HIPAA Security Rule on AWS

Technical safeguards implementation and readiness guidance

July 2026

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Amazon Web Services (AWS) product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind.

This guide is provided by AWS Security Assurance Services, LLC (“AWS SAS”), a Payment Card Industry Qualified Security Assessor Company (PCI-QSAC) and HITRUST External Assessor Firm. AWS SAS is a wholly owned subsidiary of Amazon Web Services, Inc. The information contained in this document is provided solely for informational and guidance purposes and shall not constitute legal, regulatory, or compliance advice. Recipients are solely responsible for determining the applicability of this guidance to their specific environments, business operations, and applicable legal obligations. Nothing in this document shall be construed to create any legal obligation, representation, warranty, or guarantee on the part of AWS SAS, Amazon Web Services, Inc., or their respective affiliates, officers, employees, or agents. This document does not establish a client relationship and should not be relied upon as a substitute for consultation with qualified legal counsel, independent compliance professionals, or certified assessors with knowledge of the recipient’s specific circumstances.

Contents

Abstract

This guide helps organizations understand and address HIPAA Security Rule Technical Safeguard requirements (§164.312) using AWS services. It provides practical guidance for scoping ePHI boundaries, implementing access controls, encryption, audit logging, integrity mechanisms, and transmission security in AWS environments.

The guide references AWS governance capabilities, including AWS Control Tower guardrails, service control policies (SCPs), HIPAA AWS Config conformance packs, AWS Security Hub, and Amazon Bedrock guardrails as examples of how organizations can operationalize and enforce Technical Safeguard controls. These capabilities are illustrative; the core service-level guidance applies regardless of whether an organization uses the Landing Zone Accelerator on AWS (LZA), AWS Control Tower, a manually configured environment, or third-party governance tooling.

Although using AWS services doesn't automatically guarantee compliance, appropriate use of these services can materially reduce the technical complexity of addressing Technical Safeguard requirements.

Introduction

This guide identifies Amazon Web Services (AWS) services that organizations might consider when addressing the HIPAA Security Rule Technical Safeguard requirements under 45 CFR §164.312. For each specification, the guide describes the relevant AWS service or capability and provides pointers to AWS documentation for further reference. The guidance applies regardless of whether an organization uses the Landing Zone Accelerator on AWS (LZA), AWS Control Tower, a manually configured environment.

This guide doesn't provide detailed configuration instructions, nor does it constitute legal or compliance advice. Ensuring that any AWS service is correctly configured, validated, and operated in a manner consistent with applicable HIPAA obligations remains the sole responsibility of the customer. Customers should consult qualified legal counsel, security, privacy, and compliance professionals, and AWS documentation when making decisions specific to their environment.

This guide focuses on the Technical Safeguards (§164.312) only. The HIPAA Security Rule's General Rules (§ 164.306), Administrative Safeguards (§164.308), Physical Safeguards (§164.310), Organizational Requirements (§164.314), and Policies and Procedures and Documentation Requirements (§164.316) are out of scope. Organizations subject to HIPAA are responsible for implementing all relevant safeguard categories as required by the Security Rule.

HIPAA regulatory framework and applicability

Overview of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), enacted by the United States Congress in 1996, establishes federal standards for protecting sensitive patient health information. HIPAA was primarily designed to ensure continuity of health insurance coverage during employment transitions, but it also authorized the establishment of standards governing the handling, protection, and disclosure of electronic health information (also referred to as electronic protected health information or ePHI) by healthcare organizations and their technology partners.

For organizations building or operating systems on AWS that interact with healthcare data, two HIPAA rules are directly relevant: the Privacy Rule and the Security Rule. The Privacy Rule (45 CFR Part 164, Subpart E) governs the permissible uses and disclosures of protected health information in any form. The Security Rule (45 CFR Part 164, Subpart C) governs the technical, administrative, and physical safeguards required to protect ePHI. This whitepaper focuses exclusively on the Security Rule and its Technical Safeguard requirements.

HIPAA applicability

HIPAA compliance obligations extend to two categories of organizations, defined by their relationship to protected health information.

Covered entities are organizations whose primary function directly involves the creation or use of PHI. As defined by HHS 45 CFR 160.163 (Covered Entities and Business Associates), the three categories of covered entities are:

- **Healthcare providers** – Hospitals, clinics, physicians, pharmacies, and other providers of healthcare, but only if they transmit health information electronically in connection with a HIPAA-covered transaction (such as electronically submitting claims to a health plan)
- **Health plans** – Health insurance companies, HMOs, employer-sponsored group health plans, and government programs such as Medicare and Medicaid
- **Healthcare clearinghouses** – Entities that translate healthcare data between non-standard and standard formats, such as billing processing services

Business associates (BAs) are organizations that create, receive, maintain, or transmit PHI on behalf of a covered entity in the course of providing a service regulated by HIPAA. Business associates are directly subject to the Security Rule and bear independent compliance obligations—not simply obligations delegated by the covered entity. Common examples of business associates in cloud environments include:

- Cloud infrastructure providers hosting healthcare applications that process ePHI
- Software as a service (SaaS) vendors offering electronic health record (EHR), billing, or clinical decision support systems
- Analytics and reporting platforms that process claims data or clinical outcomes data
- Managed security service providers monitoring systems that contain ePHI

The chain doesn't stop at business associates. Subcontractors that handle PHI on a BA's behalf are also considered business associates under HIPAA and face the same compliance requirements

Organizations building healthcare workloads on AWS typically act as either a covered entity—such as a hospital or health plan—or as a business associate This matters practically: you must sign a BAA with AWS, configure services to meet Security Rule requirements, and understand that you're independently liable to HHS if a breach occurs.

Protected health information and ePHI

Protected health information (PHI) is individually identifiable health information—any information that relates to an individual's past, present, or future physical or mental health condition; the provision of healthcare to that individual; or the past, present, or future payment for the provision of healthcare—where the information can be used to identify the individual. PHI might not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and might be limited to demographic or other information not indicative of the type of healthcare services provided to an individual. If the information is tied to a covered entity, then it is PHI by definition, because it's indicative that the individual received healthcare services or benefits from the covered entity.

Electronic protected health information (ePHI) is PHI that is created, stored, transmitted, or received in electronic form. The Security Rule applies specifically to ePHI.

The US Department of Health and Human Services (HHS) defines 18 categories of identifiers that can make health information individually identifiable—including names, dates, geographic data, contact details, Social Security numbers, medical record numbers, device identifiers, IP addresses, biometrics, and photographs. For the complete list published by HHS, see Methods for De-identification of PHI.

Data is considered de-identified—and no longer subject to HIPAA—only when all 18 identifiers have been removed (Safe Harbor method) or when a qualified statistician certifies that the risk of identifying an individual is very small (Expert Determination method). It's highly recommended that organizations should use de-identified or synthetically generated data in development, test, and sandbox environments. Real ePHI must not be used in non-production systems without the same safeguards applied in production.

Although the data is de-identified; the remaining information might still be sufficient to identify an individual when combined with other available data. Assess the risk of re-identification, minimize quasi-identifiers where appropriate, and prohibit attempts to re-identify individuals through technical, administrative, and contractual controls.

The Business Associate Agreement with AWS

A Business Associate Agreement (BAA) is a legally required contract between a covered entity (or business associate) and any organization that handles PHI on their behalf. The BAA defines the permitted uses and disclosures of PHI, establishes the BA's obligations to protect that PHI, and specifies the consequences of a breach, including notification obligations and liability allocation.

AWS offers a standard BAA to customers that covers a defined set of HIPAA-eligible AWS services. Customers accept the BAA through AWS Artifact on the AWS Management Console. Several operational requirements follow from accepting the BAA that architects and compliance teams must understand:

- For organizations using AWS Organizations, the AWS BAA can be accepted once by an authorized management account user to automatically cover existing and future member accounts within the organization. Individual per-account acceptance isn't required when using AWS Organizations. Organizations not using AWS Organizations must accept the AWS BAA in each individual account that processes, stores, or transmits ePHI. To learn more, see Accepting agreements for your organization in AWS Artifact.
- The AWS BAA covers AWS responsibilities—the security of the underlying cloud infrastructure, physical data centers, and managed service platforms. It doesn't certify that customer workloads running on those services are HIPAA compliant. Appropriate configuration, monitoring, and operation of AWS services within the customer's environment remains entirely the customer's responsibility.
- Not all AWS services are covered under the AWS BAA. Customers must verify that every AWS service processing ePHI appears on the current list of HIPAA-eligible services before deploying PHI workloads. For the current list, see HIPAA Eligible Services. Services not on this list must not be used to store, process, or transmit ePHI. By default, AWS services in preview or beta aren't considered HIPAA-eligible unless a separate BAA is established.

The three safeguard categories

The HIPAA Security Rule organizes its requirements into three safeguard categories. All three are required—a technically strong implementation doesn't compensate for deficiencies in administrative or physical safeguards, and vice versa. Assessors evaluate all three categories, as detailed in the following table.

