Clearwater

Whitepaper

Complying with HIPAA in an Amazon Web Services Environment

Table of Contents

Introduction

Across many industries, the last four years have shown a dramatic increase in cloud adoption and cloud usage, including a rapid acceleration into cloud services. In particular, we've seen this trend manifest itself throughout healthcare.

In late 2021, Gartner estimated that global cloud revenue would likely reach $474 billion in 2022, up from $408 billion the previous year. That same report estimates that more than 85% of organizations will embrace a cloud-first principle by 2025.

For healthcare specifically, the Healthcare Cloud Computing – Global Market Trajectory & Analytics report estimates that the industry's global cloud computing market is expected to reach almost $77 billion by 2026.

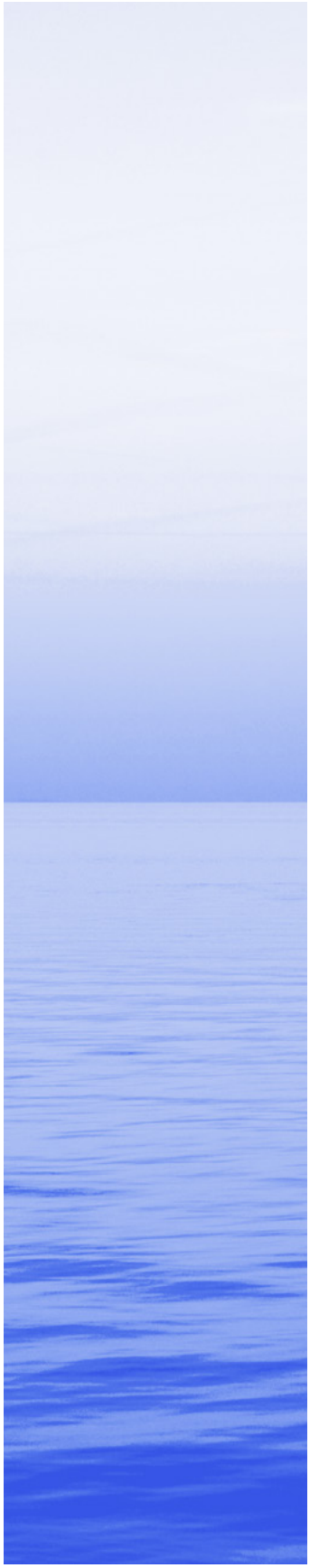
AWS cloud

As of the third quarter of 2021, the most popular vendor in cloud infrastructure services was Amazon Web Services (AWS), controlling about 32 percent of the market.

We have seen many health IT and digital health companies developing their solutions on AWS, both start-up and existing. They are making this choice because of the power of functionality provided and the perceived cost savings.

Many of these organizations are developing solutions that will be used to create, receive, maintain or transmit electronic protected health information (ePHI) on behalf of covered entity (CE) healthcare customers. When this happens, the organizations become "business associates" (BA). They are required to comply with the Health Insurance Portability and Accountability Act (HIPAA), including the need to execute a business associate agreement with their customers, furthering their contractual requirements to comply.

Often these organizations don't know where to start regarding HIPAA compliance. Clearwater will often receive requests for "the list of controls I need to implement to comply" or similar requests for a standard compliance strategy. Unfortunately, HIPAA compliance is not as straightforward as implementing a well-defined set of controls.



According to Gartner, more than 85% of organizations will embrace a cloud-first principle by 2025.

HIPAA security rule

The Security Rule requires covered entities and business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. This applies to covered entities using the cloud, although the cloud provider is responsible for some of these safeguards as a business associate.

Specifically, entities must:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce. Fortunately, the HIPAA Security Rule does go a bit further in defining the required administrative, technical, and physical controls:

Administrative safeguards

- **Security management process**. An entity must identify and analyze potential risks to ePHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security personnel.** An entity must designate a security official responsible for developing and implementing its security policies and procedures.
- **Contingency planning.** An entity must create and maintain a Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan.

- **Evaluation.** An entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.
- **Business associate contracts.** An entity must enter into and maintain business associate agreements as required. Physical Safeguards
- **Workstation and device security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media to ensure appropriate protection of electronic protected health information (ePHI).
- **Device and media controls.** An entity should implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility. Technical Safeguards
- **Access control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (ePHI).
- **Audit controls.** A covered entity must implement hardware, software, and/ or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI.
- **Person or entity authentication.** An entity should implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- **Maintain policy and procedures.** An entity should maintain/retain policy and procedures for six years from creation or the last effective day.

Entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications listed above must be implemented. In contrast, the "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not deemed reasonable and appropriate, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard if the alternative measure is considered reasonable and appropriate.

Addressable standards include:

Administrative safeguards

- **Workforce security.** Creating policy and procedures around the authorization and supervision of staff, workforce clearance, and termination procedures. Information Access Management. Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient's role (role-based access).
- **Workforce training and management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI. A covered entity must train all workforce members regarding its security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- **Contingency plan.** An entity should regularly test and revise data backup, disaster recovery, and emergency mode operation plans and procedures.

Physical safeguards

- **Facility access and control.** An entity must limit physical access to its facilities while ensuring that authorized access is allowed.
- **Device and media controls.** An entity should maintain a record of movements of hardware and electronic media and any person responsible therefore. An entity should also create an exact copy of ePHI, when needed, before the movement of equipment.

Technical safeguards

- **Access controls.** An entity should implement and enforce automatic logoff procedures and should implement controls to encrypt and decrypt ePHI.
- **Integrity controls.** A covered entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that ePHI has not been improperly altered or destroyed.
- **Transmission security.** A covered entity must implement technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network.

HIPAA in the cloud and AWS specific requirements

In addition to the HIPAA Security Rule requirements described above, organizations utilizing AWS must also comply with AWS requirements. Like a health IT or digital health company is asked by its customers to sign a Business Associate Agreement (BAA), an organization building on AWS that will create, receive, maintain, or transmit ePHI within its Cloud environment should enter into a BAA with AWS. AWS provides a standard BAA for this purpose, describing to an extent the shared security responsibility and expectations for the parties.

Processing electronic Protected Health Information (ePHI) on AWS requires the same security standards as processing ePHI in an on-premises data center. But when using AWS, a shared responsibility model applies where AWS is responsible for some of the security controls (like physical controls), and the cloud customer is responsible for other security controls (like configuring user accounts).

Department of Health and Human Services guidance states that all business associates of covered entities should, at a minimum, enter into a business associate agreement with their cloud service provider (CSP). It is worth noting that doing so will require "the business associate to appropriately safeguard the ePHI, including implementing the requirements of the Security Rule". Moreover, those parties "must conduct risk analyses to identify and assess potential threats and vulnerabilities to the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit."

HHS further notes that a Service Level Agreement (SLA) is "commonly used to address more specific business expectations between the CSP and its customer, which also may be relevant to HIPAA compliance." There are some unique aspects to this when considering a relationship with AWS, addressed below.

Creating a business associate relationship with AWS

AWS has some stipulations regarding how it can be used to process ePHI and be HIPAA compliant, but AWS provides flexibility on how a solution can be architected. To process ePHI on AWS, AWS requires the customer to enable the AWS Business Associate Addendum. This makes AWS a business associate for the customer account. The customer remains the covered entity, with AWS as a business associate. The covered entity is ultimately responsible for the protection of ePHI. It must obtain "satisfactory assurances" that a business associate will properly protect the ePHI they have in accordance with HIPAA. AWS provides documentation of third-party evaluations that they are taking proper security measures. Although AWS is a large cloud provider with several customers and third-party reviews, it is ultimately the covered entity's

responsibility to protect ePHI and obtain "satisfactory assurances" that every business associate (including AWS) is protecting ePHI they have.

Five stipulations from AWS

The stipulations that AWS has for processing ePHI on the AWS are:

1. All ePHI data must be encrypted at rest
2. All ePHI data must be encrypted in transit
3. The highest level of auditing for HIPAA services in AWS must be used
4. The maximum retention of logs for HIPAA services in AWS must be used
5. Only HIPAA-eligible AWS services can be used

Flexibility in solutions

Other than the five stipulations listed above, AWS has no additional requirements on how a solution must be architected or developed for processing ePHI. The HIPAA Security Rule still applies, and controls must be put in place, but AWS doesn't add additional requirements. AWS also provides templates for setting up compliant architectures and a reference architecture that can be used as a model for architecting a solution.

Summing up

The HIPAA Security Rule uses the standard that "reasonable and appropriate" security measures are put in place to protect ePHI. Certain baseline administrative, physical, and technical safeguards are required, and others are addressable. An entity must implement the required safeguards and have a good reason for not implementing the addressable requirements. The Security Rule doesn't prescribe how that is to be done. HHS states that they encourage "covered entities and business associates seeking information about types of cloud computing services and technical arrangement options to consult a resource offered by the National Institute of Standards and Technology; SP 800-145". Additionally, common security control frameworks are frequently used in assessment and analysis, like NIST 800- 53.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact