ONE GUY CONSULTING

The HIPAA Compliance Glossary

1,300 HIPAA and compliance terms in plain English, A to Z, with citations to the federal regulation text.

oneguyconsulting.com/glossary

HIPAA Compliance Made Approachable

How to use this glossary

Every term in this document is defined in plain English. Where a definition comes straight from the regulation, the citation sits next to the term so you can read the source text yourself. Where a term deserves more than a paragraph, a link points to a detailed guide on oneguyconsulting.com.

The searchable, always-current version of this glossary lives at **oneguyconsulting.com/glossary**. This PDF is a snapshot; the page is the living document.

Citations reference Title 45 of the Code of Federal Regulations as published in the eCFR. Terms of art such as PHI, covered entity, and business associate are used exactly as the regulation defines them.

> **A note on scope.** This glossary is educational material, not legal advice. One Guy Consulting is not a law firm. Definitions summarize federal HIPAA regulations; how a requirement applies to your organization depends on your circumstances. For legal questions, consult legal counsel.

One Guy Consulting · hello@oneguyconsulting.com · oneguyconsulting.com

A

Access Controls
45 CFR § 164.312(a)(1) TECHNICAL SAFEGUARDS

The technical standard requiring policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs granted access rights under § 164.308(a)(4). Its specifications are unique user identification, emergency access procedure, automatic logoff, and encryption and decryption.

Guide: ePHI access control best practices

Accounting of Disclosures
45 CFR § 164.528 PATIENT RIGHTS

The individual's right to an accounting of disclosures of PHI made in the six years before the request, excluding disclosures for treatment, payment, and operations, to the individual, under authorization, for the facility directory, for national security, to correctional institutions, and certain others. Respond within 60 days with one 30-day extension; the first accounting in any 12-month period is free.

Addressable Implementation Specification
45 CFR § 164.306(d)(3) SECURITY RULE

For an addressable specification, the entity must assess whether it is a reasonable and appropriate safeguard in its environment. If it is, implement it. If not, document why and implement an equivalent alternative measure if reasonable and appropriate. Addressable does not mean optional; every addressable specification requires a documented decision.

Guide: Addressable does not mean optional

Administrative Requirements
45 CFR § 164.530 ADMINISTRATIVE

The Privacy Rule's administrative requirements: designate a privacy official and complaint contact, train the workforce, maintain safeguards, provide a complaint process, apply and document sanctions, mitigate harm, refrain from intimidation and retaliation, not require waiver of rights, maintain written policies and procedures, and retain documentation for six years.

Administrative Safeguards
45 CFR § 164.304 ADMINISTRATIVE

Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information, and to manage the conduct of the workforce in relation to protecting that information.

Guide: The three HIPAA safeguards

Affiliated Covered Entity
45 CFR § 164.105(b) PRIVACY RULE

Legally separate covered entities under common ownership or control may designate themselves a single affiliated covered entity for Privacy, Security, and Breach Notification Rule compliance. The designation must be documented and retained.

Assigned Security Responsibility
45 CFR § 164.308(a)(2) SECURITY RULE

The required standard to identify the security official responsible for developing and implementing the entity's Security Rule policies and procedures.

Audit Controls
45 CFR § 164.312(b) TECHNICAL SAFEGUARDS

The required technical standard to implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Audit Trail
45 CFR § 164.312(b) TECHNICAL SAFEGUARDS

The activity record produced by audit controls: who accessed what, when, and what they did. The rule requires mechanisms that record and examine information system activity; the resulting logs are typically the first evidence OCR requests.

Authorization
45 CFR § 164.508 PRIVACY RULE

The individual's written permission for uses and disclosures not otherwise permitted or required by the Privacy Rule. Must contain the core elements and required statements of § 164.508(c). Psychotherapy notes, marketing, and sale of PHI each require authorization with specific conditions.

Guide: Authorization form requirements

Automatic Logoff
45 CFR § 164.312(a)(2)(iii) TECHNICAL SAFEGUARDS

The addressable specification to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Availability
45 CFR § 164.304 SECURITY RULE

The property that data or information is accessible and usable upon demand by an authorized person.

Access Management 45 CFR § 164.308(a)(4)(i) ADMINISTRATIVE

The required information access management standard: implement policies and procedures for authorizing access to ePHI consistent with the applicable requirements of the Privacy Rule.

Administrative Simplification 45 CFR § 160.103 ADMINISTRATIVE

The HIPAA statutory requirements for transactions, code sets, identifiers, privacy, security, and enforcement. An administrative simplification provision is defined at § 160.103, and 45 CFR Parts 160, 162, and 164 implement them.

Adverse Event Report 45 CFR § 164.512(b)(1)(iii) PRIVACY RULE

PHI may be disclosed to a person subject to FDA jurisdiction with respect to an FDA-regulated product or activity, including to collect or report adverse events, track products, enable recalls, repairs, or replacement, and conduct post-marketing surveillance.

Agency Relationship 45 CFR § 160.402(c) ENFORCEMENT

A covered entity or business associate is liable for a civil money penalty for the acts or omissions of its agent, including a workforce member or business associate acting as agent, determined under the federal common law of agency and acting within the scope of the agency.

Alternative Communication 45 CFR § 164.522(b) PATIENT RIGHTS

The accommodation mechanism for confidential communications: a different phone number, address, or channel; providers may not demand a reason, and plans may require an endangerment statement.

Anonymization 45 CFR § 164.514(a), (b) PRIVACY RULE

The regulation's term is de-identification, achieved by expert determination or safe harbor; information de-identified under either method falls outside HIPAA.

Asset Inventory SECURITY RULE

A maintained list of systems, devices, applications, and media that create, receive, maintain, or transmit ePHI. A risk analysis is incomplete if the organization does not know where ePHI exists.

Assignment of Benefits ADMINISTRATIVE

A patient's authorization allowing a provider to receive payment directly from a health plan. It is a payment workflow concept and should not be confused with a HIPAA authorization for non-TPO use of PHI.

Authentication 45 CFR § 164.304 TECHNICAL SAFEGUARDS

The corroboration that a person is the one claimed.

Authorization Revocation 45 CFR § 164.508(b)(5) PATIENT RIGHTS

An individual may revoke an authorization at any time, in writing, except to the extent the entity has already taken action in reliance on it or the authorization was obtained as a condition of insurance coverage during a contestability period.

Access Certification TECHNICAL SAFEGUARDS

A formal review confirming that user access remains appropriate for job duties. Certifications help detect excessive permissions, stale accounts, and role drift.

Amendment Denial 45 CFR § 164.526(d) PATIENT RIGHTS

Permitted grounds: the record was not created by the entity (unless the originator is no longer available), is not part of the designated record set, would not be available for inspection under § 164.524, or is accurate and complete. Denial triggers a written notice with the right to a statement of disagreement that travels with future disclosures.

Application Whitelisting TECHNICAL SAFEGUARDS

A control that allows only approved software to run. Whitelisting can reduce malware risk on workstations and servers that access ePHI.

Administrative Access Review SECURITY RULE

An administrative safeguard concept involving Administrative Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Audit Evidence ENFORCEMENT

A compliance oversight concept involving Administrative Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Administrative Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Administrative Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Administrative Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Training Record ADMINISTRATIVE

An administrative safeguard concept involving Administrative Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Administrative Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Administrative Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Administrative Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Administrative PHI Handling PRIVACY RULE

A privacy-rule concept involving Administrative PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Administrative Security Control SECURITY RULE

An administrative safeguard concept involving Administrative Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Administrative Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Administrative Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Administrative Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Administrative Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Administrative User Provisioning SECURITY RULE

An administrative safeguard concept involving Administrative User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Administrative Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Administrative Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Administrative Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Administrative Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Administrative Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Administrative Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Evidence Packet SECURITY RULE

An administrative safeguard concept involving Administrative Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Administrative System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Administrative Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Administrative Claims Transaction SECURITY RULE

An administrative safeguard concept involving Administrative Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Administrative Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Patient Request PATIENT RIGHTS

A patient-rights concept involving Administrative Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Administrative Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Administrative Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Administrative Exception Register SECURITY RULE

An administrative safeguard concept involving Administrative Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

B

50 TERMS

Breach 45 CFR § 164.402 ENFORCEMENT

The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. Three exclusions apply: unintentional, good faith acquisition by a workforce member acting within their authority; inadvertent disclosure between persons authorized to access PHI at the same entity or arrangement; and disclosures where the unauthorized recipient would not reasonably have been able to retain the information. An impermissible use or disclosure is presumed to be a breach unless the entity demonstrates a low probability that the PHI has been compromised.

Guide: Building a breach response plan

Breach Notification Rule 45 CFR Part 164, Subpart D (§§ 164.400-164.414) ENFORCEMENT

Requires notification following a breach of unsecured PHI: to individuals under § 164.404, to the media for breaches involving more than 500 residents of a state or jurisdiction under § 164.406, to the Secretary under § 164.408, and by business associates to covered entities under § 164.410.

Guide: Breach Notification Rule compliance

Breach Risk Assessment 45 CFR § 164.402(2) ENFORCEMENT

The four-factor assessment that can rebut the presumption of breach: the nature and extent of the PHI involved, including identifiers and likelihood of re-identification; the unauthorized person who used or received it; whether the PHI was actually acquired or viewed; and the extent to which the risk has been mitigated.

Business Associate (BA) 45 CFR § 160.103 BUSINESS ASSOCIATES

A person who, on behalf of a covered entity but not as a member of its workforce, creates, receives, maintains, or transmits PHI for functions such as claims processing, data analysis, utilization review, quality assurance, patient safety activities, billing, or practice management; or who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving PHI. The definition expressly includes health information organizations, e-prescribing gateways, personal health record vendors acting for a covered entity, and subcontractors that handle PHI for another business associate.

Guide: HIPAA for business associates

Business Associate Agreement (BAA) 45 CFR §§ 164.504(e), 164.314(a) BUSINESS ASSOCIATES

The written contract required before a business associate may create, receive, maintain, or transmit PHI for a covered entity. Required provisions: permitted uses and disclosures, no further use, appropriate safeguards including Security Rule compliance for ePHI, breach and security incident reporting, subcontractor flow-down, support for access, amendment, and accounting rights, HHS access, return or destruction of PHI at termination, and authorization to terminate for violation.

Guide: What is a BAA?

Behavioral Health Record PRIVACY RULE

Health information related to mental health or substance use treatment. It is generally PHI when held by a covered entity, while psychotherapy notes and certain substance use disorder records may receive heightened protections.

Billing Service 45 CFR § 160.103 BUSINESS ASSOCIATES

Billing on a provider's behalf is a named business associate activity, and a billing service converting data between standard and nonstandard formats also appears in the health care clearinghouse definition.

Biometric Identifier 45 CFR § 164.514(b)(2)(i)(P) PRIVACY RULE

A safe harbor identifier category: biometric identifiers, including finger and voice prints, must be removed for de-identification.

Guide: The 18 HIPAA identifiers

Bring Your Own Device (BYOD) TECHNICAL SAFEGUARDS

A policy allowing workforce members to use personal devices for work. If those devices access ePHI, the organization must address authentication, encryption, remote wipe, screen lock, and termination procedures.

Guide: Mobile device security in healthcare

Business Continuity 45 CFR § 164.308(a)(7) ADMINISTRATIVE

HIPAA addresses business continuity through the contingency plan standard: data backup, disaster recovery, emergency mode operation, testing and revision, and application and data criticality analysis.

