise more than half of the HIPAA Security Rules, solidifying the importance of having ample protocols in place. Compliance with these standards requires "an evaluation of security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived

from a number of factors unique to each covered entity," according to HHS.gov. Working with your Data Center on the evaluation, analysis and implementation of solutions allows for more seamless collaboration and, therefore, better compliance across the board.

Likewise, technology safeguards are necessary for controlling access to e-PHI by any party with or without authorization. As a Data Center participates in the storage and protection of your organization's e-PHI, working collaboratively and sharing knowledge of existing conditions, potential risks, current protections and plans of action in the event of a breach is necessary for the adequate protection of data. Policies and safeguards must be both comprehensive and easily understood by all parties for sufficient protection and compliance.

This means creating rules and guidelines for:

- Access to e-PHI
- Defining and protecting entry points
- Securely backing up data
- Transmitting data
- Generating reports

Physical Safeguards address the potential threat to e-PHI surrounding the physical electronic information systems, related buildings and equipment. These safeguards are in place to protect against natural hazards, such as building fires, physical damage to data servers, environmental hazards and unauthorized intrusions.

Protective measures such as the redundant backup of data, which ensures the availability and integrity of data after damage to data servers or destruction of electronic equipment, are Physical Safeguards.

Because there are no specific requirements on the type of technology Covered Entities must employ, the guidelines are flexible. Covered Entities must create and implement their own safeguards to ensure adequate protection for e-PHI. But healthcare providers and other Covered Entities aren't often thoroughly versed enough in the field of IT security to create adequate standards and safeguards without outside expertise. It's in this case that working collaboratively with a Data Center with in-depth knowledge of HIPAA provides value.

Any changes to the current environment, like the addition of an external vendor, require evaluation of existing safeguards and updates as necessary. The addition of a third-party vendor introduces additional physical endpoints, data sources, transmissions and other factors that create inherent risk to e-PHI. This is why ongoing evaluation is a necessary requirement, and

a requirement best handled in collaboration with a Data Center partner that demonstrates the knowledge necessary to provide appropriate recommendations and services.

WILLINGNESS TO SIGN A BAA WITH YOU

A Business Associate Agreement (BAA) isn't just a requirement of HIPAA, it's a critical foundation for any working relationship between Covered Entities, Business Associates, third-party vendors, and Data Centers and Managed Services Firms. A Data Center must be willing to sign a comprehensive BAA with your organization.

Data Centers should also maintain BAAs with any vendors or consultants they work with to ensure across-the-board compliance. The need for a BAA is a trickle-down process impacting the entire vendor chain. In other words, Business Associates maintain BAAs with their vendors, who in turn must implement BAAs with their third-party contractors and vendors, and so on. The Department of Health and Human Services describes some examples of vendor and contractor arrangements that qualify as Business Associates:

- Third-party administrators assisting providers with claims processing
- CPAs providing accounting services to health providers when access to e-PHI is possible
- Attorneys providing legal services to health plans when access to e-PHI is possible
- Consultants providing utilization reviews to hospitals
- Healthcare clearinghouses that provide claims transactions and forward processed transactions to payers
- Independent medical transcriptionists serving physicians
- Pharmacy benefits managers managing a health plan's pharmacist network

Due to the trickle-down effect, Data Centers providing data storage and security services to any of the above-described vendors and Business Associates therefore qualify as Business Associates also. This necessitates a Business Associate Agreement with any Covered Entity and Business Associate with which the Data Center conducts business.

The Business Associate Agreement is the first step in the requirements for implementing a strict set of policies and procedures for maintaining HIPAA compliance and protecting e-PHI.

A BAA should:

- Describe the allowable and required use of e-PHI
- Provide that the Business Associate will not use or share any private data, other than what is outlined in the Agreement, unless necessary or required by law
- Require the Business Associate to implement adequate safeguards to prevent any unauthorized use or disclosure, outside of what is provided for in the contract
- Outline the reporting requirements in the event of a breach, also noting that the Agreement may be terminated should a breach occur and remedies are unsuccessful

Data Centers should utilize BAAs as a standard practice with all Covered Entities and related Business Associates.

