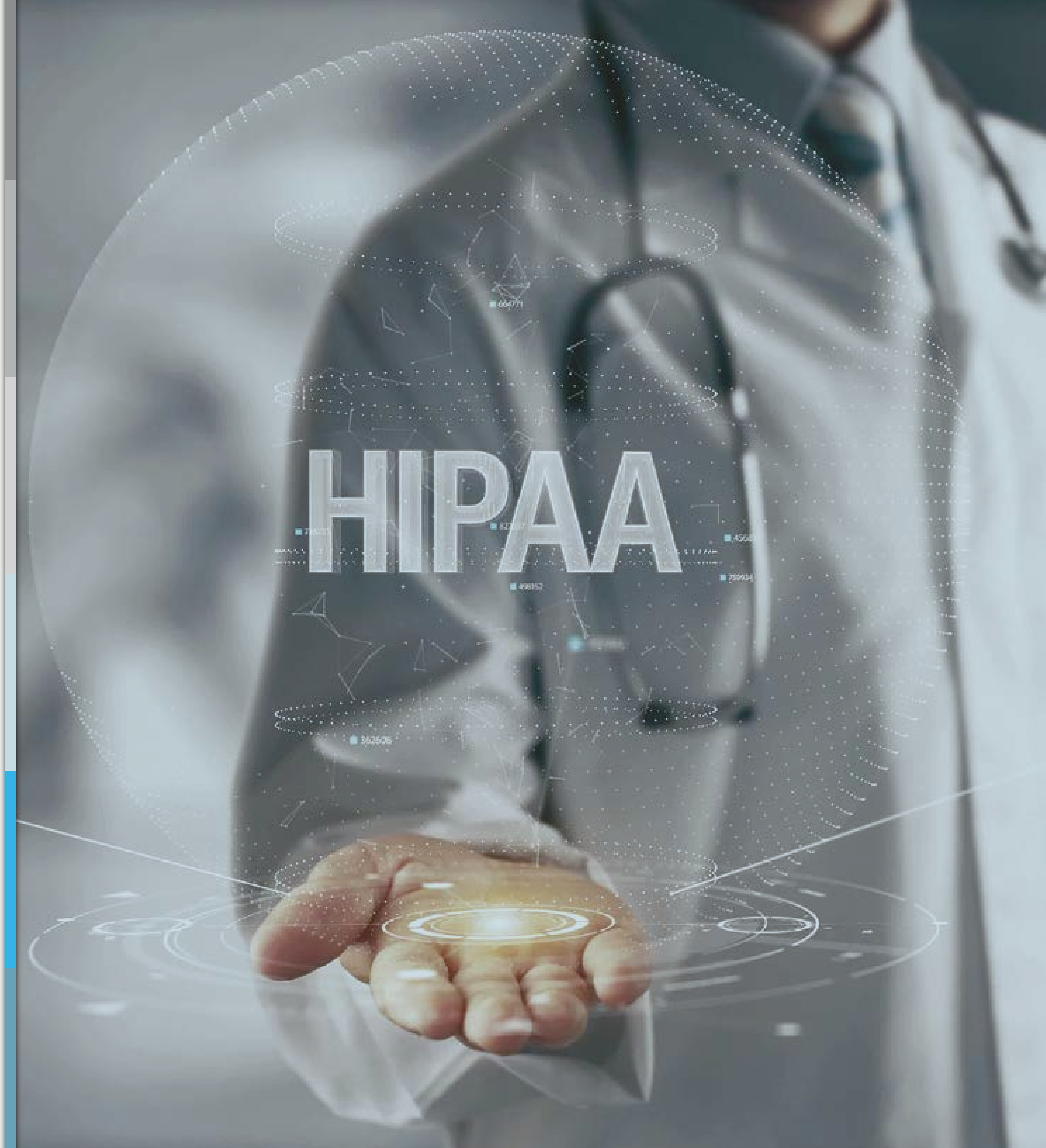
DATABANK
Data Center Evolved™

HIPAA COMPLIANT HOSTING IN A DATA SECURITY DRIVEN AGE

HIPAA
HITECH
Compliant

It’s been more than twenty years since The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a legal foundation for securing Protected Health Information (PHI). The Act directs the Department of Health and Human Services (DHHS) to set standards and regulations employed by medical facilities and associated organizations to protect sensitive patient information.