Business Associate Due Diligence

45 CFR § 164.502(e)(1) BUSINESS ASSOCIATES

The satisfactory assurances requirement is the regulatory hook: the covered entity must have a documented basis (the BAA, and in practice vetting behind it) that the BA will appropriately safeguard PHI.

Business Associate Inventory

BUSINESS ASSOCIATES

A current list of vendors and partners that create, receive, maintain, or transmit PHI for the organization. The inventory helps confirm every business associate has a signed BAA and an owner.

Business Associate Subcontractor

45 CFR §§ 160.103, 164.502(e)(1)(ii) BUSINESS ASSOCIATES

A subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate is itself a business associate, and the BA must obtain the same satisfactory assurances from it that the covered entity obtained from the BA.

Balance Billing

45 CFR §§ 149.410-149.440 ADMINISTRATIVE

The No Surprises Act rules prohibit balance billing for out-of-network emergency services, for nonemergency services by nonparticipating providers at participating facilities absent notice and consent, and for air ambulance services by nonparticipating providers.

Batch Claims

45 CFR § 162.1102 ADMINISTRATIVE

Claims submitted together electronically remain the health care claims transaction and must use the adopted X12N 837 standard.

Bring Your Own Device

TECHNICAL SAFEGUARDS

A workforce device model where personal phones or laptops are used for work. BYOD needs access controls, encryption, remote wipe expectations, and clear PHI handling rules.

Business Continuity Plan

45 CFR § 164.308(a)(7) ADMINISTRATIVE

The contingency plan standard is HIPAA's business continuity requirement: backup, disaster recovery, emergency mode operation, testing, and criticality analysis for systems holding ePHI.

Backup Retention

45 CFR § 164.308(a)(7)(ii)(A) TECHNICAL SAFEGUARDS

The rule requires retrievable exact copies of ePHI; how long backups are kept is a risk-based decision, not a stated timeframe.

Beneficiary Identifier

45 CFR § 164.514(b)(2)(i)(l) PRIVACY RULE

A safe harbor identifier category: health plan beneficiary numbers must be removed for de-identification.

Billing Audit

45 CFR § 164.501 ADMINISTRATIVE

Conducting or arranging auditing functions is a named health care operation, and claims review appears in the payment definition.

Benefit Enrollment

45 CFR § 162.1502 ADMINISTRATIVE

Enrollment and disenrollment in a health plan is a named HIPAA transaction with the X12N 834 as its adopted standard.

Billing Compliance

45 CFR § 164.501 ADMINISTRATIVE

Auditing functions, including fraud and abuse detection and compliance programs, are health care operations by definition.

Biometric Login

45 CFR § 164.312(d) TECHNICAL SAFEGUARDS

Authenticating by fingerprint or face implements the person or entity authentication standard: verifying that the one seeking access to ePHI is the one claimed.

Block Storage

TECHNICAL SAFEGUARDS

A storage model used by servers and cloud systems. When block volumes contain ePHI, encryption, snapshots, access, and disposal need documented safeguards.

Board Reporting

ADMINISTRATIVE

Regular reporting to leadership on compliance risks, incidents, vendor status, and remediation. Board-level visibility helps show governance and accountability.

Business Associate Access Review

BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Access Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Audit Evidence

BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Audit Evidence. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Policy Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Policy Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Risk Finding BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Risk Finding. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Training Record BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Training Record. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Incident Log BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Incident Log. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate PHI Handling BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate PHI Handling. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Security Control BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Security Control. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Privacy Workflow BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Privacy Workflow. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Retention Check BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Retention Check. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Business Associate Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Business Associate User Provisioning BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate User Provisioning. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Encryption Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Encryption Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Backup Test BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Backup Test. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Contingency Task BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Contingency Task. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Compliance Calendar BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Compliance Calendar. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Evidence Packet BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Evidence Packet. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate System Inventory BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate System Inventory. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Business Associate Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Business Associate Claims Transaction BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Claims Transaction. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Eligibility Workflow BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Eligibility Workflow. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Patient Request PATIENT RIGHTS

A patient-rights concept involving Business Associate Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Business Associate Workforce Attestation BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Workforce Attestation. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Business Associate Exception Register BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Business Associate Exception Register. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Certification (HIPAA) ENFORCEMENT

There is no official government-issued HIPAA certification for organizations. No agency certifies that a covered entity is "HIPAA compliant." OCR has explicitly stated that compliance is an ongoing obligation, not a certification status. Individuals can earn credentials such as Certified HIPAA Professional (CHP), but these are professional designations, not government certifications.

Civil Money Penalty (CMP) 45 CFR § 160.103 ENFORCEMENT

The monetary penalty the Secretary may impose for violations of the administrative simplification provisions, in the amount determined under § 160.404.

Guide: Current HIPAA penalty amounts

Cloud Computing TECHNICAL SAFEGUARDS

The use of remote servers to store, manage, and process ePHI. Cloud service providers that store or process ePHI are business associates and must sign a BAA. The covered entity remains responsible for ensuring the provider implements appropriate safeguards. Simply storing encrypted data in the cloud does not eliminate the need for a BAA.

Guide: Cloud storage and HIPAA

Complaint (HIPAA) 45 CFR §§ 164.530(d), 160.306 ENFORCEMENT

Two tracks: the covered entity's internal complaint process, and complaints to the Secretary. Any person may file with OCR, in writing, within 180 days of when they knew or should have known of the act, and OCR may investigate.

Guide: How to respond to a HIPAA complaint

Compliance Program ADMINISTRATIVE

The overall system of policies, procedures, training, documentation, and oversight that an organization uses to meet HIPAA requirements. Includes a risk analysis, written policies, workforce training, sanctions policy, breach response plan, and BAAs. Having one is the primary factor OCR considers when determining enforcement severity.

Guide: Our HIPAA compliance guide

Compound Authorization 45 CFR § 164.508(b)(3) PRIVACY RULE

An authorization generally may not be combined with any other document to create a compound authorization, with narrow exceptions for research study authorizations and combining psychotherapy notes authorizations with each other.

Conduit Exception BUSINESS ASSOCIATES

An exception to the business associate definition for entities that transport PHI but do not routinely access it. The US Postal Service, UPS, and ISPs are conduits and do not need a BAA. However, a cloud company storing PHI is not a conduit. The line between conduit and business associate is narrow.

Confidential Communications 45 CFR § 164.522(b) PATIENT RIGHTS

Providers must permit and accommodate reasonable requests to receive PHI communications by alternative means or at alternative locations; health plans must accommodate when the individual states that disclosure could endanger them.

Confidentiality 45 CFR § 164.304 SECURITY RULE

The property that data or information is not made available or disclosed to unauthorized persons or processes.

Consent 45 CFR § 164.506(b) PRIVACY RULE

A covered entity may obtain the individual's consent to use or disclose PHI for treatment, payment, or health care operations. Consent is optional under the Privacy Rule and never substitutes for an authorization where one is required.

Contingency Plan 45 CFR § 164.308(a)(7)(i) ADMINISTRATIVE

The required standard to establish policies and procedures for responding to an emergency or other occurrence, such as fire, vandalism, system failure, or natural disaster, that damages systems containing ePHI.

Corrective Action Plan (CAP) ENFORCEMENT

A formal agreement between OCR and an entity requiring specific steps to resolve HIPAA violations. CAPs typically run one to three years and include monitoring, reporting, and remediation. Once a CAP is in place, you are on the government's timeline.

Covered Entity (CE) 45 CFR § 160.103 PRIVACY RULE

A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.

Guide: Covered entity, defined

Covered Functions 45 CFR § 164.103 PRIVACY RULE

Those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Criminal Penalties ENFORCEMENT

Penalties imposed by the Department of Justice for knowing HIPAA violations. Three tiers: up to $50,000 and one year in prison for knowing violations, up to $100,000 and five years for false pretenses, up to $250,000 and ten years for intent to sell or use PHI for personal gain. Criminal enforcement targets individuals.

Change Control SECURITY RULE

A documented process for evaluating and approving changes to systems, workflows, or vendors that affect ePHI. Major changes should trigger security evaluation and risk analysis updates.

Claim Attachment 45 CFR § 162.103 ADMINISTRATIVE

Attachment information is defined as documentation of health care or characteristics of health care provided; health claims attachments are a named HIPAA transaction, but no attachment standard has been adopted to date.

Claim Status Inquiry 45 CFR § 162.1402 ADMINISTRATIVE

The health care claim status transaction, conducted with the adopted X12N 276 request and 277 response standards.

Clearinghouse 45 CFR § 160.103 PRIVACY RULE

Short for health care clearinghouse: an entity that converts health information between nonstandard and standard formats for other entities, including billing services, repricing companies, and value-added networks performing those functions.

Clinical Quality Measure PRIVACY RULE

A measurement of healthcare quality using clinical data. If the measure uses identifiable patient information, HIPAA rules for use, disclosure, minimum necessary, and data sharing still apply.

Code Set 45 CFR § 162.103 ADMINISTRATIVE

Any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes, including both the codes and their descriptors.

Compensating Control 45 CFR § 164.306(d)(3)(ii)(B)(2) SECURITY RULE

HIPAA's version of a compensating control: when an addressable specification is not reasonable and appropriate, the entity implements an equivalent alternative measure that accomplishes the same protective purpose, and documents the decision.

Coordination of Benefits 45 CFR § 162.1802 ADMINISTRATIVE

The adopted standards for the coordination of benefits information transaction: the ASC X12N 837 implementations, with NCPDP for retail pharmacy.

Credentialing File 45 CFR § 164.501 ADMINISTRATIVE

Reviewing the competence or qualifications of health care professionals and conducting credentialing activities are named health care operations.

Cross-Border Data Transfer BUSINESS ASSOCIATES

Movement of PHI or ePHI outside the United States or to a vendor with offshore operations. HIPAA does not ban offshore handling, but covered entities must manage BAAs, safeguards, and applicable state or contractual limits.

Custodian of Records ADMINISTRATIVE

The person or role responsible for maintaining and producing records in response to valid requests. In healthcare, this can include medical record access requests, subpoenas, audits, and retention obligations.

Cross-Site Scripting (XSS) TECHNICAL SAFEGUARDS

A web application vulnerability that can let attackers run malicious scripts in a user's browser. In healthcare portals, XSS can expose sessions, messages, or other ePHI.

Covered Entity Access Review SECURITY RULE

An administrative safeguard concept involving Covered Entity Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Audit Evidence ENFORCEMENT

A compliance oversight concept involving Covered Entity Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Covered Entity Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Training Record ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Covered Entity Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Covered Entity Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Covered Entity Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Covered Entity PHI Handling PRIVACY RULE

A privacy-rule concept involving Covered Entity PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Covered Entity Security Control SECURITY RULE

An administrative safeguard concept involving Covered Entity Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Covered Entity Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Covered Entity Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Covered Entity Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Covered Entity User Provisioning SECURITY RULE

An administrative safeguard concept involving Covered Entity User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Covered Entity Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Covered Entity Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Covered Entity Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Covered Entity Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Covered Entity Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Evidence Packet SECURITY RULE

An administrative safeguard concept involving Covered Entity Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Covered Entity System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Covered Entity Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Covered Entity Claims Transaction SECURITY RULE

An administrative safeguard concept involving Covered Entity Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Covered Entity Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Covered Entity Patient Request PATIENT RIGHTS

A patient-rights concept involving Covered Entity Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

D

50 TERMS

Data Aggregation 45 CFR § 164.501 BUSINESS ASSOCIATES

With respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of that PHI with PHI received as business associate of another covered entity, to permit data analyses relating to the health care operations of the respective covered entities.