Safeguard category	CFR reference	Scope
Administrative Safeguards	§164.308	Security management process, risk analysis, workforce training, contingency planning, business associate oversight, information access management

Safeguard category	CFR reference	Scope
Physical Safeguards	§164.310	Facility access controls, workstation use and security, device and media controls
Technical Safeguards	§164.312	Access control, audit controls, integrity mechanisms, person or entity authentication, transmission security

This whitepaper addresses Technical Safeguards only. However, the Technical Safeguards can’t be properly scoped without first completing the risk analysis required by the Administrative Safeguards (§164.308(a)(1))—the risk analysis determines which controls are reasonable and appropriate for the organization, which is the foundation of every implementation decision in this guide.

Implementation obligation

The Security Rule designates each implementation specification as either Required or Addressable. The 2025 Notice of Proposed Rulemaking (NPRM) proposes to make all Technical Safeguard specifications required, eliminating the Addressable designation.

Required specifications must be implemented as described with no flexibility on whether to implement—only on how, to the extent the rule allows.

Addressable specifications aren't optional. If a control is reasonable and appropriate for your environment, implement it. If it genuinely isn't, document why and implement an equivalent control that achieves the same security outcome

The NPRM changes this picture significantly. HHS published a Notice of Proposed Rulemaking in January 2025 that proposes eliminating the Addressable designation—encryption at rest and encryption in transit would both become Required. Although the final rule has not yet been published, the direction is clear, and the risk environment already supports treating all specifications as Required. Additionally, many of these controls are either enforced or directly supported by AWS through the AWS BAA and built-in service capabilities.

Understanding the HIPAA security rule

The HIPAA Security Rule (45 CFR §164.302–§164.318) establishes national standards for protecting ePHI. The rule requires covered entities and business associates to implement safeguards that ensure the confidentiality, integrity, and availability of ePHI.

Technical Safeguards overview

The Technical Safeguards (§164.312) contain five standards and nine implementation specifications. The following table reflects the current rule designations. Under the proposed 2025 NPRM, specifications currently marked Addressable would become Required—implement all as Required for new workloads.

The standard is distinct from its implementation specifications. Compliance with individual implementation specifications doesn't, by itself, ensure compliance with the standard.

Standard	Specification	Current type	NPRM proposed
Access control §164.312(a)(1)	(See below)	Required	Required
	Unique user identification	Required	Required
	Emergency access procedure	Required	Required
	Automatic logoff	Addressable	Required
	Encryption and decryption	Addressable	Required
Audit controls §164.312(b)	(No sub-specifications)	Required	Required
Integrity §164.312(c)(1)	(See below)	Required	Required
	Mechanism to authenticate ePHI	Addressable	Required
Person or entity authentication §164.312(d)	(No sub-specifications)	Required	Required

Standard	Specification	Current type	NPRM proposed
Transmission security §164.312(e)(1)	(See below)	Required	Required
	Integrity controls	Addressable	Required
	Encryption	Addressable	Required

Important note: Pending HIPAA Security Rule updates (NPRM 2025)

Action is required for organizations planning new AWS healthcare workloads.

On January 6, 2025, the Office for Civil Rights (OCR) published a Notice of Proposed Rulemaking (NPRM) in the Federal Register proposing significant updates to the HIPAA Security Rule. As of June 2026, this remains a proposed rule—it has not been finalized. The public comment period closed March 7, 2025.

Organizations building new workloads or modernizing existing environments should be aware of the key proposed changes, as they signal the direction of potential future requirements. The following table summarizes these proposed changes.

Proposed change	Current rule	NPRM
Encryption at rest and in transit	Addressable	Required (with limited exceptions)
Multi-factor authentication	Addressable	Required for all ePHI access (with limited exceptions)
Technology asset inventory	Not explicitly required	Required—documented, current inventory
Vulnerability scanning	Addressable	Required—defined frequency
Penetration testing	Not explicitly required	Required—annual
Recovery time objective	Not explicitly required	Required—72-hour RTO for critical systems

Proposed change	Current rule	NPRM
Business associate verification	BAA required	Required—annual written verification of BA safeguards
Required vs. Addressable distinction	Mixed	All addressable specifications become Required
Network segmentation	Not explicitly required	Required—documented architecture limiting lateral movement; close or disable unused ports and services
Anti-malware protection	Addressable (training item only)	Required—mandatory deployment on all relevant systems; removal of unnecessary software
Patch management	Implied in maintenance provisions	Required—15 calendar days for critical-risk, 30 days for high-risk; documented exceptions required
Configuration management	Not explicitly required	Required—technical controls enforcing baseline configurations on all electronic information systems

The guidance in this document is designed to align with both the current rule and the direction of the proposed changes. Implementing encryption, multi-factor authentication (MFA), and asset inventory as Required rather than Addressable is strongly recommended for organizations building new workloads today.

The AWS BAA, available through AWS Artifact, contains obligations that might independently require certain security controls as a condition of the agreement. Organizations should review the current BAA text to understand which controls are contractually required in addition to any regulatory obligations under the Security Rule.

For the current status of the NPRM, refer to Regulatory Initiatives.

AWS Shared Responsibility Model for HIPAA

Understanding the AWS Shared Responsibility Model is the foundation for correctly scoping your HIPAA compliance program. AWS and the customer each own a distinct set of controls.

The following figure lists the responsibilities of the HIPAA Technical Safeguards Shared Responsibility Model. The matrix maps each §164.312 Technical Safeguard to two responsibility layers. Dark blue (top) shows what the customer must configure and operate. Orange (bottom) shows what AWS operates as part of its security of the cloud commitment. Both layers are required—AWS providing the capability doesn't satisfy the requirement; the customer must enable and enforce it. Rows marked NPRM Proposed are not yet enforceable under the current Security Rule.

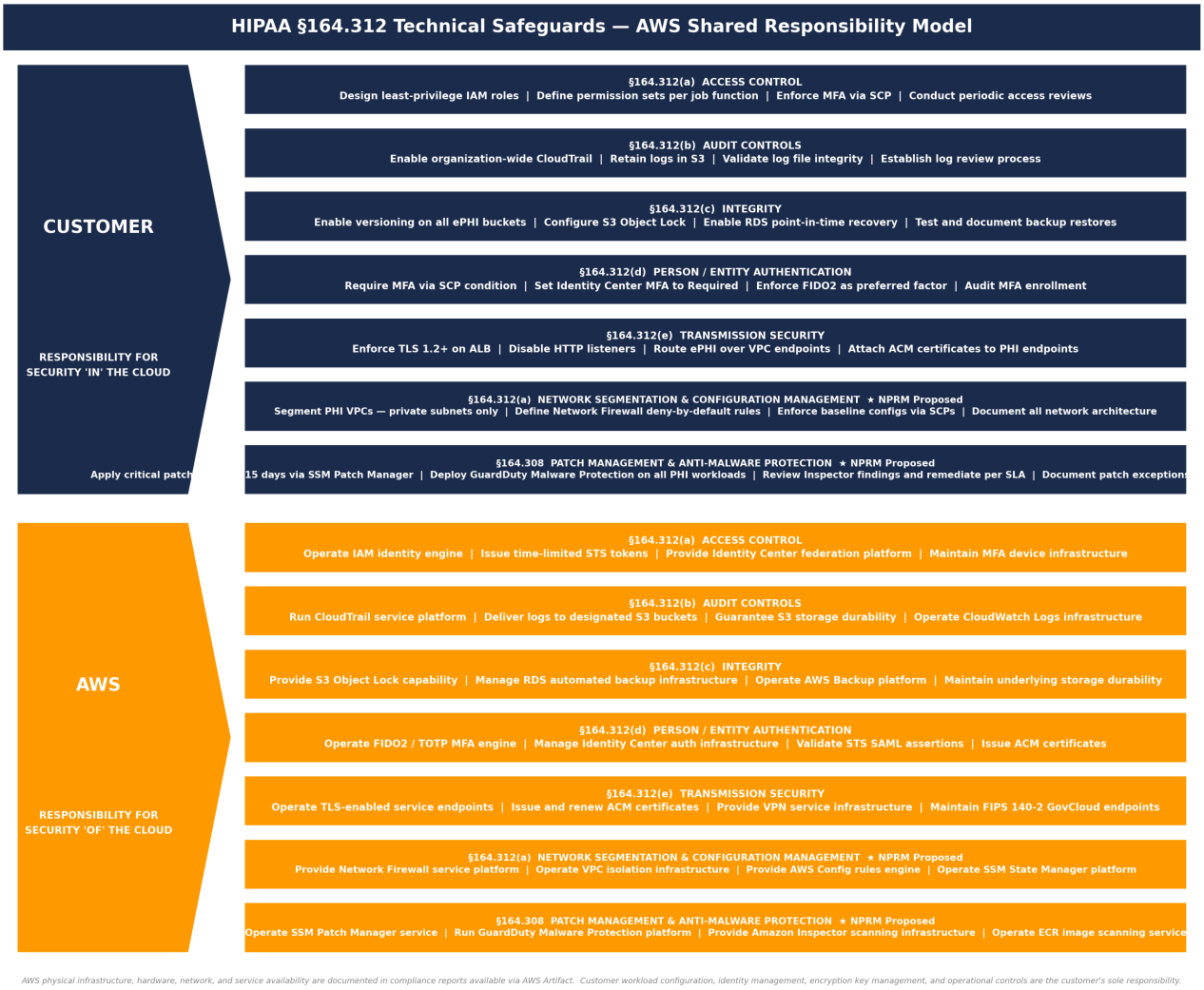

Figure 1: HIPAA Technical Safeguards Shared Responsibility Matrix

What AWS manages

AWS maintains responsibility for protecting the infrastructure that runs AWS Cloud services—the hardware, software, networking, and facilities. This includes physical data center security, hardware and network infrastructure, virtualization infrastructure, and global network security. These controls are documented in AWS compliance reports available through AWS Artifact.

