CELEBRATING 29 YEARS OF EXCELLENCE

HIPAA Compliant IT Infrastructure Guide

HIPAA Audited

GDPR READY

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

HITECH Audited

atlantic.net

Secure Cloud Services
Managed & Compliant Infrastructure

888-618-DATA (3282)
sales@atlantic.net
www.atlantic.net

Table of Contents

This e-book looks at healthcare law and what organizations must do to maintain compliance.

Introduction

With healthcare IT growing, the need for federally compliant infrastructure to process and store the electronic protected health information (ePHI) that is protected by the Health insurance Portability and Accountability Act (HIPAA) is on the rise as well.

HIPAA infrastructure must meet evolving standards

HIPAA was passed in 1996 to allow United States citizens to keep their health insurance when they changed employment (the P in HIPAA, portability) while safeguarding their health records (the first A in HIPAA, accountability). Under the law, healthcare providers, plans, and data clearinghouses (called covered entities by HIPAA) were given guidelines they had to follow – in which case they would achieve HIPAA compliance and avoid violations. These covered entities were expected to sign contracts with all of their business associates (BAs), service providers that handled their patient information. The contracts themselves were called business associate agreements (BAAs).

HIPAA was updated in 2009 through the Health Information Technology for Economic and Clinical Health Act, or HITECH. HITECH was contained within the American Recovery and Reinvestment Act, or ARRA – the economic stimulus package enacted by the 111th US Congress and signed by President Obama in response to the Great Recession. This new law made several changes, most notably reflecting changes in technology and including the BAs in the types of organizations covered by the regulations (making those firms directly responsible for meeting federal stipulations).

The most critical aspect of HIPAA related to digital systems is the Security Rule[1]. Geared toward keeping unauthorized parties away from ePHI, this key HIPAA rule created standards that were to be used by healthcare organizations when gen-

erating, receiving, utilizing, or storing this highly confidential data. To protect this information (i.e., to be certain it is secure, has integrity, and is kept private), covered entities have to implement safeguards of three types: technical, administrative, and physical.

The regulations of HIPAA can be adapted to suit the specific situation. For example, the size of a business might impact what it includes its HIPAA-compliant infrastructure. Plus, since HIPAA does not mandate specific technologies – instead basing its expectations on the current industry standards – organizations must be aware that the law is dynamic and that keeping abreast of the changing nature of IT security is key to maintaining compliance.

It is also important to know that HIPAA extends beyond what is in the code or tools that are in place to protect servers, as noted by Kayla Matthews in *Data Center Journal*[2]. Staff training is necessary, as is continuing education on the topic. Plus, it is necessary to have various policies and procedures in place that apply to data protections, how they are supported, and steps to follow in the event of a breach.

Cost of HIPAA-compliant infrastructure

Complying with HIPAA – including servers and all other aspects – is unfortunately costly, as noted by Jen Stone of *Security Metrics*[3]. For medium and large HIPAA-regulated firms, costs include a risk analysis and management plan ($20,000+); remediation (variable); policy creation and training ($5000+); onsite audit ($40,000+); penetration testing ($5000+); and vulnerability scans ($800). As those figures indicate, the total bill is usually $50,000 or more for entities of this size.

Costs are not quite as extreme for small organizations. For those institutions, Stone estimated compliance at $4000 to $12,000, a figure that included a risk analysis and management plan ($2000); remediation

($1000 to $8000); and policy creation and training ($1000 to $2000). The total bill is approximately $4000-$12,000, per her estimate. Costs will vary based on the way that your organization handles ePHI.

Compliance goes beyond audits & contracts

Data centers have to meet strict security requirements in order to comply with HIPAA. The complexity of achieving the rules is simplified through *independent audits*[2] that determine whether HIPAA-compliance safeguards are implemented. Audits and consultation can to help validate the compliance of a system whether it is your own or that of a third-party hosting provider you are considering.

When looking at services for colocation or hosting, organizations need to sign business associates agreements; however, these contracts do not absolve them of the need to comply with the law beyond that relationship. Plus, due diligence must be performed when selecting a healthcare business associate. Beyond healthcare-specific audits, you can also check for compliance with the Statement on Standards for Attestation Engagements 18, aka SSAE 18 (formerly SSAE 16), a widely recognized way to audit systems developed by the American Institute of Certified Public Accountants. The adoption of *SSAE 18 certification*[4] in addition to a HIPAA compliance audit creates redundancy in third-party security evaluation of the infrastructure partner you choose.