Data Backup Plan 45 CFR § 164.308(a)(7)(ii)(A) ADMINISTRATIVE

The required specification to establish and implement procedures to create and maintain retrievable exact copies of ePHI.

Data Use Agreement (DUA) 45 CFR § 164.514(e)(4) BUSINESS ASSOCIATES

The agreement required before disclosing a limited data set: it establishes the permitted uses and disclosures, identifies who may use or receive the data, and binds the recipient to safeguards, non-re-identification, no contacting of individuals, and flow-down to agents.

Decedent PHI 45 CFR § 164.502(f) PRIVACY RULE

A covered entity must protect a deceased individual's PHI for 50 years following death; after that, the information is no longer PHI.

De-identification 45 CFR § 164.514(a), (b) PRIVACY RULE

Health information that does not identify an individual, and for which there is no reasonable basis to believe it can be used to identify, is not individually identifiable. The rule provides two methods: expert determination and safe harbor. Properly de-identified information is no longer PHI.

Guide: De-identification requirements

Designated Record Set 45 CFR § 164.501 PATIENT RIGHTS

A group of records maintained by or for a covered entity that is: the medical and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or records used, in whole or in part, to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Device and Media Controls 45 CFR § 164.310(d)(1) TECHNICAL SAFEGUARDS

The required standard for policies and procedures governing the receipt and removal of hardware and electronic media containing ePHI into and out of a facility, and their movement within it.

Direct Treatment Relationship 45 CFR § 164.501 PRIVACY RULE

A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship; the provider delivers care, services, or results directly to the individual rather than through another provider.

Disaster Recovery Plan 45 CFR § 164.308(a)(7)(ii)(B) ADMINISTRATIVE

The required specification to establish, and implement as needed, procedures to restore any loss of data.

Disclosure 45 CFR § 160.103 PRIVACY RULE

The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Documentation Requirements 45 CFR § 164.316(b)(1) ADMINISTRATIVE

Maintain Security Rule policies and procedures in written form (which may be electronic), and maintain a written record of any action, activity, or assessment the Rule requires to be documented.

Guide: HIPAA documentation requirements

Data Classification SECURITY RULE

The practice of labeling information by sensitivity and handling requirements. PHI and ePHI should be classified so workforce members know when stronger access, storage, transmission, and disposal controls apply.

Data Loss Prevention (DLP) TECHNICAL SAFEGUARDS

Technology and procedures designed to detect or block improper transmission of sensitive data. DLP can help prevent PHI from leaving through email, web uploads, removable media, or unmanaged cloud tools.

Data Mapping ADMINISTRATIVE

Documenting where PHI is collected, stored, used, transmitted, disclosed, and destroyed. Data mapping supports risk analysis, minimum necessary review, breach response, and vendor management.

Data Minimization 45 CFR § 164.502(b) PRIVACY RULE

HIPAA's data minimization principle is the minimum necessary standard: limit uses, disclosures, and requests of PHI to what the purpose actually requires.

Delegated Access TECHNICAL SAFEGUARDS

Access granted to a person acting on behalf of another user, patient, or organization. Delegated access should be documented, limited by role, and traceable in audit logs.

Directory Information 45 CFR § 164.510(a) PRIVACY RULE

The narrow facility directory categories: name, facility location, general condition, and religious affiliation, shareable under the informed no-objection rules; not a license for broader disclosure.

Disposal 45 CFR § 164.310(d)(2)(i) TECHNICAL SAFEGUARDS

The required specification for policies and procedures addressing the final disposition of ePHI and the hardware or electronic media on which it is stored.

Downtime Procedure 45 CFR § 164.308(a)(7)(ii)(C) ADMINISTRATIVE

Documented manual operations during system unavailability implement the emergency mode operation specification: continuing critical business processes while protecting ePHI.

Denial Management 45 CFR § 164.501 ADMINISTRATIVE

Working denied claims falls inside the definition of payment: billing, claims management, collection activities, and related health care data processing.

Delegated Administration TECHNICAL SAFEGUARDS

A model where certain users can manage accounts, roles, or settings for a defined area. Delegated admin rights should be limited, logged, and reviewed.

Device Hardening TECHNICAL SAFEGUARDS

Configuring devices to reduce security risk before use. Hardening can include disabling services, enforcing encryption, patching, and applying baseline settings.

Digital Signature 45 CFR § 162.103 TECHNICAL SAFEGUARDS

The regulation defines electronic signature for transactions: an electronic sound, symbol, or process attached to or logically associated with attachment information and executed by a person with the intent to sign it.

Disclosure Authorization Log 45 CFR § 164.508(b)(6) PRIVACY RULE

A covered entity must document and retain every signed authorization, as required by § 164.530(j).

Downtime Form 45 CFR § 164.308(a)(7)(ii)(C) ADMINISTRATIVE

The paper capture tool used during system downtime, part of emergency mode operation procedures for continuing critical processes while protecting ePHI.

Designated Access Review SECURITY RULE

An administrative safeguard concept involving Designated Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Audit Evidence ENFORCEMENT

A compliance oversight concept involving Designated Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Designated Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Designated Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Designated Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Training Record ADMINISTRATIVE

An administrative safeguard concept involving Designated Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Designated Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Designated Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Designated Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Designated PHI Handling PRIVACY RULE

A privacy-rule concept involving Designated PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Designated Security Control SECURITY RULE

An administrative safeguard concept involving Designated Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Designated Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Designated Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Designated Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Designated Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Designated User Provisioning SECURITY RULE

An administrative safeguard concept involving Designated User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Designated Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Designated Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Designated Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Designated Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Designated Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Designated Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Evidence Packet SECURITY RULE

An administrative safeguard concept involving Designated Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Designated System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Designated Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Designated Claims Transaction SECURITY RULE

An administrative safeguard concept involving Designated Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Designated Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Patient Request PATIENT RIGHTS

A patient-rights concept involving Designated Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Designated Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Designated Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Designated Exception Register SECURITY RULE

An administrative safeguard concept involving Designated Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Media
45 CFR § 160.103 TECHNICAL SAFEGUARDS

Electronic storage material on which data is or may be recorded electronically (hard drives, removable or transportable digital memory such as magnetic tape or disk, optical disk, or digital memory card), and transmission media used to exchange information already in electronic storage media (internet, extranet or intranet, leased lines, dial-up lines, private networks, and physical movement of removable storage media). Paper-to-paper faxes and voice telephone calls are not electronic media transmissions if the information did not exist in electronic form immediately before the transmission.

Electronic Protected Health Information (ePHI)
45 CFR § 160.103 SECURITY RULE

Protected health information that is transmitted by electronic media or maintained in electronic media (paragraphs (1)(i) and (1)(ii) of the definition of protected health information).

Guide: What is ePHI?

Emergency Access Procedure
45 CFR § 164.312(a)(2)(ii) TECHNICAL SAFEGUARDS

The required specification to establish and implement procedures for obtaining necessary ePHI during an emergency.

Emergency Mode Operation Plan
45 CFR § 164.308(a)(7)(ii)(C) ADMINISTRATIVE

The required specification for procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

Encryption
45 CFR § 164.304 TECHNICAL SAFEGUARDS

The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Guide: HIPAA encryption requirements

Enforcement Rule
45 CFR Part 160, Subparts C, D, and E ENFORCEMENT

The compliance and investigation procedures, civil money penalty provisions, and hearing procedures for the administrative simplification rules: complaints, investigations, penalty amounts and factors, affirmative defenses, and appeals.

Guide: What triggers an OCR investigation

Evaluation
45 CFR § 164.308(a)(8) SECURITY RULE

The required standard to perform periodic technical and nontechnical evaluation, based initially on the Security Rule standards and thereafter in response to environmental or operational changes, establishing the extent to which policies and procedures meet the Rule's requirements.

Expert Determination
45 CFR § 164.514(b)(1) PRIVACY RULE

A person with appropriate knowledge and experience with generally accepted statistical and scientific principles determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual, and documents the methods and results.

Encryption at Rest
45 CFR § 164.312(a)(2)(iv) TECHNICAL SAFEGUARDS

The addressable specification to implement a mechanism to encrypt and decrypt ePHI. Data encrypted consistent with HHS guidance is also secured, taking its loss outside breach notification.

Encryption in Transit
45 CFR § 164.312(e)(2)(ii) TECHNICAL SAFEGUARDS

The addressable specification to implement a mechanism to encrypt ePHI whenever deemed appropriate during transmission.

Endpoint Detection and Response (EDR)
TECHNICAL SAFEGUARDS

Security tooling that monitors computers and servers for suspicious activity and helps contain malware or unauthorized access. EDR supports HIPAA's expectation that organizations detect and respond to security incidents.

Enterprise Risk Management
ADMINISTRATIVE

An organization-wide approach for identifying and managing operational, compliance, financial, and security risks. HIPAA risk analysis should connect to this broader governance process when one exists.

Enrollment Transaction
45 CFR § 162.1502 ADMINISTRATIVE

The enrollment and disenrollment transaction, conducted with the adopted ASC X12N 834 standard.

Exception Request SECURITY RULE

A request to deviate from a standard, policy, or control for a documented reason. Security exceptions should be time-limited, risk-reviewed, approved, and tracked through remediation.

External Audit ADMINISTRATIVE

An assessment performed by an outside party to evaluate compliance, controls, or financial processes. External audits do not create official HIPAA certification, but they can identify gaps and support remediation.

Electronic Funds Transfer 45 CFR §§ 162.1601, 162.1602 ADMINISTRATIVE

The health care EFT and remittance advice transaction: transmission of payment and payment processing information from a health plan to a provider's financial institution, with adopted standards at § 162.1602 and CAQH CORE operating rules at § 162.1603.

Electronic Remittance Advice 45 CFR § 162.1602 ADMINISTRATIVE

The 835 remittance advice adopted as the standard for explaining health plan payment of claims.

Emergency Contact Information 45 CFR § 164.510(b) PRIVACY RULE

A covered entity may disclose to a family member, relative, close personal friend, or person identified by the individual the PHI directly relevant to that person's involvement in the individual's care or payment, and may notify such persons of the individual's location, general condition, or death.

Endpoint Detection and Response TECHNICAL SAFEGUARDS

Security tooling that monitors endpoints for suspicious activity, malware, and compromise. EDR supports detection and response for systems that access or store ePHI.

Evidence of Compliance 45 CFR §§ 164.316(b), 164.530(j) ADMINISTRATIVE

HIPAA's documentation requirements define the evidence: written policies and procedures, written records of required actions and assessments, and six-year retention.

Eligibility Inquiry 45 CFR § 162.1202 ADMINISTRATIVE

The eligibility for a health plan transaction, conducted with the adopted X12N 270 inquiry and 271 response standards.

Email Encryption Gateway 45 CFR § 164.312(e)(2)(ii) TECHNICAL SAFEGUARDS

A gateway that encrypts outbound email carrying ePHI implements the addressable transmission encryption specification.

Employee Health Record 45 CFR § 160.103 PRIVACY RULE

Employment records held by a covered entity in its role as employer are excluded from the definition of PHI. The same lab result can be PHI in the patient chart and a non-PHI employment record in the HR file.

Endpoint Inventory TECHNICAL SAFEGUARDS

A list of laptops, desktops, phones, tablets, servers, and other endpoints. Inventory supports patching, encryption tracking, access review, and incident response.

Exception Register ADMINISTRATIVE

A maintained list of approved deviations from policy or standard controls. Each exception should include owner, reason, compensating controls, and expiration.