What the customer manages

The preceding figure maps customer and AWS responsibilities to each §164.312 Technical Safeguard specification. At a high level, customer responsibilities for HIPAA workloads on AWS include:

- Conduct and document a risk analysis covering all AWS hosted ePHI systems, which determines which technical controls are reasonable and appropriate for your environment
- ePHI boundary definition and data classification
- Identity and access management configuration (roles, policies, MFA enforcement)
- Encryption configuration at rest and in transit
- Audit log configuration, retention period, and review
- Network and firewall configuration
- Application-level access controls
- Connected devices including desktop and laptop computers, mobile phones, medical devices, industrial equipment
- The AWS BAA doesn't cover third-party software or desktop applications; customers are responsible for securing endpoint devices and applications that connect to HIPAA-eligible AWS services, including implementing appropriate endpoint security controls to protect ePHI
- Signing the AWS BAA through AWS Artifact in each in-scope account or AWS Organizations level account

Later in this document, we provide implementation details for each §164.312 specification. The services used to implement these controls are HIPAA-eligible and covered under the AWS BAA. Refer to HIPAA Eligible Services for the current list.

Establishing an ePHI boundary on AWS: Landing Zone architecture

The Landing Zone Accelerator on AWS (LZA) provides a prescriptive multi-account architecture that organizations might use as a foundation for establishing an ePHI boundary on AWS. The LZA automates

the deployment of a secure, scalable account structure aligned with AWS Security Best Practices and supports HIPAA-eligible service configurations.

The ePHI boundary is defined by the set of accounts where ePHI is permitted to reside or transit. All accounts within this boundary require a signed BAA with AWS.

The following figure illustrates the recommended organizational unit (OU) structure for a HIPAA-aligned LZA deployment. The orange dashed boundary identifies the OUs and accounts where ePHI might reside. AWS services listed within the ePHI boundary that process ePHI are HIPAA-eligible and covered under the AWS BAA. For the authoritative list of eligible services, see HIPAA Eligible Services.

Implementation details for each Technical Safeguard specification are provided later in this document.

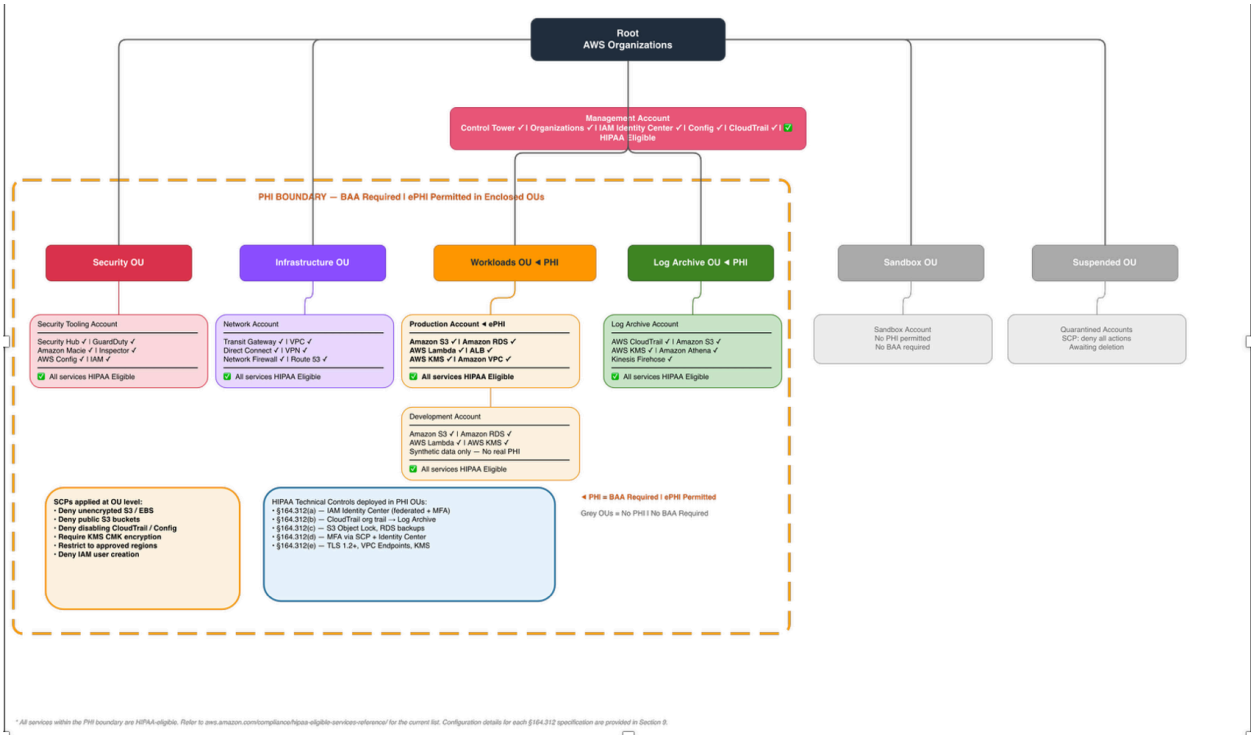

Figure 2: Landing Zone Accelerator on AWS, recommended OU structure for HIPAA workloads

The preceding figure shows the AWS Organizations hierarchy deployed by the LZA. The orange dashed boundary identifies the ePHI boundary—accounts within this boundary might process, store, or transmit ePHI and require a signed BAA with AWS. The Management account hosts Control Tower, AWS Organizations, AWS IAM Identity Center, and AWS Config. The Security OU contains the Security Tooling account running AWS Security Hub, Amazon GuardDuty, Amazon Macie, and Amazon Inspector for centralized threat detection and compliance monitoring. The Infrastructure OU contains the Network

account managing AWS Transit Gateway, virtual private cloud (VPC) connectivity, and AWS Network Firewall. The Workloads OU contains the Production account—primary ePHI storage and processing using Amazon Simple Storage Services (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Lambda, and AWS Key Management Service (AWS KMS)—and the Development account (synthetic data only, no real ePHI). The Log Archive OU contains the Log Archive account, which receives the AWS CloudTrail organization trail and enforces immutable log retention using Amazon S3 Object Lock. The Sandbox and Suspended OUs sit outside the ePHI boundary and don't require a BAA. Service control policies (SCPs) applied at the OU level enforce encryption, prevent disabling of audit controls, and restrict deployment to approved AWS Regions.

ePHI data flow and encryption at each layer

The previous section established the account and OU structure used to define the ePHI boundary. Before configuring the individual Technical Safeguard controls described later in this document, it's useful to understand how ePHI flows through that architecture—and which §164.312 specification applies at each point in the flow.

The specific services, entry points, and data stores that process ePHI will vary by customer workload. An organization running a patient portal will have a different flow than one processing clinical images or exchanging HL7 messages with a third-party EHR. Customers are responsible for mapping their own ePHI flows and identifying every point where ePHI is stored, processed, or transmitted. The following diagram illustrates a representative reference architecture—a web-tier workload with Amazon RDS and Amazon S3 storage—to show how the §164.312 specifications map to AWS services at each layer. Customers should use this as a starting point and adapt it to reflect their specific workload topology.

The numbered arrows in the diagram trace the ePHI path through each AWS service layer, with the applicable §164.312 specification annotated at each step. Later in this document, we provide the implementation details for each specification shown.