HIPAA
HITECH
Compliant



THE DIGITAL TRANSFORMATION HAS UNINTENDED CONSEQUENCES

According to P&S Research, The global Cyber Security market is expected to reach $165.2 billion by 2023. And with good reason. As evidenced in the headlines, healthcare data breaches continue to rise, with growing vulnerabilities in telemedicine and IOT-linked medical devices and equipment. This poses a serious threat to the privacy of patients and to the wellbeing of the companies entrusted with the security of their protected healthcare information (PHI). Given the depth of information in a medical record including family history, demographic data, insurance information, and medications to name a few, the value of healthcare related data is greater on the black market than a financial record. In fact, Forbes states that there were nine times more medical than financial records breached in 2016 — 27 million — representing nearly 10% of the U.S. population. In addition, stolen medical records are used to commit Medicare and Medicaid fraud costing tax payers billions of dollars. No surprise, safeguarding systems has become a top priority for Healthcare companies and IT healthcare professionals.

The increasing movement towards electronic health records (EHR) and health information exchange by healthcare providers has improved the efficiency and effectiveness of the healthcare provided to patients. However, it has also created a complex set of challenges for healthcare professionals charged with protecting patient data. Information security is essential for safeguarding electronic Protected Health Information (ePHI) and preventing HIPAA violations from occurring. A proactive approach in maximizing your security includes taking a detailed look at your organization’s administrative, technical and physical security environments and identifying where external resources can address critical gaps. As healthcare becomes increasingly digitized, understanding how to protect patient data is necessary for any organization that manages ePHI.

A proactive approach in maximizing your security includes taking a detailed look at your organization’s administrative, technical and physical security environments and identifying where external resources can address critical gaps.

UNDERSTANDING AND ADDRESSING RISK IS ESSENTIAL

More than a decade ago, the Health Information Technology for Economic and Clinical Health (HITECH) Act made it a national goal and incentivized the adoption and implementation of electronic heath records (EHR) by 2015. Over the last several years, we have witnessed the difficulty that migrating PHI from a physical source to an electronic source has posed across healthcare segments.

Challenges that commonly arise when any department strives to protect ePHI include:

- Protecting ePHI that is shared or stored with a third party such as a cloud provider
- Ensuring tools used to inform patients about sensitive data are secure
- Providing access controls to only permit use or access by the personnel who require it
- Losing important healthcare information
- Incorrect data input as a result of manual error
- Identity theft
- System viruses, ransomware, malware or other failures
- Loss of connectivity or system performance failures
- Lack of application testing
- Total loss of data
- Downtime

If an organization does not address technical challenges posed by migration and growing cyber threats, they are at risk. Non-compliance of HIPAA rules and regulations can result in fines, legal, reputational, and personal damages for both the patient and organizations involved in the loss. HITECH has created an environment of transparency where data breaches are reported to the DHHS and can result in severe financial and reputational risks. HITECH mandates if a breach results in the disclosure or acquisition of more than 500 individuals' details, the breach will be published on The U.S. Department of Health & Human Services' (HHS) website along with the penalty.

Penalties for non-compliance and the mishandling of ePHI can impact every employee in an organization. It is necessary to provide safeguards for employees and identify the proper procedures for handling and protecting EHR.

GOVERNANCE AND STRUCTURE HELP REDUCE RISK

HIPAA COMPLIANCE OVERVIEW

Following a rigorous security framework can reduce risk and ultimately drive operational excellence. HIPAA compliance sets national standards associated with managing ePHI and ensures every employee in the healthcare industry follows a similar set of rules and goals. Compliance ultimately depends on meeting the spirit and intent of the law and ensuring that security and privacy rules are met.

The U.S. Department of Health and Human Services Office for Civil Rights enforces the three core Administrative Simplification rules that create HIPAA compliance. These rules include the HIPAA Privacy Rule (provides the circumstances under which intentional uses and disclosures of patient information are permitted), the HIPAA Security Rule, (provides safeguards required to prevent unintentional uses and disclosures of patient information) and the HIPAA Breach notification rule (describes the notifications that patients are required to receive if an unintentional use or disclosure of patient information occurs.).

According to DHHS, HIPAA compliance must be adopted by Covered Entities defined as healthcare providers who transmit any health information electronically including health plans and healthcare clearinghouses. Additionally, a Business Associate, defined as any person or entity that performs a function or activity on behalf of or provides certain services to a Covered Entity. A Business Associate must adhere to HIPAA privacy and security rules as described in the Business Associate Agreement.

COMPLIANCE AND EHR

Compliance requires that all systems and methods for storing and transferring data must be evaluated to identify possible risks. Additionally, appropriate measures must be put into practice to prevent disclosures from occurring.

For example, if a company has paper files and documents, the appropriate data may be digitized and the information electronically secured. Any physical data, charts or related items must be placed in a secure location with appropriate security controls and or properly destroyed in a manner that renders the documents completely unusable.