Electronic Access Review SECURITY RULE

An administrative safeguard concept involving Electronic Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Audit Evidence ENFORCEMENT

A compliance oversight concept involving Electronic Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Electronic Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Electronic Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Electronic Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Training Record ADMINISTRATIVE

An administrative safeguard concept involving Electronic Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Electronic Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Electronic Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Electronic Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Electronic PHI Handling PRIVACY RULE

A privacy-rule concept involving Electronic PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Electronic Security Control SECURITY RULE

An administrative safeguard concept involving Electronic Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Electronic Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Electronic Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Electronic Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Electronic Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Electronic User Provisioning SECURITY RULE

An administrative safeguard concept involving Electronic User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Electronic Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Electronic Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Electronic Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Electronic Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Electronic Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Electronic Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Evidence Packet SECURITY RULE

An administrative safeguard concept involving Electronic Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Electronic System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Electronic Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Electronic Claims Transaction SECURITY RULE

An administrative safeguard concept involving Electronic Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Electronic Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Patient Request PATIENT RIGHTS

A patient-rights concept involving Electronic Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Electronic Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Electronic Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Electronic Exception Register SECURITY RULE

An administrative safeguard concept involving Electronic Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Access Controls
45 CFR § 164.310(a)(1) TECHNICAL SAFEGUARDS

The required standard to implement policies and procedures to limit physical access to electronic information systems and the facilities housing them, while ensuring that properly authorized access is allowed.

Facility Directory
45 CFR § 164.510(a) PRIVACY RULE

A covered health care facility may maintain a directory holding the individual's name, location in the facility, general condition, and religious affiliation, and disclose it to clergy or to persons who ask for the individual by name, if the individual was informed and given the chance to object. Religious affiliation goes only to clergy.

Facility Security Plan
45 CFR § 164.310(a)(2)(ii) TECHNICAL SAFEGUARDS

The addressable specification for policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering, and theft.

FERPA
45 CFR § 160.103; 20 U.S.C. 1232g PRIVACY RULE

Education records covered by FERPA, and the student treatment records described at 20 U.S.C. 1232g(a)(4)(B)(iv), are excluded from the definition of protected health information. Student health records at FERPA-covered schools generally follow FERPA, not HIPAA.

False Pretenses
ENFORCEMENT

A criminal HIPAA culpability concept involving obtaining or disclosing PHI under deceptive circumstances. It carries higher potential criminal penalties than a knowing violation without false pretenses.

Fax Transmission
45 CFR § 160.103 PRIVACY RULE

Under the electronic media definition, a paper-to-paper fax is not an electronic media transmission when the information did not exist in electronic form immediately before transmission; the faxed PHI remains PHI and misdirected faxes remain disclosures.

Guide: Is faxing HIPAA compliant?

Fee Limitation
45 CFR § 164.524(c)(4) PATIENT RIGHTS

Access fees may include only reasonable, cost-based labor for copying, supplies for the copy, postage, and preparation of an agreed summary. Retrieval fees are not permitted.

Firewall
TECHNICAL SAFEGUARDS

A network security control that filters traffic between networks or systems. Firewalls help reduce exposure of systems containing ePHI and should be configured, monitored, and reviewed.

Forensic Analysis
SECURITY RULE

Technical investigation of a security incident to determine what happened, which systems were affected, and whether ePHI was accessed or exfiltrated. Findings often inform breach risk assessment.

Fundraising Communication
45 CFR § 164.514(f) PRIVACY RULE

A covered entity may use limited categories of PHI for its own fundraising, must provide a clear and conspicuous opportunity to opt out with each communication, may not condition treatment or payment on the choice, and must honor elections.

Facility Maintenance Record
45 CFR § 164.310(a)(2)(iv) TECHNICAL SAFEGUARDS

The addressable specification to document repairs and modifications to the physical components of a facility related to security, for example hardware, walls, doors, and locks.

Federated Identity
TECHNICAL SAFEGUARDS

An identity model where a trusted provider authenticates users for multiple applications. It can simplify access management but still needs MFA, logging, and timely deprovisioning.

Firewall Rule Review
TECHNICAL SAFEGUARDS

A periodic check of network access rules to remove unnecessary exposure. Reviews help show reasonable protection against anticipated threats to ePHI systems.

First Report of Injury
45 CFR §§ 164.512(l), 160.103 PRIVACY RULE

PHI may be disclosed as authorized by, and to the extent necessary to comply with, workers' compensation laws and similar no-fault programs for work-related injuries or illness. First report of injury is also a named HIPAA transaction in the § 160.103 transaction definition, though no standard has been adopted for it.

Formulary 45 CFR § 156.122 ADMINISTRATIVE

For essential health benefits, a plan must cover prescription drugs per USP category and class counts, use a pharmacy and therapeutics committee, and publish an up-to-date, accurate, and complete drug list. HIPAA-side, formulary communications appear in the marketing definition's refill reminder carve-out at § 164.501.

Fraud Waste and Abuse 45 CFR § 164.501 ADMINISTRATIVE

Fraud and abuse detection and compliance programs are named health care operations; related payment-side review activities appear in the payment definition.

Guide: Fraud, waste, and abuse training

Full Disk Encryption 45 CFR §§ 164.312(a)(2)(iv), 164.402 TECHNICAL SAFEGUARDS

Implements the encryption specification; a lost laptop whose disk was encrypted consistent with the HHS guidance referenced in § 164.402 does not hold unsecured PHI, so its loss is not a reportable breach.

Functional Acknowledgment ADMINISTRATIVE

An electronic response confirming receipt or syntax status of a transaction file. Acknowledgments help troubleshoot HIPAA transaction exchange failures.

Failover Procedure 45 CFR § 164.308(a)(7)(ii)(B), (C) TECHNICAL SAFEGUARDS

Switching to standby systems during an outage implements the disaster recovery and emergency mode operation specifications for systems containing ePHI.

File Integrity Monitoring 45 CFR § 164.312(c)(2) TECHNICAL SAFEGUARDS

Implements the addressable mechanism to authenticate ePHI: electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Fax Cover Sheet PRIVACY RULE

A cover page used when sending records by fax. It should limit PHI, identify the intended recipient, and include misdirected-fax instructions.

Federated Login TECHNICAL SAFEGUARDS

A login method where one identity provider authenticates users across multiple systems. It can improve control if MFA, logging, and deprovisioning are enforced.

Field-Level Encryption 45 CFR § 164.312(a)(2)(iv) TECHNICAL SAFEGUARDS

Encrypting specific database fields implements the addressable mechanism to encrypt and decrypt ePHI.

File Transfer Protocol TECHNICAL SAFEGUARDS

A protocol used to move files between systems. PHI transfers should use secure variants and approved workflows, not plain unencrypted FTP.

Fraud Investigation Disclosure 45 CFR § 164.512(d) ENFORCEMENT

The health oversight provision: PHI may be disclosed to a health oversight agency for audits, civil, administrative, or criminal investigations, inspections, licensure actions, and proceedings overseeing the health care system and government benefit programs.

Facility Access Review SECURITY RULE

An administrative safeguard concept involving Facility Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Audit Evidence ENFORCEMENT

A compliance oversight concept involving Facility Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Facility Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Facility Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Facility Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Training Record ADMINISTRATIVE

An administrative safeguard concept involving Facility Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Facility Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Facility Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Facility Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Facility PHI Handling PRIVACY RULE

A privacy-rule concept involving Facility PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Facility Security Control SECURITY RULE

An administrative safeguard concept involving Facility Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Facility Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Facility Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Facility Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Facility Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Facility User Provisioning SECURITY RULE

An administrative safeguard concept involving Facility User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Facility Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Facility Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Facility Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Facility Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Facility Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Facility Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Evidence Packet SECURITY RULE

An administrative safeguard concept involving Facility Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Facility System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Facility Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Facility Claims Transaction SECURITY RULE

An administrative safeguard concept involving Facility Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Facility Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Patient Request PATIENT RIGHTS

A patient-rights concept involving Facility Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Facility Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Facility Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Facility Exception Register SECURITY RULE

An administrative safeguard concept involving Facility Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Gap Analysis ADMINISTRATIVE

An evaluation comparing your current HIPAA posture against regulatory requirements to identify deficiencies. Typically follows a risk assessment and produces a list of areas where policies, procedures, or technical controls are missing. The output feeds directly into a remediation plan.

Guide: What is a HIPAA gap analysis?

Genetic Information 45 CFR § 160.103 PRIVACY RULE

With respect to an individual: information about the individual's genetic tests, the genetic tests of family members, the manifestation of a disease or disorder in family members, and any request for or receipt of genetic services or participation in clinical research including genetic services by the individual or a family member. Includes genetic information of a fetus carried by the individual or a family member and of any embryo legally held through assisted reproductive technology. Excludes information about the sex or age of any individual.

Group Health Plan 45 CFR § 160.103 PRIVACY RULE

An employee welfare benefit plan (as defined in section 3(1) of ERISA), including insured and self-insured plans, to the extent the plan provides medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise, that has 50 or more participants or is administered by an entity other than the employer that established and maintains the plan.

Gag Clause ADMINISTRATIVE

A contractual term that restricts legally required or permitted disclosure. In healthcare compliance, agreements should not prevent required reporting, patient rights fulfillment, or cooperation with regulators.

Gateway Provider 45 CFR § 160.103 BUSINESS ASSOCIATES

The business associate definition expressly includes health information organizations, e-prescribing gateways, and other persons providing data transmission services with routine access to PHI.

General Designation ADMINISTRATIVE

A broad role or ownership assignment used in policies, such as designating privacy, security, records, or incident response responsibility. HIPAA programs work better when these designations are named and documented.

Good Faith ENFORCEMENT

A compliance posture showing an organization attempted to follow HIPAA through reasonable policies, training, documentation, and response. Good faith does not erase violations, but it can affect enforcement outcomes.

Governance Committee ADMINISTRATIVE

A group responsible for privacy, security, risk, and compliance oversight. In larger organizations, a committee helps ensure HIPAA decisions are tracked, assigned, and reviewed.

Granular Access TECHNICAL SAFEGUARDS

Access permissions divided by role, location, patient relationship, function, or data type. Granular access helps support minimum necessary use and reduces broad exposure of ePHI.

Guardrail Policy ADMINISTRATIVE

A practical policy that defines boundaries for risky workflows such as texting, cloud storage, remote work, or AI tools. Guardrails help workforce members make compliant choices without memorizing regulations.

Genomic Data 45 CFR § 160.103 PRIVACY RULE

Genetic information (an individual's genetic tests, family members' tests, family disease manifestation, and genetic services participation) is health information by definition and is PHI when individually identifiable and held by a covered entity or business associate.

Geofencing Risk PRIVACY RULE

Privacy and security risk created when location-based tools collect or target people around healthcare facilities. Patient location data can create sensitive inferences.

Grievance Process 45 CFR § 164.530(d) PATIENT RIGHTS

Covered entities must provide a process for individuals to complain about the entity's privacy policies and its compliance, designate a contact person or office, and document all complaints received and their disposition.

Group Practice PRIVACY RULE

A healthcare provider organization where multiple clinicians furnish services. HIPAA duties apply to the covered entity and should be implemented across shared systems and workforce roles.

Guest Wireless Network TECHNICAL SAFEGUARDS

A separate network for patients and visitors. It should be isolated from systems that create, receive, maintain, or transmit ePHI.

Guided Risk Remediation SECURITY RULE

A prioritized workflow that turns risk analysis findings into assigned actions, due dates, evidence, and closure notes. Remediation tracking is what makes risk analysis operational.

General Release Form 45 CFR § 164.508(c) PRIVACY RULE

A broad release is HIPAA-valid only if it contains the authorization core elements and required statements; missing elements or vague descriptions make it defective, and a defective authorization permits nothing.