HITECH mandates EDI for data transmission

Especially since HITECH and its focus on interoperability (among its other concerns), easy and rapid transfer of medical data between systems has been critical to regulators. The sending and receiving of ePHI is to occur according to *electronic data interchange (EDI) standards*[5].

The *EDI rule*[5], which uses a protocol

standard for data transmission as its basis, X12N EDI. The rule mandates that the protocol must be used in the vast majority of situations in which electronic data is sent. The rule contains guidelines for data transmission that severely control the manner in which data is sent between devices. The rule provides the various kinds of transactions for which HIPAA is relevant and advises the specific format that must be used for data transfer in that case. Instructions are included for electronic transactions such as coordination of benefits (COB); referrals and authorizations; eligibility verifications and responses; claims status and remittance advices (RA); and health care claims.

The reasoning behind the rule is to simplify the transmission of health data by reducing from the hundreds of possible ways in which healthcare data has been formatted to the one standard approach of EDI. the primary reason this approach is important is that it better enables the accessibility and portability of medical records and minimizes the amount of money that must be spent on administration to manage data transmission.

Checklist for HIPAA-compliant infrastructure & related needs

The step-by-step needs for infrastructural compliance can be organized within a HIPAA compliance checklist. This one, based on the one created by *AdviseTech*[6] and elaborated with the expertise of HIPAA engineers at *Atlantic.Net*[7], provides an overview of core concerns when setting up servers for a compliant healthcare environment:

Physical security before data access

- Limited-access premises and parking
- Limited-access building
- No signs designating where the data center is
- Attendant or security guard at the entryway
- Need for photo ID at entrance
- Procedure for signing in and out of the facility

Infrastructure facility and security: access privileges

- Access limited to the data center building
- Need for biometric access
- Access restriction signs
- Individual, distinct IDs for each staff member's access
- Procedure to give access and take it away
- Vendor and guest rule for accompaniment by a staff member
- Reconciling of access with staff

Infrastructure facility and security: access monitoring

- Real-time access tracking
- Ongoing digital door-access log
- Guest log written by hand
- Positioning of cameras at each cage, aisle, and door-access point

Infrastructure facility and security: data safeguarding

- Availability of shredder
- Locked and secure server and communication cabinets
- Secure network sockets and cables

Logical access controls

- Comprehensive delineation demarcating one client from the next, so that the setting is private
- Defined and distinct server roles
- Logging and access control applied to all infrastructure handling PHI
- Firewall implemented in between private and public server environments
- Management of production changes
- Program to manage problems or incidents
- Response plan for security events
- Risk management and mitigation process

Documented controls and policies

- Access controls/policy
- Firewalls and related policy
- Password management system and policy
- Antimalware solution and policy
- Data classification system and policy
- Encryption mechanisms and policy
- Retention system and policy
- Destruction system and policy

Firewall

- Firewall dedicated to each individual environment
- Total separation from other clients
- Redundant firewalls
- Point-to-point virtual private network (VPN)
- Triple DES (3DES) to apply the DES encryption algorithm three times per data block
- Multi-factor authentication (MFA)
- Remote access via SSL VPN
- Internet protocol security (IPsec) in tunnel mode
- Filters for ingress and egress

Network

- Internal zone for the private server
- Public services demilitarized

zone (DMZ; i.e., the part of the network that exposes the external-facing services to the Internet or other outside networks)
- Private virtual local area network (VLAN)

Preventing breaches

- Intrusion prevention strategies
- Intrusion detection system (IDS) to know right away when anyone gets in
- Distributed denial of service (DDoS) mitigation solution
- Web application firewalls (WAF) as applicable
- Secure sockets layer (SSL) offloading of intrusion detection system / intrusion prevention

Antimalware

- Enterprise-quality antivirus solution
- Reporting that is centralized
- Logging of aberrant processes
- Intrusion prevention

Business associate checklist

- Organization is willing to sign a BAA
- Encryption of data throughout environment
- Insurance that is sufficient for the setting
- Backups both locally and off-site
- Logging and management of vulnerabilities
- Presence of HIPAA policies for HR, training, and security incident response
- Compliant with Statement on Standards for Attestation Engagements 18 (SSAE 18, formerly SSAE 16) SOC 1 and 2
- Willing to be part of your HIPAA audits
- HIPAA-trained personnel, organization-wide
- Training in general understanding of IT security