ABILITY TO DEMONSTRATE DETAILED, WRITTEN INTERNAL POLICIES AND PROCEDURES THAT PROTECT THE CONFIDENTIALITY, AVAILABILITY, AND INTEGRITY OF YOUR e-PHI

The initial BAA is merely a starting point in the process of working with a third-party vendor or contractor. Any time a Covered Entity or Business Associate engages with a third-party provider or vendor that will be in contact with e-PHI, both parties must work collaboratively to adequately maintain the proper configurations, processes and procedures to protect e-PHI per the HIPAA Privacy and Security Rules.

When Covered Entities and Business Associates work with any third-party provider, proper coordination and supervision of the relationship between all involved parties is necessary to ensure continued compliance. This supervision and coordination must be ongoing and is necessary for keeping all parties on the same page and up to speed on compliance, potential risks, safeguards and response plans.

The HIPAA Privacy Rule outlines prohibitions against improper use and disclosure of e-PHI. The HIPAA Security Rule supports and promotes this objective with three clear goals:

+ Confidentiality: e-PHI is not available or disclosed to unauthorized persons
+ Availability: e-PHI is accessible and usable on-demand by authorized persons
+ Integrity: e-PHI is not altered or destroyed in an unauthorized manner

A Data Center partner must work closely with you to implement certain administrative, physical and technical safeguards to ensure HIPAA data security is in place, according to the U.S. Department of Health and Human Services.

You and your Data Center must have the following administrative safeguards in place:

Administrative Safeguards

+ SECURITY MANAGEMENT PROCESS
A Data Center must have processes in place for identifying and analyzing potential risks to e-PHI, implementing security measures that reduce risks and vulnerabilities to acceptable and reasonable levels. Risks impact confidentiality, integrity, and confidentiality and can take many forms, including unauthorized access, destruction of data, improper transmission, inadequate protection, and more.

+ SECURITY PERSONNEL Your Data Center must designate a security official who is primarily responsible for developing and implementing its security policies and procedures. A designated security official maintains responsibility for the oversight and implementation of all security policies and procedures, serving as the primary point of contact for all security issues. A single responsible official streamlines the process of overseeing the many complex requirements and regulations under the HIPAA Security Rule, Privacy Rule, and Omnibus Rule.

+ INFORMATION ACCESS MANAGEMENT
The Privacy Rule standard limits the use and disclosure of e-PHI to the "minimum necessary." As such, the Security Rule requires Covered Entities, as well as their Business Associates, to implement policies and procedures for authorizing access to e-PHI only under essential circumstances. Data Centers implementing role-based access comply with these requirements by deeming necessary access and permitting access only to the extent necessary under specific circumstances.

+ WORKFORCE TRAINING AND MANAGEMENT
All Data Center workforce members who work with e-PHI should be authorized, closely supervised, and thoroughly trained in the Data Center's security policies and procedures. Having appropriate sanctions in place, and applying appropriate sanctions against workforce members who violate these policies and procedures are also necessary administrative safeguards.

+ EVALUATION Periodic assessments of the extent to which security measures, policies and procedures are adequate and meet expected standards are necessary for meeting the requirements of the Security Rule as well as ensuring continued compliance. These periodic evaluations are often the key risk identifiers, allowing Covered Entities and Business Associates to take rapid action and implement appropriate plans for mitigating risks.

You and your Data Center should also have the following physical safeguards in place:

Physical Safeguards

+ FACILITY ACCESS AND CONTROL
Physical access to Data Center facilities must be limited and restricted to authorized personnel only, and to times when access is considered reasonable and necessary. However, Data Centers should also ensure that necessary access is readily available to authorized persons for ensuring the continuous delivery of essential patient care and all related services.