Governance Charter ADMINISTRATIVE

A document defining a compliance committee's scope, members, meeting cadence, authority, and recordkeeping expectations.

Graymail Filtering TECHNICAL SAFEGUARDS

Filtering for low-value bulk email that can hide important notices or security alerts. Healthcare organizations should avoid filtering that buries breach or vendor notices.

Group Policy Object TECHNICAL SAFEGUARDS

A centralized Windows configuration rule. GPOs can enforce password, lockout, logging, encryption, and workstation controls for ePHI environments.

Granular Permission TECHNICAL SAFEGUARDS

A narrow access permission tied to a specific task, record type, or function. Granular permissions support least privilege and better audit review.

Guardian Access 45 CFR § 164.502(g)(3) PATIENT RIGHTS

A parent, guardian, or person acting in loco parentis is generally the unemancipated minor's personal representative, except when the minor lawfully consented to the care, may lawfully obtain it without parental consent, or a parent has agreed to confidentiality between the minor and the provider.

Guideline Document ADMINISTRATIVE

A practical document explaining how to follow a policy in daily work. Guidelines should stay consistent with approved HIPAA policies and training.

Guest Account TECHNICAL SAFEGUARDS

A temporary or limited account used by visitors, contractors, or support personnel. Guest accounts should expire automatically and avoid unnecessary PHI access.

GxP Validation ADMINISTRATIVE

A regulated-system validation concept often seen in life sciences. It is not a HIPAA requirement, but validation evidence may matter where health data systems overlap.

Governance Access Review ADMINISTRATIVE

An administrative safeguard concept involving Governance Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Audit Evidence ENFORCEMENT

A compliance oversight concept involving Governance Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Governance Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Governance Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Governance Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Training Record ADMINISTRATIVE

An administrative safeguard concept involving Governance Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Governance Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Governance Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Governance Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Governance PHI Handling ADMINISTRATIVE

An administrative safeguard concept involving Governance PHI Handling. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Security Control ADMINISTRATIVE

An administrative safeguard concept involving Governance Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Privacy Workflow ADMINISTRATIVE

An administrative safeguard concept involving Governance Privacy Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Governance Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Governance Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Governance User Provisioning ADMINISTRATIVE

An administrative safeguard concept involving Governance User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Governance Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Governance Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Governance Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Governance Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Governance Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Compliance Calendar ADMINISTRATIVE

An administrative safeguard concept involving Governance Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Evidence Packet ADMINISTRATIVE

An administrative safeguard concept involving Governance Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Governance System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Governance Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Governance Claims Transaction ADMINISTRATIVE

An administrative safeguard concept involving Governance Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Eligibility Workflow ADMINISTRATIVE

An administrative safeguard concept involving Governance Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Patient Request PATIENT RIGHTS

A patient-rights concept involving Governance Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Governance Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Governance Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Governance Exception Register ADMINISTRATIVE

An administrative safeguard concept involving Governance Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

H

Health Care
45 CFR § 160.103 PRIVACY RULE

Care, services, or supplies related to the health of an individual, including preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or affecting the structure or function of the body; and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse
45 CFR § 160.103 PRIVACY RULE

A public or private entity, including a billing service, repricing company, community health management information system, and value-added networks and switches, that either processes health information received from another entity from a nonstandard format into standard data elements or a standard transaction, or receives a standard transaction and converts it into nonstandard format or content for a receiving entity.

Health Care Component
45 CFR § 164.103 PRIVACY RULE

A component or combination of components of a hybrid entity designated as performing covered functions, in accordance with § 164.105(a)(2)(iii)(D).

Health Care Operations
45 CFR § 164.501 PRIVACY RULE

Activities of the covered entity, to the extent related to its covered functions, including: quality assessment and improvement; population-based activities to improve health or reduce costs; case management and care coordination; reviewing competence and qualifications of professionals, evaluating performance, credentialing, training, accreditation, certification, and licensing; conducting or arranging medical review, legal services, and auditing functions, including fraud and abuse detection and compliance; business planning and development; and business management and general administrative activities, including customer service, internal grievance resolution, sale or transfer of assets, and creating de-identified information or limited data sets.

Health Care Provider
45 CFR § 160.103 PRIVACY RULE

A provider of services as defined in section 1861(u) of the Social Security Act, a provider of medical or health services as defined in section 1861(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Information
45 CFR § 160.103 PRIVACY RULE

Any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for health care.

Health Information Exchange (HIE)
45 CFR § 171.102 BUSINESS ASSOCIATES

Defined for information blocking: an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of technology or services for access, exchange, or use of electronic health information among more than two unaffiliated individuals or entities.

Health Plan
45 CFR § 160.103 PRIVACY RULE

An individual or group plan that provides, or pays the cost of, medical care. The definition enumerates 17 categories, including group health plans, health insurance issuers, HMOs, Medicare Parts A and B, Medicaid, Medicare supplement issuers, long-term care policy issuers (excluding certain nursing home fixed indemnity policies), multi-employer welfare plans, and listed government programs. Excepted-benefit policies and government programs whose principal purpose is not providing or paying for health care are excluded.

HHS
45 CFR § 160.103 ENFORCEMENT

The Department of Health and Human Services. In Parts 160 through 164, Secretary means the Secretary of HHS or any officer or employee to whom the authority has been delegated.

HIPAA
PRIVACY RULE

The Health Insurance Portability and Accountability Act of 1996. Established national standards for protecting individually identifiable health information. Key provisions include the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. Despite its name, the law's privacy and security impact far exceeds its original insurance portability focus.

Guide: What is HIPAA?

HITECH Act ENFORCEMENT

The Health Information Technology for Economic and Clinical Health Act of 2009. Made business associates directly liable for HIPAA violations, established the Breach Notification Rule, increased penalties, required periodic audits, and created the public breach portal. Most enforcement mechanisms that give HIPAA its teeth come from HITECH.

Guide: How HITECH changed HIPAA

Hybrid Entity 45 CFR § 164.103 PRIVACY RULE

A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that designates health care components in accordance with the rules.

Harm Threshold 45 CFR § 164.402(2) ENFORCEMENT

The pre-2013 interim standard asking whether an incident posed significant risk of harm to the individual. The Omnibus Rule replaced it with the presumption of breach plus the four-factor low probability of compromise assessment.

Healthcare API 45 CFR § 170.315(g)(10) TECHNICAL SAFEGUARDS

The ONC certification criterion for a standardized API for patient and population services: certified health IT must support FHIR-based API access, the technical foundation for patient-facing apps and data exchange.

Healthcare Clearinghouse Transaction 45 CFR § 162.930 ADMINISTRATIVE

When acting as a business associate, a clearinghouse may receive a standard transaction on a covered entity's behalf and translate it into nonstandard format for the entity, and receive nonstandard transactions and translate them into standard ones.

Health Plan Identifier (HPID) ADMINISTRATIVE

A planned unique identifier for health plans that was never fully implemented as a required standard. Current HIPAA identifier requirements focus on NPIs for providers and EINs for employers in transactions.

Hosted EHR 45 CFR § 160.103 BUSINESS ASSOCIATES

An EHR vendor hosting a provider's records maintains ePHI on the provider's behalf and is a business associate by definition; the BAA and Security Rule obligations attach.

Human Review ADMINISTRATIVE

Manual evaluation by a qualified person before making a compliance-sensitive decision, such as breach determination, disclosure approval, or denial of access. Human review helps avoid automated policy errors.

Health App Data PRIVACY RULE

Information collected by consumer health apps. It may fall outside HIPAA unless handled by a covered entity or business associate, but it can still be sensitive and regulated elsewhere.

Healthcare Common Procedure Coding System 45 CFR §§ 162.103, 162.1002 ADMINISTRATIVE

HCPCS is defined at § 162.103 and adopted at § 162.1002 as a standard code set for physician services, other health care services, and medical supplies, orthotics, and durable medical equipment.

Hardware Asset Tag TECHNICAL SAFEGUARDS

A unique label assigned to a device. Asset tags help track laptops, drives, and equipment that may access or store ePHI.

Hash Value TECHNICAL SAFEGUARDS

A fixed-length value generated from data to help detect changes. Hashes can support integrity checks for files, logs, and evidence packets.

Help Desk Verification 45 CFR § 164.514(h) TECHNICAL SAFEGUARDS

The verification standard: before disclosure, verify the identity of a person requesting PHI and their authority to have access, if not already known, and obtain any required documentation, statements, or representations.

Hosted Database BUSINESS ASSOCIATES

A database operated in a cloud or vendor environment. If it stores ePHI, the hosting arrangement needs safeguards, access controls, and usually a BAA.

Human Resources Boundary 45 CFR § 160.103 PRIVACY RULE

The PHI definition draws the line: records a covered entity holds in its role as employer (sick notes, FMLA paperwork, drug test results in HR files) are excluded from PHI, while identical clinical information in the patient record is PHI.

HIPAA Access Review SECURITY RULE

An administrative safeguard concept involving HIPAA Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Audit Evidence ENFORCEMENT

A compliance oversight concept involving HIPAA Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

HIPAA Policy Review ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Training Record ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving HIPAA Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

HIPAA Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving HIPAA Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

HIPAA PHI Handling PRIVACY RULE

A privacy-rule concept involving HIPAA PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

HIPAA Security Control SECURITY RULE

An administrative safeguard concept involving HIPAA Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Privacy Workflow PRIVACY RULE

A privacy-rule concept involving HIPAA Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

HIPAA Retention Check ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Disclosure Log PATIENT RIGHTS

A patient-rights concept involving HIPAA Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

HIPAA User Provisioning SECURITY RULE

An administrative safeguard concept involving HIPAA User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving HIPAA Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

HIPAA Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving HIPAA Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

HIPAA Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Compliance Calendar SECURITY RULE

An administrative safeguard concept involving HIPAA Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Evidence Packet SECURITY RULE

An administrative safeguard concept involving HIPAA Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA System Inventory ADMINISTRATIVE

An administrative safeguard concept involving HIPAA System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving HIPAA Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

HIPAA Claims Transaction SECURITY RULE

An administrative safeguard concept involving HIPAA Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving HIPAA Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Patient Request PATIENT RIGHTS

A patient-rights concept involving HIPAA Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

HIPAA Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving HIPAA Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

HIPAA Exception Register SECURITY RULE

An administrative safeguard concept involving HIPAA Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

I

50 TERMS

Implementation Specification 45 CFR § 160.103 SECURITY RULE

Specific requirements or instructions for implementing a standard.

Incidental Use and Disclosure 45 CFR § 164.502(a)(1)(iii) PRIVACY RULE

A use or disclosure incident to an otherwise permitted use or disclosure is itself permitted, provided the entity applied reasonable safeguards and the minimum necessary standard. Overheard hallway conversations despite precautions are the classic example.

Individually Identifiable Health Information (IIHI) 45 CFR § 160.103 PRIVACY RULE

A subset of health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; relates to a person's physical or mental health, health care, or payment for health care; and identifies the individual or provides a reasonable basis to believe it could be used to identify the individual.

Guide: Our guide to PHI

Information System Activity Review 45 CFR § 164.308(a)(1)(ii)(D) SECURITY RULE

The required specification to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Integrity 45 CFR § 164.304 SECURITY RULE

The property that data or information have not been altered or destroyed in an unauthorized manner.

Integrity Controls 45 CFR § 164.312(e)(2)(i) TECHNICAL SAFEGUARDS

The addressable specification under transmission security: implement measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Identity Proofing TECHNICAL SAFEGUARDS

The process of verifying a person's identity before granting portal access, releasing records, or enrolling them in a system. Weak identity proofing can lead to improper disclosure of PHI.