Checklist for selecting a managed host

- Security patching
- 24/7 complete oversight
- Easy access to clear performance metrics
- Host assumes the responsibility to restore any dropped service, respond appropriately to alarms, and escalate any serious issues as appropriate
- Secure portal for submission and management of tickets
- Access controls based on roles
- Specific, dedicated person to help you make any adjustments to your HIPAA-compliant infrastructure
- Tech support available 24/7

Summarized steps for HIPAA-compliant infrastructure

If that checklist is a bit overwhelming, the basic summary of what you need to do for compliance is expressed in these nine key steps covered by Brandon Butler in *NetworkWorld*[8]:

- Put substantial and robust audit controls into place.
- Use your audit logs to assess the activity within your system.
- Deploy access management and identity controls, logging everyone who accesses a system and sending out notifications to administrators whenever configurations are adjusted.
- Install a disaster recovery system, making certain that all information is backed up so that you are prepared for your contingency plan, which should incorporate emergency response procedures.
- Perform penetration testing, code scanning, and vulnerability scanning on all parts of your infrastructure that process or store electronic health data.
- Sign a well-written, fair, and thorough business associate agreement with each of your service providers, establishing key expectations of your relationship, including how

patients can get access to their records, what steps each of you are taking to ensure data security, and how each party should respond in the event of a breach.

- Control access by making certain that users are logged and unique. Make it possible to automatically log off users, have sophisticated authentication processes, and have groups that account for stateful security.
- Ensure that all PHI and other confidential data is encrypted by implementing a purpose-designed strategy to encrypt confidential data that is at rest and in motion.
- Secure transmissions through the use of object keys as possible, along with in-motion encryption via Advanced Encryption Standard 256 (AES 256; which is applicable to both SSL and transport layer security, or TLS).

Rules for Cloud Hosting

Organizations that must meet HIPAA regulations are increasingly concerned with how they can proceed in adoption of cloud services, one of which is cloud hosting or infrastructure as a service (IaaS). Note that the bulk of these rules apply to any third-party HIPAA hosting scenario.

The *"Guidance on HIPAA & Cloud Computing"*[9] document from the *Department of Health & Human Services (HHS)* notes that the most important concerns for covered entities and business associates are the Privacy, Security, and Breach Notification Rules. As the guidelines indicate, these rules together protect patient health data through restrictions on its disclosure and use, safeguards to protect against disclosure and use that is not permitted, and the rights of individuals related to their ePHI. These rules should be pivotal in determining strategy for HIPAA-compliant IT infrastructure.

The cloud parameters clarify that the establishment of a relationship between a HIPAA covered entity and IaaS provider that handles any electronic health data makes the cloud host a business associate. In turn, when a business associate signs up

with an IaaS provider to process, store, or otherwise handle its electronic PHI, the cloud provider again becomes a business associate.

The cloud host is a BA in these cases, even if it is only in contact with health records that are encrypted and for which the service does not possess a key. Since a business associate relationship is created, a business associate agreement must be signed between the cloud provider and HIPAA-regulated firm that is using its services. The cloud host, in these cases, must meet the demands of the BAA and also has to meet direct compliance with the relevant HIPAA specifications.

The business associate agreement is critical in defining how the cloud service will perform. The BAA should include language that sets forth allowed and necessary ePHI uses and disclosures. The uses and disclosures will be a bit different depending on the nature of the relationship and services being performed. The BAA should also stipulate that the BA must protect the data that it is handling, a main crux of which is the tenets of the Security Rule.

The *HIPAA Security Rule*[1], as a refresher, created standards to safeguard electronic protected health information. The Security Rule is concerned with the security, integrity, and privacy of digital information, as can be achieved through certain technical, physical, and administrative safeguards. There are various tools and resources provided by the HHS that pertain to the Security Rule:

- *HIPAA Security Risk Assessment Tool*[10]
- *NIST HSR Toolkit*[11]
- *Risk Analysis Guidance*[12]

Note that many organizations look for exceptions to the HIPAA law, hoping it might not apply to them. With cloud hosts, the desire is that they might fit the definition of a conduit for ePHI, as is true of the US postal service. It is unlikely that an IaaS provider will meet that same

definition. The only way it does is if the service is transmission-only, with any storage that does occur being temporary and incident to the transmission.