As the volume of ePHI grows it is increasingly common for healthcare organizations to contract a third party or vendor to host and secure their data. It is important for a covered entity to understand that although a vendor may perform functions on the covered entities behalf, the covered entity remains responsible for HIPAA compliance. This is where a Business Associate Agreement (BAA) is essential to the use of vendors. The BAA will clearly identify the responsibility for compliance for each party in the relationship.

The HIPAA Omnibus Final Rule, published in 2013, added a comprehensive privacy and security risk assessment of Business Associates to assist Covered Entities in risk assessment of Business Associates and potentially protect them from damages. The rule requires a new vetting process when selecting vendors to ensure those third parties also adhere to HIPAA privacy rules.

Over time, HIPAA has expanded to include rules regarding digitized patient privacy and security. New regulations determine who has access to EHR and ePHI, when it is appropriate to transmit information, how a facility must manage ePHI, and how to keep ePHI from being lost, damaged, or stolen. Additionally, HIPAA now provides guidance for a plethora of technological risks.

Every employee of an organization with access to ePHI must take measures to prevent the mishandling of patient data regardless of position and access. Even if an employee does not directly interact with ePHI, he or she must be trained to handle digitized patient data and understand evolving HIPAA policies and procedures.

Becoming HIPAA compliant and maintaining HIPAA compliance is a process that requires both time and effort, but has significant benefits for the business. Compliance ensures a company can securely handle HIPAA data, has a procedure for prescribed processes, and is aware of the risks and costs of conducting business securely.

DEVELOPING A COMPLIANCE PLAN

Compliance starts with a clear security plan designed to protect ePHI from loss of confidentiality and integrity, inadvertent disclosure and addresses appropriate solutions if a security breach occurs.

All compliance plans should include a breach response plan and risk assessment plan that identifies possible security breaches that could arise from internal and external threats. For example, an employee telling a third party about sensitive information would be classified as an internal threat. Internal risks include accidentally deleting files, downloading viruses ransomware or other malware, or leaving the system open for hackers. Human errors also account for a portion of security breaches and must be recognized within the risk assessment.

The basic parts of a HIPAA compliance plan include:

- A security plan that determines how the business or facility intends to secure and manage information
- An incident and breach response plan
- Standards for handling sensitive data
- Identification of possible risks and response to risks
- A basic plan of action for normal activities
- Compliance plans for every employee
- Possible strategies for human errors or mistakes
- Recovery plans for any lost data or accidental deletions

Compliance plans are created by the Covered Entity. However, it is not uncommon for the Covered Entity to employ a qualified assessor or advisor to audit business operations or provide recommendations when creating a plan. For portions of the plan that require implementation by a vendor, the Covered Entity would utilize that vendor during the assessment of the Covered Entity's environment.

However, the vendor would only be responsible for assessing the portion of the Covered Entity's compliance plan they will implement. For instance, a managed hosting provider would only review environments within their domain, excluding any local environments and other areas not identified in the Business Associate Agreement (BAA).

As HIPAA rules evolve, compliance plans must address security, privacy and incident response plans and activities should also mature. Recently, many businesses have employed vendors to help accommodate pieces of their compliance plan that require resources beyond a Covered Entity's scope of business operations.

USING A VENDOR

The process of maintaining HIPAA compliance often results in a complex set of obstacles and challenges. A vendor provides a healthcare provider or medical facility with the tools needed to adapt to changing technology as well as adhere to standards in medical care and maintain information. Working with a vendor simplifies the process of maintaining HIPAA compliance as the vendor serves and supports a Covered Entity.

A Covered Entity's compliance plan would determine services an organization may need a vendor to implement. Once a plan of action is determined, the vendor will be required to sign a Business Associate Agreement (BAA) before providing any services.

The BAA is a contract or legally binding document that governs the responsibilities of each party and guides and protects both parties when HIPAA violations take place. Additionally, the BAA determines who is responsible for potential complications such as a breach in security or employee errors. All BAA's must include permitted uses and disclosures, requirement to use appropriate safeguards, requirement to report non-permitted uses and disclosures, and requirement to extend same terms to subcontractors/agents.

Vendors may have access to ePHI the Covered Entity is responsible for managing. Even if the vendor does not have direct access to ePHI, they may provide a specific service or several services to the facility or company that would accomplish data related tasks. Often vendors provide long-term services such as ePHI management, security, and HIPAA compliant hosting.