Impermissible Disclosure 45 CFR § 164.502(a) PRIVACY RULE

The Privacy Rule's baseline standard: a covered entity or business associate may not use or disclose PHI except as the rule permits or requires. Every breach starts as an impermissible use or disclosure.

Incident Response Plan 45 CFR § 164.308(a)(6) SECURITY RULE

The required security incident procedures standard: identify and respond to suspected or known security incidents, mitigate harmful effects to the extent practicable, and document incidents and their outcomes.

Guide: HIPAA incident management guide

Indirect Treatment Relationship 45 CFR § 164.501 PRIVACY RULE

A relationship in which the provider delivers health care based on the orders of another provider, and typically furnishes services, products, or reports of diagnosis or results directly to that other provider rather than to the individual. Labs and pathologists are the classic examples.

Information Blocking 45 CFR § 171.103 PATIENT RIGHTS

A practice by an actor (health care provider, health IT developer of certified health IT, or health information network or exchange) that is likely to interfere with access, exchange, or use of electronic health information, except as required by law or covered by a regulatory exception. For developers and networks the standard is knows or should know; for providers, knows the practice is unreasonable and likely to interfere.

Internal Audit ADMINISTRATIVE

A self-directed review of policies, procedures, training, access, vendors, or safeguards. Internal audits help catch compliance gaps before a complaint, breach, or regulator review.

Identity and Access Management TECHNICAL SAFEGUARDS

The people, process, and technology used to manage users, authentication, roles, access reviews, and termination. IAM is central to ePHI access control.

Immutable Backup TECHNICAL SAFEGUARDS

A backup that cannot be altered or deleted for a defined period. Immutable backups can improve ransomware resilience and support contingency planning.

Incident Commander ADMINISTRATIVE

The person assigned to coordinate incident response activities. The role should manage escalation, communications, evidence preservation, and decision tracking.

Incident Severity SECURITY RULE

A rating that indicates the impact and urgency of a privacy or security event. Severity levels help determine response timelines, notification review, and leadership involvement.

Independent Contractor 45 CFR § 160.103 BUSINESS ASSOCIATES

The workforce definition turns on direct control, not payroll: a contractor working under the entity's direct control is workforce; one operating independently with PHI is analyzed as a business associate.

Insurance Verification 45 CFR § 164.501 ADMINISTRATIVE

Determination of eligibility or coverage is named inside the Privacy Rule's definition of payment, making verification a permitted payment activity under § 164.506; the electronic version is the 270/271 eligibility transaction at § 162.1202.

Inventory of Information Systems SECURITY RULE

A maintained list of applications, databases, devices, integrations, and repositories that store or transmit ePHI. It is a practical foundation for risk analysis.

Incident Evidence Packet ENFORCEMENT

A collected set of logs, screenshots, notices, timelines, and decisions used to evaluate a privacy or security incident. It supports consistent breach assessment and later investigation response.

Image Archive TECHNICAL SAFEGUARDS

A repository for clinical images, scanned documents, or diagnostic files. Archives containing patient identifiers require access control, retention, and backup safeguards.

Inbound Fax Queue PRIVACY RULE

A workflow where received faxes wait for review and routing. Queues can contain PHI and should have restricted access and timely cleanup.

Indemnification Clause BUSINESS ASSOCIATES

A contract term allocating responsibility for certain losses. Vendor agreements involving PHI should review indemnity alongside BAAs, insurance, and liability limits.

Inference Risk PRIVACY RULE

The risk that seemingly limited data can reveal sensitive facts when combined with other information. Inference risk matters for analytics, location, and small populations.

Integration Account TECHNICAL SAFEGUARDS

A service account used by one system to connect to another. Integration accounts should be unique, scoped, rotated, and monitored.

Individual Access Review PATIENT RIGHTS

A patient-rights concept involving Individual Access Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Audit Evidence PATIENT RIGHTS

A patient-rights concept involving Individual Audit Evidence. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Policy Review PATIENT RIGHTS

A patient-rights concept involving Individual Policy Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Risk Finding PATIENT RIGHTS

A patient-rights concept involving Individual Risk Finding. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Training Record PATIENT RIGHTS

A patient-rights concept involving Individual Training Record. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Incident Log PATIENT RIGHTS

A patient-rights concept involving Individual Incident Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Vendor Review PATIENT RIGHTS

A patient-rights concept involving Individual Vendor Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual PHI Handling PATIENT RIGHTS

A patient-rights concept involving Individual PHI Handling. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Security Control PATIENT RIGHTS

A patient-rights concept involving Individual Security Control. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Privacy Workflow PATIENT RIGHTS

A patient-rights concept involving Individual Privacy Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Retention Check PATIENT RIGHTS

A patient-rights concept involving Individual Retention Check. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Individual Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual User Provisioning PATIENT RIGHTS

A patient-rights concept involving Individual User Provisioning. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Encryption Review PATIENT RIGHTS

A patient-rights concept involving Individual Encryption Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Backup Test PATIENT RIGHTS

A patient-rights concept involving Individual Backup Test. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Contingency Task PATIENT RIGHTS

A patient-rights concept involving Individual Contingency Task. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Compliance Calendar PATIENT RIGHTS

A patient-rights concept involving Individual Compliance Calendar. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Evidence Packet PATIENT RIGHTS

A patient-rights concept involving Individual Evidence Packet. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual System Inventory PATIENT RIGHTS

A patient-rights concept involving Individual System Inventory. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Individual Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Claims Transaction PATIENT RIGHTS

A patient-rights concept involving Individual Claims Transaction. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Eligibility Workflow PATIENT RIGHTS

A patient-rights concept involving Individual Eligibility Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Patient Request PATIENT RIGHTS

A patient-rights concept involving Individual Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Workforce Attestation PATIENT RIGHTS

A patient-rights concept involving Individual Workforce Attestation. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Individual Exception Register PATIENT RIGHTS

A patient-rights concept involving Individual Exception Register. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

J

50 TERMS

Joint Notice of Privacy Practices
45 CFR § 164.520(d) PRIVACY RULE

Covered entities participating in an organized health care arrangement may produce a single joint notice meeting stated conditions; provision of the joint notice by any one participating entity satisfies the requirement for the others at that service delivery site.

Joint Venture BUSINESS ASSOCIATES

A business arrangement between two or more parties. When a healthcare joint venture involves PHI, the parties must analyze covered entity status, business associate roles, BAAs, and permitted uses.

Judicial Proceeding
45 CFR § 164.512(e) PRIVACY RULE

In judicial or administrative proceedings, PHI may be disclosed in response to a court or tribunal order (limited to what the order expressly authorizes), or to a subpoena or discovery request accompanied by satisfactory assurances of notice to the individual or a qualified protective order.

Jurisdiction ENFORCEMENT

The legal authority of a regulator, court, or state over an entity or matter. HIPAA obligations may intersect with state privacy, breach, medical record, and consumer protection laws.

Just-in-Time Access TECHNICAL SAFEGUARDS

Temporary access granted only when needed for a specific task, incident, or patient care purpose. It reduces standing privileges and can support minimum necessary access.

Job Aid ADMINISTRATIVE

A short operational reference that helps workforce members follow privacy or security procedures. Job aids should match the approved policy and avoid creating conflicting instructions.

Job Description Access Mapping TECHNICAL SAFEGUARDS

A process that maps workforce duties to system permissions. It supports role-based access and helps justify why each role needs specific ePHI access.

Joint Commission Survey ADMINISTRATIVE

An accreditation review that may examine privacy, documentation, safety, and operational controls. It is not a HIPAA audit but can surface related compliance gaps.

Jurisdictional Requirement PRIVACY RULE

A state, federal, or local legal requirement that applies in addition to HIPAA. More stringent privacy laws may need to be followed alongside HIPAA.

Just Culture ADMINISTRATIVE

An accountability model that distinguishes human error, risky behavior, and reckless conduct. It can help sanctions policies stay consistent and fair.

Juvenile Record PATIENT RIGHTS

A health record for a minor. Parent access, minor consent, abuse concerns, and state law can change who may access or authorize disclosure.

Justification Memo ADMINISTRATIVE

A short record explaining why a safeguard, disclosure, or addressable specification decision was made. It helps preserve compliance reasoning for later review.

Judicial Proceeding Disclosure
45 CFR § 164.512(e) PRIVACY RULE

The litigation pathway: court order, or subpoena and discovery requests with satisfactory assurances (notice to the individual or a qualified protective order); the disclosure is limited to the PHI expressly authorized.

Junk Fax Prevention PRIVACY RULE

Controls that reduce improper or unsolicited faxing of patient information. Fax workflows should verify recipient numbers and minimize PHI on cover sheets.

Jail Health Record
45 CFR §§ 164.501, 164.512(k)(5) PRIVACY RULE

Correctional institution is defined at § 164.501; a covered entity may disclose an inmate's PHI to the institution or law enforcement custodian when necessary for the individual's health care, safety and security of the institution, officers, employees, transport, or law enforcement on the premises.

Job Shadowing Access ADMINISTRATIVE

Temporary access for trainees or observers. Access should be supervised, limited, and documented when PHI may be visible.

Joint Security Review BUSINESS ASSOCIATES

A shared review between a covered entity and vendor covering safeguards, incidents, access, and open remediation items.

Journal Entry Log ADMINISTRATIVE

A record of manual financial or billing adjustments. If entries reference patients or claims, they should be protected and retained appropriately.

Jumbo Export SECURITY RULE

A large data export from an EHR, billing system, or analytics tool. Bulk exports raise minimum necessary, access, encryption, and retention concerns.

Jurisdictional Hold ADMINISTRATIVE

A preservation requirement driven by a regulator, court, or state law. It may override routine destruction schedules for PHI or compliance evidence.

Jail Medical Unit 45 CFR §§ 164.501, 164.512(k)(5) PRIVACY RULE

Care delivered inside a correctional institution operates under the correctional provisions: disclosures to the institution are permitted for treatment, institutional safety, and custody purposes, and inmates lack certain rights such as notice acknowledgment while in custody.

Jitter in Monitoring TECHNICAL SAFEGUARDS

Small timing variation in logs, alerts, or network signals. Analysts should account for jitter when reconstructing incidents involving ePHI systems.

Job Function Test PRIVACY RULE

A check that PHI access is tied to the user's actual job function. It supports minimum necessary and role-based access decisions.

Joint Investigation ENFORCEMENT

An investigation involving multiple parties, such as a covered entity, business associate, insurer, or regulator. Roles, evidence, and communications should be coordinated.

Justified Disclosure PRIVACY RULE

A disclosure supported by a permitted purpose, authorization, legal requirement, or patient right. The reason and scope should be documented when not routine.

Joint Access Review SECURITY RULE

An administrative safeguard concept involving Joint Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Audit Evidence ENFORCEMENT

A compliance oversight concept involving Joint Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Joint Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Joint Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Joint Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Training Record ADMINISTRATIVE

An administrative safeguard concept involving Joint Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Joint Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Joint Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Joint Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Joint PHI Handling PRIVACY RULE

A privacy-rule concept involving Joint PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Joint Security Control SECURITY RULE

An administrative safeguard concept involving Joint Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Joint Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Joint Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Joint Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Joint Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Joint User Provisioning SECURITY RULE

An administrative safeguard concept involving Joint User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Joint Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Joint Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Joint Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Joint Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Joint Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Joint Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Evidence Packet SECURITY RULE

An administrative safeguard concept involving Joint Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Joint System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Joint Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Joint Claims Transaction SECURITY RULE

An administrative safeguard concept involving Joint Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Joint Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Patient Request PATIENT RIGHTS

A patient-rights concept involving Joint Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Joint Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Joint Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Joint Exception Register SECURITY RULE

An administrative safeguard concept involving Joint Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Key Management TECHNICAL SAFEGUARDS

Procedures for generating, distributing, storing, rotating, and destroying encryption keys. HIPAA does not specify key management by name, but effective encryption requires it. Poorly managed keys (stored alongside encrypted data, shared, or never rotated) undermine encryption entirely.