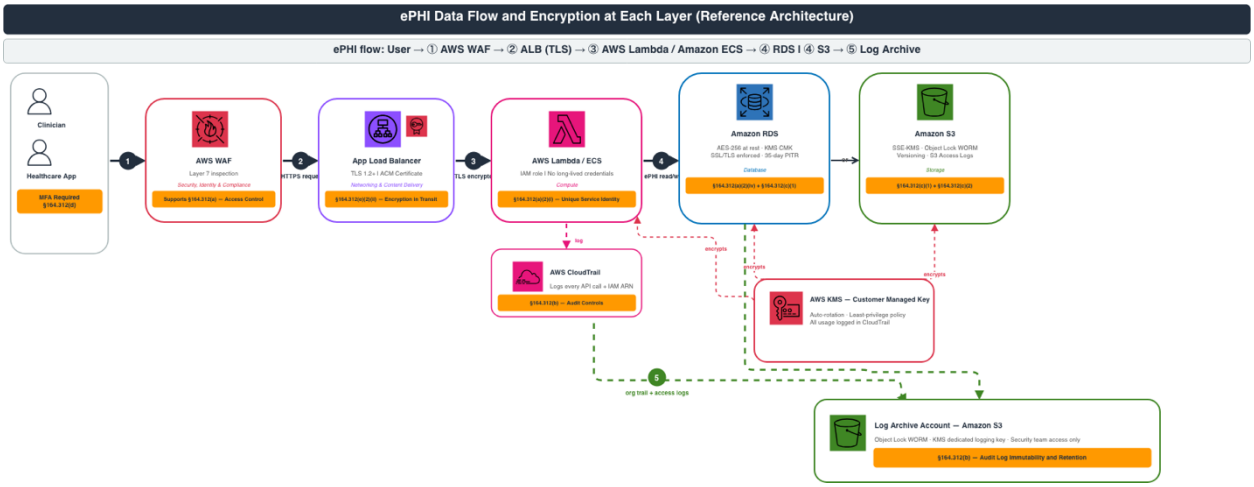

Figure 3: A reference architecture for a web-tier workload. The actual ePHI flow will vary by workload. Customers are responsible for mapping and documenting their own data flows.

The numbered arrows in the preceding diagram trace the ePHI flow through each AWS service layer. The §164.312 specification applicable at each step is noted in parentheses.

1. An authenticated user sends an HTTPS request. MFA is enforced at sign-in using IAM Identity Center (§164.312(d)).
2. AWS WAF inspects the request at Layer 7, then the Application Load Balancer (ALB) terminates TLS 1.2+ using an AWS Certificate Manager (ACM) certificate. No unencrypted path to ePHI exists (§164.312(e)(2)(ii)).
3. The compute layer—Lambda or Amazon Elastic Container Service (Amazon ECS)—processes ePHI using a least-privilege AWS Identity and Access Management (IAM) execution role. CloudTrail logs every API call with the caller's identity (§164.312(a)(2)(i), §164.312(b)).
4. ePHI is written to or read from encrypted storage—Amazon RDS (AES-256, KMS CMK, SSL enforced, PITR) or Amazon S3 (SSE-KMS, S3 Object Lock, S3 Versioning). AWS KMS manages encryption keys with automatic annual rotation (§164.312(a)(2)(iv), §164.312(c)(1), §164.312(c)(2)).
5. CloudTrail logs and S3 access logs flow to the Log Archive account, where S3 Object Lock enforces log retention tamper-resistant retention period (§164.312(b)).

It's highly recommended that PHI or PII must not appear in resource names or metadata. Although encryption protects ePHI at rest and in transit, it doesn't protect identifiers stored in resource names, tags, object keys, instance identifiers, log group names, or similar metadata. These values might appear in logs, billing reports, Amazon Resource Names (ARNs), IAM policies, the AWS Management Console,

and other operational records. Use non-identifying naming conventions and never include HIPAA identifiers in resource names or metadata.

Foundation requirements before implementing technical controls

With the ePHI boundary architecture understood and the ePHI data flow mapped, the following checklist confirms the foundational steps are in place before configuring individual Technical Safeguard controls. These are prerequisites—skipping them creates gaps that no technical control can close.

#	Action	Owner	Why it matters
1	Accept the AWS BAA in every in-scope AWS account or at AWS Organizations level using AWS Artifact	CISO and Cloud Team	Legal requirement—ePHI can't be processed without a signed BAA
2	Conduct and document a HIPAA risk analysis	CISO and Compliance	Determines which controls are "reasonable and appropriate" for your environment
3	Confirm PHI boundary definition—accounts, OUs, services, and data flows in scope	Cloud Architect	Scopes downstream control decisions
4	Deploy the HIPAA Conformance Pack in AWS Config across in-scope accounts	Cloud and Security Team	Baseline continuous compliance evaluation
5	Enable AWS CloudTrail organization trail with data events	Cloud and Security Team	Required for §164.312(b) Audit Controls
6	Enable AWS Security Hub with NIST 800-53 Rev. 5 standard	Security Team	Consolidated posture management and prioritized findings
7	Designate a named HIPAA Security Officer	Leadership	Required by Administrative Safeguards (§164.308(a)(2))

#	Action	Owner	Why it matters
8	Ensure PHI is only processed on HIPAA-eligible AWS services	Cloud Architect	Non-eligible services are outside the BAA scope

For the current list of HIPAA-eligible AWS services, refer to HIPAA Eligible Services.

Implementation of Technical Safeguard controls

The following sections address a specific Technical Safeguard specification for customers to implement as guidance. The pattern for each section is: control requirement, implementation approach on AWS, and the evidence an assessor would expect to see.

§164.312 Technical Safeguards: Complete framework reference

The following table reflects the authoritative structure of 45 CFR §164.312 as published by HHS. All five standards and nine implementation specifications are addressed in this section. (Source: ecfr.gov—45 CFR §164.312.)

Standard	CFR reference	Implementation specification	Type	NPRM 2025 proposed	Primary AWS services
Access control	§164.312(a)(1)	Access control	Required	Required	AWS IAM Identity Center, SCPs, IAM
	§164.312(a)(2)(i)	Unique user identification	Required	Required	AWS IAM Identity Center, AWS CloudTrail
	§164.312(a)(2)(ii)	Emergency access procedure	Required	Required	IAM (break-glass role), AWS CloudTrail

Standard	CFR reference	Implementation specification	Type	NPRM 2025 proposed	Primary AWS services
	§164.312(a)(2)(iii)	Automatic logoff	Addressable	Required	IAM Identity Center session policy, Application Load Balancer
	§164.312(a)(2)(iv)	Encryption and decryption	Addressable	Required	AWS KMS, Amazon S3, Amazon EBS, Amazon RDS
Audit controls	§164.312(b)	Audit controls	Required	Required	AWS CloudTrail, Amazon CloudWatch, Amazon S3 Object Lock
Integrity	§164.312(c)(1)	Integrity	Required	Required	Amazon S3 Versioning, Amazon RDS PITR, AWS Backup
	§164.312(c)(2)	Mechanism to authenticate ePHI	Addressable	Required	AWS CloudTrail validation, Amazon S3 checksums
Person or entity authentication	§164.312(d)	Person or entity authentication	Required	Required	AWS IAM Identity Center, MFA, SCP
Transmission security	§164.312(e)(1)	Transmission security	Required	Required	VPC endpoints, VPN, TLS
	§164.312(e)(2)(i)	Integrity controls	Addressable	Required	Application Load Balancer TLS policy, Network Load Balancer TLS policy

Standard	CFR reference	Implementation specification	Type	NPRM 2025 proposed	Primary AWS services
	§164.312(e)(2)(ii)	Encryption in transit	Addressable	Required	AWS Certificate Manager, Application Load Balancer, Amazon RDS SSL, VPN, GovCloud FIPS
Network segmentation *(NPRM new)*	§164.312(a)(1)	Network segmentation	Not required	Required	AWS Network Firewall, VPC, AWS Transit Gateway, AWS security groups
Configuration management *(NPRM new)*	§164.312(c)	Configuration baseline	Not explicit	Required	AWS Config, AWS Systems Manager State Manager, SCPs, AWS Security Hub
Anti-malware protection *(NPRM new)*	§164.312(c)(2)(i)	Anti-malware protection	Not required	Required	Amazon Inspector, Amazon GuardDuty, AWS Security Hub
Software removal *(NPRM new)*	§164.312(c)(2)(ii)	Software removal	Not explicit	Required	AWS Systems Manager Inventory, AWS Config, AWS Systems Manager State Manager
Configuration *(NPRM new)*	§164.312(c)(2)(iii)	Configuration	Not explicit	Required	AWS Systems Manager State Manager, AWS Config

Standard	CFR reference	Implementation specification	Type	NPRM 2025 proposed	Primary AWS services
Network ports *(NPRM new)*	§164.312(c)(2)(iv)	Network ports	Not explicit	Required	AWS Network Firewall, AWS security groups, AWS Config
Maintenance *(NPRM new)*	§164.312(c)(2)(v)	Maintenance	Not explicit	Required	AWS Systems Manager Patch Manager, Amazon Inspector

Architectural Note:

The AWS services referenced throughout this section represent the implementation options available across the HIPAA-eligible service catalog. Which services apply to your environment depends entirely on your workload architecture. A clinical application running on Amazon ECS with Amazon RDS will have a different implementation pattern than a serverless API on Lambda with Amazon DynamoDB, or a data analytics pipeline on Amazon EMR with Amazon S3. The encryption, access control, audit, and transmission security controls are the same regulatory requirements—the specific AWS services and configurations that satisfy them differ by architecture.