+ WORKSTATION AND DEVICE SECURITY
Your Data Center must implement policies and procedures specifying proper use of and access to workstations and electronic media. Shared workstations, for instance, can lead to violations of the Security Rule, should an unauthorized workforce member have unnecessary access to e-PHI, including access codes and passwords which would permit access to data – even if those codes and passwords are actually never used to gain unauthorized access. In addition, Covered Entities and Business Associates must implement policies and procedures regarding the transfer, removal, disposal of, and re-use of electronic media. This ensures adequate protection of e-PHI.

Physical and administrative safeguards are just a portion of the provisions necessary for maintaining compliance and ensuring the full protection of e-PHI. You or your Data Center must also implement technical safeguards, including the following:

Technical Safeguards

+ ACCESS CONTROL This technical safeguard ensures that only authorized persons have access to e-PHI by implementing technical policies and procedures that control, limit, and block access based on authorization and permission levels. Data Centers should incorporate access controls that include specific procedures and rules for adding new users, each user's privileges for accessing various data sets, as well as each user's permissions for enabling commands and other specific tasks. This not only reduces the likelihood of unauthorized access, but it also aids in preventing accidental destruction, transfer, or compromise of data by a user who is unfamiliar with the data system and its controls.

+ AUDIT CONTROLS Hardware, software, and procedural mechanisms are implemented by compliant Data Centers for recording and examining access and all other activity within information systems that contain or use e-PHI. These audits track and monitor access levels, generating reports including the persons accessing e-PHI, under what circumstances and even at what times, providing a comprehensive overview of appropriate use and identifying inappropriate access.

+ INTEGRITY CONTROLS Maintaining the integrity of e-PHI is critically important for many reasons. Sensitive patient data impacts the delivery of appropriate healthcare, billing, insurance information, and practically every aspect of the entire healthcare system. This is important for both Covered Entities and Business Associates, regardless of what type of e-PHI is handled or transferred through the Entity or Associate. Integrity controls ensure that e-PHI is not improperly destroyed or altered in any manner, and verify that the data's integrity is intact.

+ TRANSMISSION SECURITY These technical security measures guard against unauthorized access to e-PHI when data is in-transfer over an electronic network.

CONCLUSION

Choosing a Data Center or Managed Services Firm capable of handling the many complexities surrounding HIPAA compliance isn't an easy decision. This guide represents a comprehensive overview of the many requirements under the HIPAA Security Rule, HIPAA Privacy Rule, and HIPAA Omnibus Rule that should be carefully weighed before selecting a Data Center.

Data Centers that are well-versed in HIPAA compliance and regulatory issues, especially those which already have comprehensive safeguards, policies, and other measures in place for meeting the needs of Covered Entities and Business Associates, are often the best choice. These Data Center providers are capable of handling continued risk analysis, enabling the rapid response necessary for mitigating identified and perceived risks for maximum protection of all parties involved in the planning, delivery, coordination of, documentation, or any aspect of the healthcare spectrum involving e-PHI.

Under the new HIPAA Omnibus Rule, responsibilities are extended down the complete supply chain, encompassing all third-party vendors and contractors involved in any portion of the storage, transmission, use of, or contact with e-PHI. These policies, procedures, and safeguards are necessary in the modern healthcare system for ensuring complete patient privacy and confidentiality. Maximum compliance results in the streamlined delivery of care and all administrative aspects surrounding healthcare while providing enhanced protection for patients, vendors, Covered Entities, Business Associates and all third parties involved at any stage.

The high cost of a HIPAA violation – whether it has financial or legal implications – simply isn't worth it. Outsourcing data management to a third-party Data Center partner should simply be a top priority for all Covered Entities and Business Associates working in or with the healthcare system. The costs offset by using a third-party Data Center partner are compounded by the value of adequate protection and the avoidance of thousands of dollars in fines for non-compliance. Choose your Data Center wisely, and the benefits are multi-fold. +