Key Escrow TECHNICAL SAFEGUARDS

A process for securely storing encryption keys so authorized recovery is possible if primary access is lost. Key escrow must be tightly controlled because misuse can expose encrypted ePHI.

Key Performance Indicator (KPI) ADMINISTRATIVE

A metric used to monitor compliance program performance, such as training completion, BAA coverage, unresolved risks, access review completion, or incident closure time.

Knowledge Factor TECHNICAL SAFEGUARDS

An authentication factor based on something the user knows, such as a password or PIN. Strong systems combine it with possession or biometric factors for multi-factor authentication.

Key Performance Indicator ADMINISTRATIVE

A measurable signal used to manage compliance operations, such as training completion, unresolved risks, overdue BAAs, or incident closure time.

Key Rotation TECHNICAL SAFEGUARDS

The planned replacement of encryption keys. Rotation limits exposure if a key is compromised and supports disciplined encryption management.

Key Risk Indicator SECURITY RULE

A metric that warns of increased privacy or security risk, such as terminated users with active accounts or overdue patching on ePHI systems.

Keyed Hash TECHNICAL SAFEGUARDS

A message authentication method using a secret key to verify integrity. It can help detect unauthorized changes in sensitive data workflows.

Kickoff Checklist ADMINISTRATIVE

A launch checklist used when onboarding a new system, vendor, or location. It should cover PHI flows, access roles, BAAs, training, and safeguards.

Knowledge Base Article ADMINISTRATIVE

An internal support article explaining approved procedures. Articles that mention PHI workflows should be reviewed so they do not conflict with HIPAA policies.

Known Exploited Vulnerability SECURITY RULE

A software flaw listed as actively exploited by attackers. Systems handling ePHI should prioritize remediation of known exploited vulnerabilities.

Known Good Backup TECHNICAL SAFEGUARDS

A backup verified to restore correctly and free of corruption or malware. Backup testing matters because untested backups may fail during an incident.

Known User Inventory TECHNICAL SAFEGUARDS

A list of active workforce and service accounts. It supports access reviews, deprovisioning, and detection of orphaned accounts.

KPI Dashboard ADMINISTRATIVE

A dashboard tracking compliance and security metrics. It should summarize evidence status without exposing unnecessary PHI.

Kerberos Authentication TECHNICAL SAFEGUARDS

A network authentication protocol used in many enterprise environments. When used for ePHI systems, ticket lifetimes, account hygiene, and logging matter.

Kiosk Intake TECHNICAL SAFEGUARDS

Patient intake through a shared kiosk or tablet. It needs screen privacy, session reset, authentication, and sanitation of cached PHI.

KMS Key TECHNICAL SAFEGUARDS

An encryption key managed by a key management service. KMS keys protecting ePHI should have restricted administration, rotation, and audit logs.

Knowledge Transfer ADMINISTRATIVE

The handoff of operational knowledge during staff changes or vendor transitions. For HIPAA programs, transfer should preserve policy ownership, evidence, and risk context.

Known Sender Verification TECHNICAL SAFEGUARDS

A process for confirming that a message or file came from an expected source. It helps reduce phishing and misdirected PHI workflows.

Key Custodian TECHNICAL SAFEGUARDS

A person or role responsible for protecting, issuing, rotating, or recovering encryption keys. Key custodian duties should be separated from ordinary user access where practical.

Key Backup TECHNICAL SAFEGUARDS

A protected copy of an encryption key used for recovery. Key backups need stronger controls than ordinary files because they can unlock sensitive data.

Keyboard Privacy TECHNICAL SAFEGUARDS

Workstation habits and screen placement that reduce shoulder-surfing and accidental viewing. It is a practical physical safeguard in reception and shared spaces.

Kill Chain SECURITY RULE

A model describing stages of an attack, from reconnaissance through actions on objectives. It helps security teams map defenses around ePHI systems.

Knowledge Worker Access ADMINISTRATIVE

Access granted to analysts, billing staff, compliance staff, or managers who need records for operations rather than direct care.

Kubernetes Secret TECHNICAL SAFEGUARDS

A container-platform object used to store credentials or keys. Secrets tied to ePHI applications should be encrypted, scoped, and rotated.

Key Access Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Access Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Audit Evidence ENFORCEMENT

A compliance oversight concept involving Key Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Key Policy Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Policy Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Risk Finding TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Risk Finding. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Training Record TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Training Record. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Key Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Key PHI Handling TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key PHI Handling. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Security Control TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Security Control. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Privacy Workflow TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Privacy Workflow. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Retention Check TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Retention Check. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Key Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Key User Provisioning TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key User Provisioning. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Contingency Task TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Contingency Task. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Compliance Calendar TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Compliance Calendar. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Evidence Packet TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Evidence Packet. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key System Inventory TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key System Inventory. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Key Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Key Claims Transaction TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Claims Transaction. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Eligibility Workflow TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Eligibility Workflow. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Patient Request PATIENT RIGHTS

A patient-rights concept involving Key Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Key Workforce Attestation TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Workforce Attestation. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Key Exception Register TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Key Exception Register. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Law Enforcement Disclosure
45 CFR § 164.512(f) PRIVACY RULE

Permitted disclosures to law enforcement officials: as required by law or legal process; limited identification and location information about suspects, fugitives, witnesses, or missing persons; about victims in stated circumstances; about decedents; crime on the premises; and crime emergencies.

Limited Data Set
45 CFR § 164.514(e)(2) PRIVACY RULE

PHI that excludes 16 listed direct identifiers of the individual and of relatives, employers, and household members. It may retain dates and some geography, and may be used or disclosed only for research, public health, or health care operations, and only under a data use agreement.

Log-in Monitoring
45 CFR § 164.308(a)(5)(ii)(C) TECHNICAL SAFEGUARDS

The addressable specification for procedures to monitor log-in attempts and report discrepancies.

Legal Health Record
PATIENT RIGHTS

The official business record of patient care maintained by a provider. It often overlaps with the designated record set, but the two concepts are not always identical.

Legal Hold
ADMINISTRATIVE

A process preserving records when litigation, investigation, audit, or enforcement action is reasonably anticipated. A legal hold can override normal destruction schedules.

Local Account
TECHNICAL SAFEGUARDS

A user account managed on a single device or application rather than through a central identity provider. Local accounts should be inventoried, secured, and removed when no longer needed.

Lost Device
45 CFR §§ 164.308(a)(6), 164.402 SECURITY RULE

A lost or stolen device holding ePHI is a security incident to respond to, mitigate, and document; if the data was unencrypted, breach notification analysis follows because the PHI was unsecured.

Guide: Lost device incident response

LDAP Directory
TECHNICAL SAFEGUARDS

A directory service used to manage users and groups. When tied to ePHI system access, directory accuracy affects authentication, authorization, and termination controls.

Legacy System
SECURITY RULE

An older application or device that may lack modern security features. Legacy systems containing ePHI need compensating safeguards and documented risk decisions.

Least Functionality
TECHNICAL SAFEGUARDS

A security principle that limits systems to necessary services, ports, and features. It reduces attack surface for systems handling ePHI.

Liability Cap
BUSINESS ASSOCIATES

A contract limit on damages. For vendors handling PHI, liability caps should be reviewed against breach, indemnity, and regulatory risk.

License Verification
45 CFR § 164.501 ADMINISTRATIVE

Licensing and credentialing activities appear in the definition of health care operations, permitting the PHI uses they entail.

Lifecycle Management
ADMINISTRATIVE

Managing systems, vendors, policies, and accounts from creation through retirement. Lifecycle discipline prevents stale access, outdated policies, and unsupported ePHI repositories.

Location Privacy
PRIVACY RULE

Protection of location information that may reveal care, diagnosis, or visit patterns. Location data tied to healthcare can create sensitive PHI inferences.

Log Retention
TECHNICAL SAFEGUARDS

The period audit and security logs are kept. Retention should align with investigation needs, policy requirements, and the six-year HIPAA documentation rule where applicable.

Logical Access
TECHNICAL SAFEGUARDS

Access granted through software permissions rather than physical entry. Logical access controls include authentication, authorization, session management, and logging.

Labeling Standard
ADMINISTRATIVE

Rules for marking documents, exports, tickets, or files by sensitivity. Labels help workforce members recognize PHI and apply the right handling steps.

Legal Medical Record
PRIVACY RULE

The official health record maintained for legal and business purposes. It supports patient access, amendment, disclosure, and retention processes.

Long-Term Care Record PRIVACY RULE

Documentation maintained by skilled nursing, assisted living, or long-term care providers. It is PHI when held by a covered provider.

Lost Device Procedure 45 CFR §§ 164.308(a)(6), 164.402 TECHNICAL SAFEGUARDS

The documented response path for a missing device, implementing the security incident procedures standard and feeding the breach risk assessment when unsecured ePHI is involved.

Laptop Encryption 45 CFR §§ 164.312(a)(2)(iv), 164.402 TECHNICAL SAFEGUARDS

The single highest-value safeguard for portable devices: it implements the encryption specification and keeps a lost laptop outside the breach rules because the PHI is not unsecured.

Late Entry PRIVACY RULE

A record entry made after the original event. Late entries should be clearly marked and preserve integrity of the original documentation timeline.

Letter of Representation ADMINISTRATIVE

A written statement from management, counsel, or a vendor about facts relevant to compliance. It should be supported by evidence where possible.

Live Chat Transcript PRIVACY RULE

A record of a chat interaction. If patients discuss care, billing, or identifiers, transcripts become PHI and need retention and access controls.

Local Administrator TECHNICAL SAFEGUARDS

An account with elevated privileges on a device or application. Local admin rights should be limited because they can bypass normal safeguards.

Limited Access Review SECURITY RULE

An administrative safeguard concept involving Limited Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Audit Evidence ENFORCEMENT

A compliance oversight concept involving Limited Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Limited Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Limited Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Limited Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Training Record ADMINISTRATIVE

An administrative safeguard concept involving Limited Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Limited Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Limited Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Limited Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Limited PHI Handling PRIVACY RULE

A privacy-rule concept involving Limited PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Limited Security Control SECURITY RULE

An administrative safeguard concept involving Limited Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Limited Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Limited Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Limited Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Limited Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Limited User Provisioning SECURITY RULE

An administrative safeguard concept involving Limited User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Limited Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Limited Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Limited Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Limited Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Limited Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Limited Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Evidence Packet SECURITY RULE

An administrative safeguard concept involving Limited Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Limited System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Limited Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Limited Claims Transaction SECURITY RULE

An administrative safeguard concept involving Limited Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Limited Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Patient Request PATIENT RIGHTS

A patient-rights concept involving Limited Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Limited Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Limited Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Limited Exception Register SECURITY RULE

An administrative safeguard concept involving Limited Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

M

50 TERMS

Malicious Software
45 CFR § 164.304 TECHNICAL SAFEGUARDS

Software, for example a virus, designed to damage or disrupt a system.

Marketing (HIPAA)
45 CFR § 164.501 PRIVACY RULE

A communication about a product or service that encourages recipients to purchase or use it. Marketing does not include refill reminders (if any payment received is reasonably related to the cost of making the communication) or communications for treatment, care coordination, or to describe the entity's own health-related products and services, EXCEPT that those become marketing when the covered entity receives financial remuneration from a third party whose product is being promoted. Marketing communications require prior written authorization that discloses the remuneration.