Before working through each control, map your workload architecture to identify which compute, storage, database, networking, and application services are in scope for your PHI boundary. Every service that stores, processes, or transmits ePHI needs a control implementation for each applicable specification. Services that are in the PHI boundary but not covered by a control represent a gap.

The implementations described in this section use a reference architecture as an illustrative example, Amazon Elastic Compute Cloud (Amazon EC2) or Amazon ECS for compute, Amazon RDS or Amazon S3 for storage, ALB for ingress, AWS KMS for encryption, and IAM Identity Center for identity management. These specific services aren't required by HIPAA, the regulation specifies the security outcomes that must be achieved, not the technology used to achieve them.

IAM Identity Center, for example, is one way to implement unique user identification and MFA enforcement, but organizations might use IAM directly, a third-party identity provider (IdP), or other federated identity mechanisms to satisfy the same requirements. For serverless, container, or data analytics workloads, the same principles apply—substitute the appropriate service-specific controls for your architecture.

§164.312(a)(1): Access control

Requirement: Implement technical policies and procedures for information systems that maintain ePHI to allow access only to authorized persons or software programs.

Implementation on AWS:

Access control in a HIPAA-compliant AWS environment is built on three principles: no standing access for humans, unique identities per person and service, and enforcement through policy rather than convention.

Human access is federated through IAM Identity Center connected to the organization's IdP. No IAM user accounts with console access are created in PHI accounts—an SCP enforces this. Human access is time-bound (session credentials issued by STS) and scoped to the minimum permissions required for the user's role.

Service-to-service access uses IAM roles with resource-based policies. Long-lived access keys are prohibited through SCPs and monitored using AWS Config.

Examples of supporting documentation for audit readiness:

- IAM Identity Center configuration showing federation with external IdP
- SCP denying IAM user creation in PHI OUs
- IAM roles in PHI accounts showing least-privilege permission sets
- AWS Config rule `iam-policy-no-statements-with-admin-access` showing `COMPLIANT` status
- Access review records (quarterly minimum)

Technical references:

- AWS IAM Identity Center User Guide
- Security best practices in IAM
- Strategies for achieving least privilege at scale
- Implementing policies for least-privilege permissions for AWS CloudFormation: Next steps

§164.312(a)(2)(i): Unique user identification (Required)

Requirement: Assign a unique name and/or number for identifying and tracking user identity.

Implementation on AWS:

Every IAM identity—user, role, or service principal—receives a unique ARN and unique ID. CloudTrail records the specific IAM ARN (including the federated session name, which maps to the individual user from the IdP) for every API call. This creates an unambiguous, traceable record from API action to named individual. The covered entity is responsible for confirming that unique identities are assigned and enforced at the organizational level—meaning no shared accounts, no shared credentials, and no shared workstation logins where multiple individuals authenticate under the same identity. AWS can't enforce this. The organization must implement policies, training, and operational controls that prohibit shared identities and verify compliance through access reviews.

Examples of supporting documentation for audit readiness:

- Sample CloudTrail log entries showing `userIdentity.arn` and `userIdentity.sessionContext.sessionIssuer.userName` for federated access
- IAM Identity Center configuration showing unique user assignment (no shared accounts)
- Confirmation that shared IAM accounts don't exist in PHI accounts (AWS Config rule or SCP evidence)

Technical references:

- CloudTrail userIdentity element
- Logging IAM and AWS STS API calls with AWS CloudTrail

§164.312(a)(2)(ii): Emergency access procedure (Required)

Requirement: Establish and implement procedures for obtaining necessary ePHI during an emergency.

Implementation on AWS:

A break-glass role provides elevated access during declared emergencies. The role is dormant during normal operations—it has no trust policy allowing routine assumption. During an emergency, a defined dual-authorization process (two senior staff) unlocks the role by temporarily modifying the trust policy.

AWS Security Token Service (AWS STS) issues time-bound session credentials (maximum 1-hour session). CloudTrail logs the role assumption and every action performed under it.

Post-emergency review is a formal step in the incident response process—the CloudTrail records for the emergency session are reviewed within 24 hours.

Examples of supporting documentation for audit readiness:

- Break-glass role definition and documented dual-authorization procedure
- IAM trust policy showing the role isn't routinely assumable
- CloudTrail log of the most recent break-glass test (annual testing recommended)
- Post-emergency review record template

Technical references:

- Implement break-glass procedures

§164.312(a)(2)(iii): Automatic logoff (Addressable)

Requirement: Implement electronic procedures that terminate a session after a predetermined time of inactivity.

Implementation on AWS:

Session duration is enforced at multiple layers. IAM Identity Center session policies set a maximum duration for federated console sessions. Application-level sessions implement idle timeout logic. ALB idle timeout is configured to terminate inactive connections.

Examples of supporting documentation for audit readiness:

- IAM Identity Center session duration policy screenshot
- Application session timeout configuration documentation
- ALB idle timeout setting evidence

Technical references:

- Configure the session duration in IAM Identity Center

- Edit attributes for your Application Load Balancer

§164.312(a)(2)(iv): Encryption and decryption (Addressable)

Requirement: Implement a mechanism to encrypt and decrypt ePHI.

Implementation on AWS:

All ePHI at rest is encrypted using AWS KMS customer managed keys (CMKs). CMKs are created per account, with automatic annual rotation enabled. Key policies restrict which IAM principals can perform encrypt and decrypt operations. CloudTrail logs every key usage event.

Encryption is enforced through SCPs that deny creation of unencrypted S3 buckets, unencrypted Amazon Elastic Block Store (Amazon EBS) volumes, and unencrypted RDS instances. AWS Config rules continuously monitor compliance.

KMS CMKs aren't the only permissible mechanism under §164.312(a)(2)(iv). Organizations might alternatively use SSE-C (customer-provided keys, where the customer supplies the encryption key per API request and AWS never retains it) or client-side encryption (where ePHI is encrypted before transmission to AWS using the AWS Encryption SDK or equivalent, with keys managed entirely outside AWS). The approach used should be documented in the organization's risk analysis. This guide describes encryption using KMS CMKs because it's the most common implementation for cloud-based HIPAA workloads and provides integration with AWS services, centralized key management, and CloudTrail auditability of key usage events. If SSE-C or client-side encryption is used, the supporting documentation requirements in this section will differ—evidence for key management will exist outside of AWS.

Examples of supporting documentation for audit readiness:

- KMS CMK inventory showing keys per PHI account with rotation enabled
- SCP denying `s3:CreateBucket` without encryption and denying `ec2:CreateVolume` without encryption
- AWS Config rule compliance report: `encrypted-volumes`, `s3-bucket-server-side-encryption-enabled`, and `rds-storage-encrypted` all showing as `COMPLIANT`
- AWS KMS CloudTrail log showing key usage events

Technical references:

- AWS KMS Developer Guide
- Configuring default encryption
- Encrypting Amazon RDS resources
- Amazon EBS encryption
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment

§164.312(b): Audit controls (Required)

Requirement: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Implementation on AWS:

An organization-wide CloudTrail trail captures management events and data events (S3 object-level, DynamoDB item-level) for all accounts in the PHI boundary. Logs are delivered to the Log Archive account with S3 Object Lock (Compliance mode) providing Write Once, Read Many (WORM) protection. Log file integrity validation uses SHA-256 hashing and digital signatures to detect tampering.

VPC Flow Logs capture network traffic for all PHI workload VPCs. S3 server access logs provide object-level access records. Amazon CloudWatch Logs centralizes application and system logs. Amazon CloudWatch Logs Insights and the CloudWatch unified observability data store provide a centralized query and analysis layer across log sources.

The customer's log retention configuration should be aligned with the organization's data retention policies and applicable state and federal regulations requirements.

Logs might contain ePHI: application logs from clinical systems can inadvertently capture patient identifiers, query parameters, or error messages containing health data. Audit logs should be encrypted at rest using AWS KMS on both the S3 log archive bucket and CloudWatch Logs log groups, and access should be restricted to authorized security and audit roles. Consider structured logging practices in application design to minimize ePHI capture in log data.

Examples of supporting documentation for audit readiness:

- CloudTrail organization trail configuration showing management and data events enabled for all PHI accounts
- S3 Object Lock configuration on the log archive bucket (Compliance mode, 6-year retention)

- CloudTrail log file integrity validation status (enabled)
- Log review process documentation and sample review records
- VPC Flow Logs enabled on all PHI workload VPCs
- AWS KMS encryption enabled on the S3 log archive bucket and CloudWatch Logs log groups
- Access control evidence showing log archive restricted to security and audit roles

Technical references:

- Working with CloudTrail trails
- Validating CloudTrail log file integrity
- Locking objects with Object Lock
- Logging IP traffic using VPC Flow Logs

§164.312(c)(1): Integrity (Addressable)

Requirement: Implement policies and procedures to protect ePHI from improper alteration or destruction.

Implementation on AWS:

S3 Versioning maintains a complete history of object changes. S3 Object Lock prevents deletion or overwrite for a configurable retention period. Amazon RDS automated backups and point-in-time recovery (35-day window) enable restoration from any modification event. AWS Backup centralizes backup management with configurable retention and cross-Region replication.

DynamoDB point-in-time recovery (PITR) is enabled for all PHI DynamoDB tables.

Examples of supporting documentation for audit readiness:

- S3 Versioning and S3 Object Lock configuration for all PHI S3 buckets
- RDS automated backup configuration and retention period documentation
- AWS Backup plan showing PHI data stores are included
- Evidence of backup restoration test (annual minimum)

Technical references:

- RDS automated backup
- Locking objects with Object Lock
- Logging IP traffic using VPC Flow Logs

§164.312(c)(2): Mechanism to authenticate ePHI (Addressable)

Requirement: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Implementation on AWS:

CloudTrail log file validation uses SHA-256 hashing and RSA digital signatures. Amazon S3 provides object checksums (SHA-256, CRC32) that validate data integrity during storage and retrieval. AWS Config records resource configuration states over time, enabling detection of unauthorized configuration changes.

Examples of supporting documentation for audit readiness:

- CloudTrail log file integrity validation enabled and periodically verified
- S3 object checksum verification procedure documentation
- AWS Config configuration timeline showing no unauthorized changes to PHI data stores

Technical references:

- Validating CloudTrail log file integrity with the AWS CLI
- Checking object integrity in Amazon S3
- How AWS Config Works

§164.312(d): Person or entity authentication (Required)

Requirement: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Implementation on AWS:

MFA is enforced for human access to systems containing ePHI through IAM Identity Center policies and SCPs. The SCP includes a condition that denies console actions unless `aws:MultiFactorAuthPresent` is `true`. FIDO2 security keys and TOTP tokens are supported. Service-to-service authentication uses IAM roles with certificate-based mutual TLS.

AWS Config continuously monitors MFA enforcement status across all PHI accounts.

Examples of supporting documentation for audit readiness:

- IAM Identity Center MFA enforcement policy configuration
- SCP requiring `aws:MultiFactorAuthPresent` for console access in PHI OUs
- AWS Config rule `iam-user-mfa-enabled and root-account-mfa-enabled` shows as `COMPLIANT`
- Periodic MFA enrollment audit records

Technical references:

- Configure MFA device enforcement
- Secure API access with MFA
- Available MFA types for IAM Identity Center

§164.312(e)(1): Transmission security (Required)

Requirement: Implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.

Implementation on AWS:

Transmission security is enforced at the infrastructure layer through TLS 1.2 or greater on all endpoints, VPN encryption for hybrid connectivity, and network-level controls that prevent unencrypted paths to ePHI. The PHI boundary established in earlier in this document confirms that no ePHI flows over the public internet without encryption. VPC endpoints route AWS service API traffic within the AWS network.

Examples of supporting documentation for audit readiness:

- Network topology diagram showing all transmission paths for ePHI
- Confirmation that no unencrypted paths to ePHI exist within the PHI boundary
- VPC endpoint configuration for all in-scope AWS services

Technical references:

- AWS PrivateLink User Guide
- AWS Client VPN Administrator Guide

§164.312(e)(2)(i): Integrity controls (Addressable)

Requirement: Implement security measures to confirm that electronically transmitted ePHI isn't improperly modified without detection.

Implementation on AWS:

TLS 1.2 and later protocols provide integrity protection through message authentication codes (MACs) that detect any modification of data in transit. AWS service API endpoints enforce a minimum of TLS 1.2. ALB and NLB security policies are configured to enforce TLS 1.2 or TLS 1.3.

Examples of supporting documentation for audit readiness:

- ALB and NLB security policy configuration showing TLS 1.2+ enforcement
- AWS Config rule compliance confirming TLS minimum version on all load balancers
- Evidence that no HTTP (unencrypted) listeners exist on any PHI-facing endpoint

Technical references:

- Create an HTTPS listener for your Application Load Balancer
- List of AWS Config Managed Rules

§164.312(e)(2)(ii): Encryption in transit (Addressable)

Requirement: Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Implementation on AWS:

TLS certificates managed by ACM are deployed on ALBs, CloudFront distributions, and Amazon API Gateway endpoints. The recommended security policy is ELBSecurityPolicy-TLS13-1-2-2021-06 or later. HTTP is disabled—traffic must use HTTPS. AWS Site-to-Site VPN provides encrypted IPSec tunnels for hybrid connectivity. Amazon RDS enforces SSL and TLS connections.

Examples of supporting documentation for audit readiness:

- ALB security policy configuration showing TLS 1.2+ enforcement
- AWS Config rule monitoring TLS enforcement on load balancers and Amazon RDS
- ACM certificate inventory for all PHI-facing endpoints
- Confirmation that HTTP listeners are disabled or redirect to HTTPS

Technical references:

- ALB Security Policies
- Secure communication between AWS Site-to-Site VPN
- Use HTTPS with CloudFront
- ACM certificate inventory

§164.312(a)(1): Network segmentation (NPRM proposed new specification)

Requirement (proposed): Establish technical policies ensuring ePHI is segmented to limit lateral movement during attacks. Documented architecture required. Includes closing or disabling unused network ports and services.

Implementation on AWS:

Network segmentation in an LZA based PHI environment is enforced at four layers: account isolation, VPC design, subnet tiers, and network inspection.

At the account layer, separate OUs for PHI workloads, security tooling, and logging contain the blast radius—a compromised workload account can't access the security or log archive accounts. Transit Gateway route tables enforce which accounts can communicate and block direct account-to-account traffic that doesn't traverse the inspection VPC.

Within each PHI workload VPC, private subnets are used exclusively—no internet gateway is attached to workload VPCs. Application tiers (compute, database, cache) are placed in separate subnets with security group rules permitting only the minimum required traffic between tiers.

Network Firewall is deployed in the inspection VPC with a deny-by-default policy. Stateful rules permit only known-good traffic patterns. Unused ports and protocols are blocked at the firewall layer. VPC Flow Logs capture traffic for audit purposes.

AWS Config rule `vpc-default-security-group-closed` enforces that default security groups aren't used in PHI VPCs.

Examples of supporting documentation for audit readiness:

- Network architecture diagram showing account isolation, VPC topology, subnet tiers, and all traffic flows
- Transit Gateway route table configuration showing inter-OU traffic controls
- Network Firewall rule groups showing deny-by-default policy and permitted traffic
- Security group rules for all PHI workload tiers showing least-privilege inbound and outbound
- VPC Flow Logs enabled on all PHI workload VPCs
- AWS Config rule `vpc-default-security-group-closed` shows as `COMPLIANT`

Technical references:

- AWS Network Firewall Developer Guide
- Security best practices for your VPC
- Transit gateway route tables in AWS Transit Gateway
- Logging IP traffic using VPC Flow Logs
- Security group rules

§164.312(c): Configuration management (NPRM proposed new specification)

Requirement (proposed): Deploy technical controls for configuring relevant electronic information systems, including workstations in a consistent manner. Baseline configurations required and enforced.

Implementation on AWS:

For organizations using the Landing Zone Accelerator, the LZA deployment provides a version-controlled, auditable configuration baseline. Account structure, SCPs, security service settings, and network configurations are defined in YAML and deployed using the AWS Cloud Development Kit (AWS CDK) and AWS CloudFormation. This means the configuration baseline is version-controlled, repeatable, and auditable by design.

AWS Config with the HIPAA conformance pack provides more than 80 managed rules that continuously evaluate whether running configurations match the required baseline. Any configuration drift from the baseline generates a finding in AWS Config and aggregates to Security Hub. The AWS Config configuration timeline records every configuration change against every in-scope resource.

State Manager, a capability of AWS Systems Manager, enforces desired state configurations on EC2 instances—so OS-level settings (CIS hardening, required agents, disabled services) are applied and maintained. State Manager associations remediate drift automatically on a configurable schedule.

SCPs act as the top-level configuration enforcement layer—they prevent actions that would create a resource in a non-compliant configuration (unencrypted, public-facing, in a non-approved Region) regardless of the IAM permissions of the calling identity.

The AWS Foundational Security Best Practices (FSBP) standard provides a consolidated compliance score against configuration baselines across PHI accounts.