Not knowing about the cloud environment, or any third-party infrastructure provider, is not compliance. A healthcare organization or one of its business partners that handles ePHI on its behalf must gather knowledge about the cloud system and setting so that they can perform a relevant risk analysis and, in turn, create the right risk management policies and BAAs. In performing this assessment, the HIPAA-regulated organization must name and analyze the environment for any weaknesses or risks that might undermine the ePHI so that it becomes unavailable, corrupted, or accessible to unauthorized parties.

This process should encompass health records at all levels – during their production, receipt, storage, and transmission. To be clear, the BAA will be crafted, in part, based on the risk analysis that is conducted and risk management plan that is created, which in turn are based on the particular configuration of cloud (public, private, or hybrid), among other factors.

The relationship between your firm and an IaaS provider should also be governed by a service level agreement (SLA). These documents establish what you expect of your relationship with the provider that is less technical and more business-related. These concerns are also often necessary components of HIPAA compliance, as with these common topics:

- commitments on the reliability and availability of the solution
- the nature of data recovery and backup systems, which would (in part) allow the cloud host to immediately recover from a disaster or cybercriminal attack
- the process through which any HIPAA-protected information is sent back to the client if they decide to end their use of the service

assignment of responsibility to cer-

tain parties for elements of security

- any pertinent limitations related to disclosing, retaining, or using the ePHI.

One other specific thing to check is that neither the SLA or the BAA prevents you from being able to get to your data at any point.

You will need a BAA with the cloud host even for situations in which the data is encrypted and they do not have a key. While encryption is critical to ePHI protection, other parameters of HIPAA must be addressed as well (such as availability, protection from corruption, and administrative protocols). A cloud host must find and appropriately respond to any security events that it thinks or knows might have occurred. They also must minimize any damage that occurs as a result of the breach or incident. The IaaS provider should also let the client whose information was compromised know what has happened. The cloud host needs to have policies and procedures documents that cover the actions that must be taken and that log any security events that take place. The procedures should include contacting the impacted customer.

Looking at your own infrastructure to understand cloud needs

A report by Brian Taylor in *TechRepublic*[13] noted that being aware of risks within your own on-site infrastructure will give you a better sense of your vulnerabilities in cloud. That's because signing on with a cloud host will not reduce the need for you to meet general compliance parameters (which extend beyond your relationships with infrastructure providers).

Conducting a HIPAA risk assessment and carefully reviewing your agreements with cloud hosts will give you an idea of where you have weaknesses, clarifying what you need in a provider to prevent any gaps in compliance.

Infrastructural expertise to avoid HIPAA violations

For healthcare organizations and service providers that handle electronic PHI, knowing that your infrastructure meets the needs set forth by the Department of Health and Human Services is essential. Evaluating your own infrastructure can be extraordinarily costly, time-consuming, and inconvenient. While working with an external infrastructure provider does not mean that you are free from the many responsibilities of HIPAA, a carefully selected partner and well-constructed BAA can protect you both from data breaches and from liability.

Get Help with HIPAA Compliance

HIPAA Compliant Hosting by Atlantic.Net is SOC 2 & SOC 3 certified and HIPAA & HITECH audited, designed to secure and protect critical healthcare data and records. Get a free consultation today! Call 888-618-3282 or review our solutions at https://www.atlantic.net/hi-paa-compliant-hosting/.

References

[1] *https://www.hhs.gov/hipaa/for-professionals/security/index.html*

[2] *http://www.datacenterjournal.com/health-care-hipaa-data-centers/*

[3] *http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html*

[4] *https://www.atlantic.net/why-atlantic-net/security-and-compliance/*

[5] *https://www.asha.org/practice/reimbursement/hipaa/hipaa_edi_faq/*

[6] *https://advisetech.com/wp-content/uploads/2017/07/HIPAA-Compliance-Checklist-2.pdf*

[7] *https://www.atlantic.net/hipaa-compliant-hosting/*

[8] *https://www.networkworld.com/article/3121967/cloud-computing/9-keys-to-having-a-hipaa-compliant-cloud.html*

[9] *https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html*

[10] *https://www.healthit.gov/providers-professionals/security-risk-assessment-tool*

[11] *http://scap.nist.gov/hipaa/*

[12] *https://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html?language=es*

[13] *https://www.techrepublic.com/*