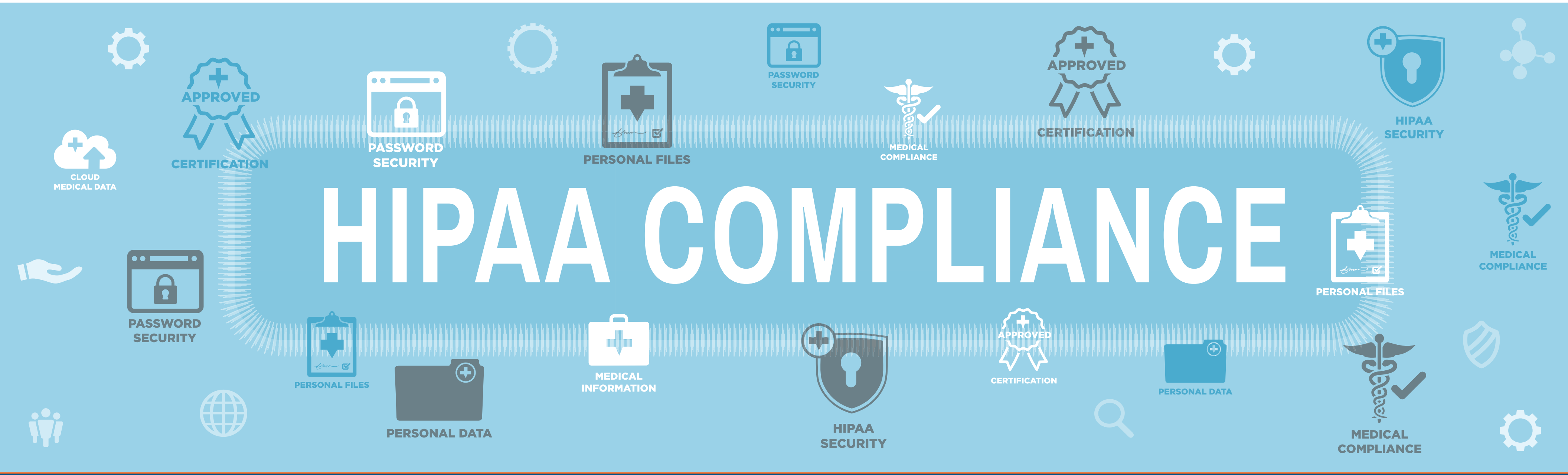
HIPAA COMPLIANT HOSTING

Data Center Colocation providers and Managed Hosting Providers understand HIPAA compliance and the laws and regulations related to HIPAA. They also staff security and compliance leaders that address these items daily for their customers. Hosting providers provide necessary security safeguards for a covered entity's ePHI as well as related services. Their vast and comprehensive knowledge of privacy rules and standards ensure the Covered Entity is able to maintain HIPAA compliance as technology evolves and hackers become more advanced.

If the Covered Entity's current system does not have appropriate precautions to protect their ePHI, a Data Center service provider may make directed changes and appropriate adjustments and modifications to ensure compliance. Data Center providers also offer security features required by HIPAA like encryption in transit or at rest. Additionally, Data Center providers may provide appropriate documentation and guidance for weak security controls.

Administrative tasks and advice about physical security are additional advantages offered by Data Center providers. For example, a Data Center provider may employ a physical biometric access control system in place to limit the risk of any data loss from a physical intruder. Their services may also include advice about audit control and TripWire, a service used to monitor the integrity of files and documents.

Data Center and managed hosting providers offer a key service to healthcare IT professionals trying to stay up-to-date with HIPAA regulations. The provider becomes an extension of the IT team and acts as a trusted partner.



CONCLUSION

All organizations face a variety of challenges, regulatory entanglements, potential threats and problems. It is likely, present and future problems such as hacking, human errors, and technological glitches will occur. A company that is not is required to be HIPAA compliant and does not meet those standards faces consequences that range from poor reputation to fines and criminal charges.

You can avoid potential problems of non-compliance by managing risks and threats before they start. The best defense is a multi-tiered approach in becoming HIPAA compliant. All Covered Entities should constantly identify new risks and threats as both technology and privacy laws evolve. In an ever-changing environment, it has become necessary to partner with trusted vendors.

Partnering with DataBank, a data center colocation and managed hosting provider, maximizes the organization's IT and compliance knowledge and abilities without hiring more employees or security professionals. DataBank is a Business Associate that employs administrative, technical and physical associated with the Security rule of HIPAA.

DataBank's consultative, proactive service, and knowledgeable approach simplifies the process of staying up-to-date with HIPAA regulations and maintaining compliance without sacrificing your IT system performance.