Examples of supporting documentation for audit readiness:

- LZA configuration YAML files under version control showing authoritative baseline
- AWS Config conformance pack compliance report showing all rules as `COMPLIANT`
- State Manager association list showing OS baseline configurations applied to all PHI instances
- Security Hub FSBP compliance score and trend over time
- SCP list showing configuration guardrails applied to PHI OUs

- Configuration change history from AWS Config timeline for any material changes

Technical references:

- Operational Best Practices for HIPAA Security
- AWS Systems Manager State Manager
- Landing Zone Accelerator on AWS (LZA) Universal Configuration
- AWS Foundational Security Best Practices standard in Security Hub CSPM
- Service control policies (SCPs)

§164.312(c)(2)(i): Anti-malware protection (NPRM proposed new specification)

Requirement (proposed): Deploy and maintain anti-malware protections on all relevant electronic information systems handling ePHI. This is a technical safeguard requirement—no longer addressed solely through workforce training under §164.308(a)(5).

Implementation on AWS:

GuardDuty can be enabled organization-wide using delegated administration, providing coverage across PHI accounts without per-account configuration. Organizations should evaluate the appropriate delegated administrator account based on their account structure.

Amazon Inspector continuously scans EC2 instances, Lambda functions, and ECR container images for software vulnerabilities. Amazon Inspector findings are aggregated in Security Hub for consolidated visibility and prioritized remediation. Amazon Inspector operates continuously—not on a scheduled scan window—so newly discovered Common Vulnerabilities and Exposures (CVEs) are evaluated against the running environment automatically.

For Amazon EC2 workloads requiring agent-based endpoint protection, organizations might deploy third-party endpoint detection and response (EDR) solutions available through AWS Marketplace. Third-party tools aren't covered under the AWS BAA—customers must execute a separate BAA with the applicable vendor prior to use in PHI environments. Macie continuously monitors S3 buckets in ePHI accounts for sensitive data exposure and anomalous access patterns, providing a data-layer complement to the compute-layer malware detection.

Examples of supporting documentation for audit readiness:

- GuardDuty organization-wide enrollment screenshot showing all ePHI accounts as members
- GuardDuty Malware Protection enabled status for Amazon EC2 and Amazon S3 in all ePHI accounts
- Amazon Inspector enabled status across all ePHI accounts with findings routed to Security Hub
- Security Hub aggregated findings view showing GuardDuty and Amazon Inspector coverage
- EDR deployment evidence (if agent-based): Fleet Manager, a capability of Systems Manager, showing agent installed on all PHI EC2 instances
- Macie findings report showing no unprotected S3 buckets containing PHI

Technical references:

- GuardDuty Malware Protection for EC2
- Automated scan types in Amazon Inspector
- Understanding cross-Region aggregation in Security Hub CSPM
- Governance and control with AWS Marketplace

§164.312(c)(2)(ii)—Software removal (NPRM proposed new specification)

Requirement (proposed): Remove extraneous and unnecessary software from the covered entity's or business associate's relevant electronic information systems.

Implementation on AWS:

Inventory, a capability of Systems Manager, provides a complete, continuously updated inventory of all software installed on EC2 instances across ePHI accounts.

Systems Manager Inventory collects installed application data, Windows Registry entries, network configurations, and running services—enabling identification of unauthorized or unnecessary software that should be removed. Where State Manager is deployed, associations can be configured to enforce desired software state and remediate drift automatically on a defined schedule. For example, removing a deprecated application from all instances in a PHI account automatically. This turns software removal from a one-time manual action into a continuously enforced control.

The AWS Config rule `ec2-instance-managed-by-ssm` confirms EC2 instances in PHI accounts are enrolled in Systems Manager, providing the visibility foundation required before software removal can be enforced. Instances not enrolled in Systems Manager are detected as non-compliant and flagged in Security Hub.

For containerized workloads, software removal is enforced at the image level: ECR image scanning and a Kyverno or OPA admission controller policy in Amazon Elastic Kubernetes Service (Amazon EKS) prevent deployment of container images that contain packages flagged as unauthorized or high-severity CVE-affected.

The approved software baseline for container images is maintained in a registry and enforced at deployment time. For AWS managed services (Amazon RDS, Lambda runtime, AWS Fargate), unnecessary software removal is an AWS responsibility under the Shared Responsibility Model—customers don't have OS-level access and AWS manages the underlying software stack.

Examples of supporting documentation for audit readiness:

- Systems Manager Inventory report showing authorized software baseline per instance type across PHI accounts
- State Manager association list showing software enforcement policies applied
- AWS Config compliance report showing `ec2-instance-managed-by-ssm` as `COMPLIANT` for all PHI instances
- Software removal procedure document naming who owns the approved software baseline, the review cadence, and the removal process for unauthorized software discovered in inventory
- Container image policy showing only approved base images are deployed in PHI workloads

Technical references:

- AWS Systems Manager Inventory
- AWS Systems Manager State Manager
- List of AWS Config Managed Rules
- Shared responsibility
- Amazon ECR image scanning

§164.312(c)(2)(iii): Configuration (NPRM proposed new specification)

Requirement (proposed): Implement specific technical security configuration settings on relevant electronic information or ePHI systems in accordance with documented security standards. Systems must be configured to the approved security baseline, not left at vendor defaults.

Implementation on AWS:

The governance framework that enforces these settings—LZA, AWS Config, SCPs, and Security Hub—is described under the parent §164.312(c) standard described earlier. This section focuses on the specific configuration content that the framework enforces.

CIS Benchmark hardening is applied to EC2 instances using State Manager. The specific settings enforced include: password complexity and history policy, account lockout thresholds, audit policy enabling logging of logon events and privilege use, disabling unnecessary services (Print Spooler, Telnet, SNMP where not required), Windows Firewall enabled on all profiles, SMB signing required, NTLMv2 enforcement, and minimum TLS version on all server roles. The benchmark level (CIS Level 1 or Level 2) is selected per instance classification and documented in the baseline document.

For Amazon WorkSpaces, a hardened golden image is maintained as the standard desktop configuration. The image is built from an approved Windows baseline with CIS L1 settings applied, unnecessary applications removed, and required security agents installed (EDR, Systems Manager agent). Users receive this preconfigured image and can't modify security-relevant settings. The image is refreshed on a defined cadence—at minimum quarterly—and security-relevant changes require a new image version.

For AWS managed services (Amazon RDS, Lambda, Amazon ECS on Fargate), the configuration baseline is enforced through service-level settings.

RDS instances are deployed with encryption enabled, minor version auto-upgrade enabled, deletion protection on, and enhanced monitoring active. Lambda functions are deployed with reserved concurrency where applicable, environment variable encryption using AWS KMS, and no inline IAM wildcard policies. These settings are enforced at deployment using infrastructure as code (IaC) and monitored by AWS Config rules.

Examples of supporting documentation for audit readiness:

- CIS Benchmark baseline document specifying which benchmark version and level applies per EC2 instance type, with rationale for any exceptions

- State Manager association execution history showing baseline applied to all PHI instances
- WorkSpaces golden image change log showing current image version, hardening steps applied, and approval sign-off
- Amazon RDS configuration inventory showing encryption, deletion protection, and auto-upgrade status for all PHI databases
- AWS Config rule compliance showing service-level configuration rules as `COMPLIANT` across all PHI accounts

Technical references:

- CIS Benchmarks for AWS
- CIS Benchmark for Windows Server
- AWS Systems Manager State Manager
- Create a custom WorkSpaces image and bundle for WorkSpaces Personal
- Best practices for Amazon RDS

§164.312(c)(2)(iv): Network ports (NPRM proposed new specification)

Requirement (proposed): Implement controls to manage network ports, protocols, and services on relevant electronic information or ePHI systems, disabling or restricting those that aren't required for approved business functions.

Implementation on AWS:

A recommended practice is to have security groups reference each other by group ID rather than CIDR ranges, scoping port access to specific resource types. Organizations should evaluate this approach as part of their network security design. Network access control lists (ACLs) at the subnet level provide a stateless secondary layer of port restriction. Critical subnets—particularly the isolated database subnet—have network ACLs denying all inbound traffic except from the application tier subnet on the specific database port.

Network Firewall in the centralized inspection VPC enforces port and protocol restrictions for all east-west and egress traffic. Network Firewall rules deny outbound traffic on non-approved ports and

protocols—preventing EC2 instances from initiating connections on ports associated with command-and-control, data exfiltration, or lateral movement patterns.

SCPs include guardrails that prevent security group rules permitting unrestricted inbound access (0.0.0.0/0) on sensitive ports (22, 3389, 1433, 3306).

AWS Config provides managed rules such as `restricted-ssh` and `restricted-common-ports` that can be used to continuously monitor for security group rules permitting unrestricted inbound access. Organizations should select AWS Config rules aligned to their documented security baseline.

VPC endpoints alleviate the need for internet-facing ports for AWS service traffic—EC2 instances communicate with Amazon S3, Service Manager, AWS KMS, and other AWS services over private endpoints without requiring outbound internet access on any port.

Examples of supporting documentation for audit readiness:

- Security group inventory showing all PHI-account security groups with inbound and outbound rules—no 0.0.0.0/0 on sensitive ports
- Network Firewall rule group showing denied protocols and ports
- AWS Config compliance report showing `restricted-ssh` and `restricted-common-ports` as `COMPLIANT` for all PHI accounts
- VPC endpoint inventory showing private connectivity for all AWS service traffic, avoiding public port requirements
- Network ACL configuration for database and application subnets
- SCP list including the security group port restriction guardrails

Technical references:

- Control traffic to your AWS resources using security groups
- Control subnet traffic with network access control lists
- AWS Network Firewall Developer Guide
- AWS Config rule: restricted-ssh
- AWS Config rule: restricted-common-ports

- Access AWS services through AWS PrivateLink
- Service control policies (SCPs)

§164.312(c)(2)(v): Maintenance (NPRM proposed new specification)

Requirement (proposed): Implement technical procedures for maintaining relevant electronic information systems handling ePHI, including applying security patches and updates in a timely manner to address known vulnerabilities.

Implementation on AWS:

Patch Manager, a capability of Systems Manager, provides automated patch management across EC2 instances in PHI accounts. Patch baselines should define which patches are approved for deployment and the severity thresholds that trigger remediation. Organizations might structure separate patch baselines for different OS types and instance roles based on their patching policy.

Patch Manager patch compliance reporting is available through the Systems Manager console and integrates with Security Hub—non-compliant instances (missing critical patches beyond the defined SLA) generate Security Hub findings routed to the security operations team.

For AWS managed services (Amazon RDS, Lambda runtimes, Amazon ECS with Fargate, Amazon ElastiCache), AWS handles OS and runtime patching under the Shared Responsibility Model. The customer is responsible for applying minor and major version updates to the managed service (for example, upgrading an RDS engine version when the current version approaches end-of-support). Amazon RDS publishes maintenance windows and notifies account owners of pending auto-applied maintenance. The customer documents the Amazon RDS and other managed service version currency as part of the maintenance evidence package.

Amazon Inspector continuously evaluates EC2 instances and Lambda functions for known CVEs and provides a prioritized remediation list. Amazon Inspector findings that represent actively exploited vulnerabilities are routed to Security Hub with CRITICAL severity and trigger an immediate response SLA outside the standard maintenance window cadence.

For container workloads, ECR image scanning (powered by Amazon Inspector) evaluates container images on push and continuously reevaluates deployed images as new CVE data becomes available. Images with unacceptable CVE counts are flagged in the continuous integration and continuous delivery (CI/CD) pipeline before deployment and in Security Hub post-deployment.

Examples of supporting documentation for audit readiness:

- Patch Manager patch compliance report showing all PHI EC2 instances as `COMPLIANT` against defined patch baseline
- Patch baseline document specifying approved patches, severity thresholds, and patching SLAs (for example, Critical: 15 days, High: 30 days)
- Maintenance window configuration showing scheduled patching windows for PHI instances
- Amazon RDS and managed service version inventory showing no end-of-support versions in use
- Amazon Inspector findings report showing no unresolved critical CVEs beyond remediation SLA
- ECR image scan results showing PHI-deployed container images with no critical unresolved CVEs
- Patch management procedure document naming patch owner, review cadence, exception process, and escalation path

Technical references:

- AWS Systems Manager Patch Manager
- Patch baselines
- AWS Systems Manager Maintenance Windows
- Getting started tutorial: Activating Amazon Inspector
- Maintaining a DB instance
- Scan images for software vulnerabilities in Amazon ECR
- Creating and updating findings in Security Hub CSPM
- AWS Shared Responsibility Model

Conclusion

This guide has demonstrated how AWS services can support HIPAA Security Rule Technical Safeguard requirements across access control, encryption, audit logging, integrity, authentication, and transmission

security. The key principle throughout is that AWS provides the platform capabilities—the customer configures, monitors, and documents them.

Three things matter most when implementing these controls. First, the AWS Shared Responsibility Model is not a formality—AWS provides the capability, but you must enable and enforce it. Second, your PHI boundary, built through LZA and SCPs, determines the scope of every control in this guide; without it, nothing else is properly scoped. Third, the 2025 NPRM makes clear that encryption, MFA, and asset inventory are heading toward mandatory status—build them in now rather than retrofitting later.

For assistance with HIPAA readiness beyond Technical Safeguards, including Administrative Safeguards, Physical Safeguards, risk analysis, and assessment preparation, contact the AWS Security Assurance Services team or your AWS account representative.

Contributors

Authors to this document include:

- Abdul Javid, Sr. Assurance Consultant, AWS Security Assurance Services LLC
- Shreya Singh, Assurance Consultant, AWS Security Assurance Services LLC

Additional contributors:

- Hector Rodriguez, HCLS Security Specialist, AWS WWPS: US Healthcare
- Kapil Temghare, Security Industry Spec II, AWS Security (Compliance)

Further reading

- Audit Protocol
- AWS HIPAA Compliance Center
- AWS Artifact (AWS BAA and compliance reports)
- Federal Register: 89 FR 106043 (the NPRM itself)
- HIPAA Security Rule: 45 CFR §164.302–§164.318
- HIPAA compliance for generative AI solutions on AWS

- HIPAA Security Rule NPRM (January 6, 2025)
- HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for ePHI
- HHS OCR Regulatory Initiatives
- HHS HIPAA Enforcement
- HHS Breach Notification Rule
- HHS De-identification of PHI
- Landing Zone Accelerator on AWS
- Operational Best Practices for HIPAA Security
- NIST SP 800-53 Rev. 5
- NIST-Security-HIPAA-Crosswalk

Glossary of terms and acronyms

The following table defines key terms, acronyms, and abbreviations used throughout this document.

Term	Definition
ARN	Amazon Resource Name—the unique identifier assigned to every AWS resource and IAM identity.
BA	Business associate—an organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity.
BAA	Business Associate Agreement (also referred to as the AWS Business Associate Addendum)—the legally required contract between AWS and a customer that covers the handling of ePHI under HIPAA.
CFR	Code of Federal Regulations—the codification of federal regulations, including the HIPAA Security Rule at 45 CFR §164.302–§164.318.
CMK	Customer managed key—an AWS KMS encryption key that a customer creates and controls, as opposed to an AWS managed key.

Term	Definition
EDR	Endpoint detection and response—agent-based endpoint security software used to detect and respond to threats on hosts.
EHR	Electronic health record—a digital record of a patient's health information maintained by a healthcare provider.
ePHI	Electronic protected health information—PHI that is created, stored, transmitted, or received in electronic form.
FIPS	Federal Information Processing Standards—US government standards for cryptographic modules; FIPS 140-2 validated endpoints are available in AWS GovCloud (US).
FSBP	Foundational Security Best Practices—the AWS Security Hub standard that evaluates accounts against a curated set of security controls.
HHS	US Department of Health and Human Services—the federal agency that administers and enforces HIPAA.
HIPAA	Health Insurance Portability and Accountability Act of 1996—the US federal law establishing standards for protecting health information.
LZA	Landing Zone Accelerator on AWS—a prescriptive, multi-account AWS architecture solution used to establish account structure, guardrails, and governance.
MFA	Multi-factor authentication—a security mechanism requiring more than one form of verification to authenticate a user.
NIST	National Institute of Standards and Technology—a US federal agency that publishes cybersecurity standards, including NIST SP 800-53.
NLB	Network Load Balancer—a Layer 4 load balancer used for high-performance TCP and UDP traffic.
NPRM	Notice of Proposed Rulemaking—the January 2025 HHS OCR proposal to update the HIPAA Security Rule.
OCR	Office for Civil Rights—the office within HHS responsible for enforcing HIPAA.
OU	Organizational unit—a container within AWS Organizations used to group accounts for policy application, such as those defined by the LZA.

Term	Definition
PHI	Protected health information—individually identifiable health information as defined under HIPAA.
PITR	Point-in-time recovery—a feature (for example, in Amazon RDS or Amazon DynamoDB) that allows restoration of data to a specific point in time.
QSAC	Qualified Security Assessor Company—a company certified by the PCI Security Standards Council to perform PCI DSS assessments.
RSA	Rivest-Shamir-Adleman—an asymmetric cryptographic algorithm used, for example, in AWS CloudTrail log file digital signatures.
SCP	Service control policy—an AWS Organizations policy used to set the maximum available permissions for accounts within an OU.
SHA	Secure Hash Algorithm—a family of cryptographic hash functions (for example, SHA-256) used for integrity verification.
SLA	Service level agreement—in this document, refers to internal timelines for applying patches based on severity.
SSE-KMS	Server-Side Encryption with AWS KMS—an S3 encryption option where AWS KMS manages the encryption keys.
VPC	Virtual private cloud—Amazon VPC is an isolated virtual network within AWS.
WAF	Web application firewall—AWS WAF inspects Layer 7 HTTP and HTTPS traffic for common exploits.
WORM	Write Once, Read Many—a storage model (implemented using Amazon S3 Object Lock) that prevents deletion or modification of data for a defined retention period.

Document revisions

Date	Description
July 2026	Version 1