Guide: HIPAA rules for marketing agencies

Media Re-use
45 CFR § 164.310(d)(2)(ii) TECHNICAL SAFEGUARDS

The required specification for procedures to remove ePHI from electronic media before the media are made available for re-use.

Minimum Necessary Standard
45 CFR §§ 164.502(b), 164.514(d) PRIVACY RULE

When using, disclosing, or requesting PHI, make reasonable efforts to limit it to the minimum necessary to accomplish the intended purpose. Does not apply to disclosures to or requests by a provider for treatment, disclosures to the individual, uses or disclosures under an authorization, disclosures to the Secretary, and uses or disclosures required by law.

Guide: The minimum necessary rule

Multi-Factor Authentication (MFA)
TECHNICAL SAFEGUARDS

Access control requiring two or more verification factors before granting access to ePHI. While HIPAA does not explicitly name MFA, the 2025 Security Rule NPRM proposes making it a required specification. Many practices already use MFA for EHR access.

Guide: Is MFA required under HIPAA?

Malware Response
45 CFR §§ 164.308(a)(5)(ii)(B), 164.308(a)(6) SECURITY RULE

Combines the awareness specification (procedures for guarding against, detecting, and reporting malicious software) with the security incident procedures standard (identify, respond, mitigate, document).

Managed Service Provider (MSP)
45 CFR § 160.103 BUSINESS ASSOCIATES

An IT provider that creates, receives, maintains, or transmits ePHI for a covered entity is a business associate; maintaining or hosting ePHI alone triggers the definition, even without viewing it.

Guide: BAA management for vendors and MSPs

Material Breach
45 CFR § 164.504(e)(1)(ii) BUSINESS ASSOCIATES

A business associate violation significant enough to trigger the covered entity's duty to take reasonable steps to cure or end it, and failing that, to terminate the contract if feasible.

Medical Record Number (MRN)
45 CFR § 164.514(b)(2)(i)(H) PRIVACY RULE

A safe harbor identifier category: medical record numbers must be removed for de-identification. Operationally, the MRN is the patient's unique identifier within a provider's systems.

Minimum Necessary Policy
45 CFR § 164.514(d)(3) PRIVACY RULE

The implementation specifications: for routine and recurring disclosures, standard protocols limiting PHI to the minimum necessary; for all other disclosures, criteria and individual review of each request.

Guide: The minimum necessary rule

Mobile Device Management (MDM)
TECHNICAL SAFEGUARDS

Technology used to enforce security settings on phones, tablets, and laptops. MDM can require encryption, passcodes, remote wipe, app controls, and separation of work data.

Guide: Mobile device security in healthcare

Master Patient Index
TECHNICAL SAFEGUARDS

A system that links patient identities across records and facilities. MPI accuracy affects patient matching, privacy, and safe information exchange.

Medical Necessity Review
45 CFR § 164.501 ADMINISTRATIVE

Review of health care services for medical necessity, coverage, or justification of charges is named within the Privacy Rule's definition of payment.

Minimum Cell Size PRIVACY RULE

A reporting rule that suppresses small counts to reduce re-identification risk. It is often used in analytics, quality reporting, and public health datasets.

Mobile Device Management TECHNICAL SAFEGUARDS

Software used to enforce settings on phones, tablets, and laptops. MDM can require encryption, passcodes, remote wipe, and application controls for devices accessing ePHI.

Model Policy ADMINISTRATIVE

A template policy adapted to an organization's actual workflows. Model policies are useful only when customized, approved, trained, and followed.

Multi-Tenant Cloud BUSINESS ASSOCIATES

A cloud environment where multiple customers share provider infrastructure. HIPAA use requires proper logical separation, safeguards, and a BAA when the provider handles ePHI.

Managed Service Provider 45 CFR § 160.103 BUSINESS ASSOCIATES

An outsourced IT provider handling systems that hold ePHI is a business associate under the definition's create, receive, maintain, or transmit language; a BAA is required.

Medical Record Number 45 CFR § 164.514(b)(2)(i)(H) PRIVACY RULE

The unique number identifying a patient within a provider's records; a listed safe harbor identifier that must be removed for de-identification.

Message Authentication Code TECHNICAL SAFEGUARDS

A cryptographic value used to verify message integrity and authenticity. It can support trustworthy transmission of sensitive health data.

Mailroom Procedure ADMINISTRATIVE

Rules for receiving, sorting, scanning, and sending mail that may include PHI. Procedures reduce misrouting and unattended-document exposure.

Managed Backup BUSINESS ASSOCIATES

A backup service operated by an internal IT team or vendor. If the service stores or can access ePHI backups, BAA and safeguard requirements apply.

Manual Workaround ADMINISTRATIVE

A temporary process used when normal systems are unavailable or not ready. Workarounds involving PHI should be approved, documented, and retired.

Media Disposal Log 45 CFR § 164.310(d)(2)(i), (iii) TECHNICAL SAFEGUARDS

The record showing media were disposed of and tracked: disposal procedures are required, and the addressable accountability specification calls for maintaining a record of the movements of hardware and electronic media and any person responsible.

Metadata Exposure PRIVACY RULE

Disclosure of information in file names, headers, logs, or document properties. Metadata can reveal patient identity, diagnosis, location, or workflow details.

Minimum Necessary Access Review PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Access Review. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Audit Evidence ENFORCEMENT

A compliance oversight concept involving Minimum Necessary Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Minimum Necessary Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Training Record ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Minimum Necessary Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Minimum Necessary Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Minimum Necessary Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Minimum Necessary PHI Handling PRIVACY RULE

A privacy-rule concept involving Minimum Necessary PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Security Control PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Security Control. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Minimum Necessary Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Minimum Necessary User Provisioning PRIVACY RULE

A privacy-rule concept involving Minimum Necessary User Provisioning. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Minimum Necessary Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Minimum Necessary Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Minimum Necessary Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Minimum Necessary Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Compliance Calendar PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Compliance Calendar. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Evidence Packet PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Evidence Packet. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Minimum Necessary Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Minimum Necessary Claims Transaction PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Claims Transaction. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Eligibility Workflow PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Eligibility Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Minimum Necessary Patient Request PATIENT RIGHTS

A patient-rights concept involving Minimum Necessary Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Minimum Necessary Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Minimum Necessary Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Minimum Necessary Exception Register PRIVACY RULE

A privacy-rule concept involving Minimum Necessary Exception Register. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

National Provider Identifier (NPI)

45 CFR §§ 162.406, 162.410 ADMINISTRATIVE

The standard unique health identifier for health care providers: a 10-position all-numeric identifier with a check digit and no embedded intelligence. Covered providers must obtain an NPI, disclose it on request, use it in standard transactions, and report changes within 30 days.

NIST

SECURITY RULE

The National Institute of Standards and Technology. Develops cybersecurity standards referenced by OCR. Key documents: NIST SP 800-66 (HIPAA Security Rule implementation), the Cybersecurity Framework, and NIST SP 800-53 (security controls). HHS has cited NIST guidance in multiple enforcement actions.

Notice of Privacy Practices (NPP)

45 CFR § 164.520 PRIVACY RULE

Individuals have a right to adequate written notice of the entity's uses and disclosures of PHI, the individual's rights, and the entity's legal duties, with a required header, content elements, effective date, distribution rules, posting requirements, and website availability.

Guide: Notice of Privacy Practices guide

Network Segmentation

TECHNICAL SAFEGUARDS

Dividing a network into zones to limit movement between systems. Segmentation can reduce the blast radius of malware and protect systems containing ePHI from unnecessary exposure.

Non-Routine Disclosure

45 CFR § 164.514(d)(3)(ii) PRIVACY RULE

For disclosures not made on a routine and recurring basis, develop criteria designed to limit PHI to the minimum necessary and review each request individually against those criteria.

Notification Letter

45 CFR § 164.404(c), (d) ENFORCEMENT

Individual breach notice must describe, to the extent possible, what happened and when, the types of information involved, steps individuals should take, what the entity is doing to investigate and mitigate, and contact procedures. Written notice goes by first-class mail, or email if the individual agreed, without unreasonable delay and no later than 60 days after discovery.

NPP Acknowledgment

45 CFR § 164.520(c)(2)(ii) PRIVACY RULE

A provider with a direct treatment relationship must make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice at first service delivery, and if not obtained, document the effort and why it failed.

National Drug Code

45 CFR § 162.1002 ADMINISTRATIVE

The adopted standard medical data code set for drugs and biologics in retail pharmacy transactions: National Drug Codes as maintained and distributed by HHS in collaboration with drug manufacturers.

Need-to-Know Access

45 CFR § 164.514(d)(2) PRIVACY RULE

The workforce minimum necessary specification: identify the persons or classes of persons who need access to PHI to carry out their duties, the categories of PHI needed, and appropriate conditions on that access.

Non-Disclosure Agreement

BUSINESS ASSOCIATES

A confidentiality contract. An NDA may protect business information, but it does not replace a BAA when a vendor handles PHI for a covered entity.

Non-Repudiation

TECHNICAL SAFEGUARDS

Assurance that a person cannot reasonably deny a transaction or action. Digital signatures, audit logs, and strong authentication support non-repudiation.

Notification Log

ENFORCEMENT

A record of breach or incident notices sent to patients, HHS, media, business associates, or partners. It supports evidence of timely notification.

Nursing Facility Record

PRIVACY RULE

Clinical and administrative documentation maintained by a nursing facility. These records are PHI when held by a covered provider or related business associate.

Near Miss

SECURITY RULE

An event that could have caused a privacy or security incident but was caught before harm occurred. Tracking near misses improves training and controls.

Network Access Control

TECHNICAL SAFEGUARDS

Technology that decides whether devices may connect to a network. NAC can enforce posture checks before access to networks with ePHI systems.

Network Attached Storage TECHNICAL SAFEGUARDS

Shared storage connected to a network. NAS devices containing PHI need access controls, encryption where appropriate, backups, and patching.

Network Diagram SECURITY RULE

A map of systems, segments, connections, and data flows. Current diagrams make risk analysis and incident response more accurate.

Normal Form of Production PATIENT RIGHTS

The format in which records are provided to a requester. Patient access workflows should honor requested electronic form when readily producible.

Notice Delivery Method 45 CFR § 164.404(d) PRIVACY RULE

Breach notice methods: written notice by first-class mail to the last known address (or email if the individual agreed), substitute notice when contact information is insufficient, and urgent notice by telephone in addition to written notice when there is possible imminent misuse.

Network Egress Control TECHNICAL SAFEGUARDS

A safeguard that limits or monitors outbound traffic from systems and networks. Egress controls can reduce unauthorized PHI exports and improve breach detection.

National Plan Identifier ADMINISTRATIVE

A proposed identifier for health plans that has not been implemented as a required standard. Organizations should avoid assuming an adopted plan identifier exists.

Network Flow Log TECHNICAL SAFEGUARDS

A record of network traffic metadata between systems. Flow logs help investigate unusual transfers, lateral movement, and possible PHI exfiltration.

No Surprises Act Record 45 CFR Part 149 ADMINISTRATIVE

Documentation generated under the surprise billing rules (notice and consent records, good faith estimates, required disclosures) lives under 45 CFR Part 149.

Nonproduction Environment TECHNICAL SAFEGUARDS

A test, staging, or development environment. Live PHI should be avoided there unless safeguards, approvals, and masking controls are in place.

NPI Enumeration 45 CFR § 162.408 ADMINISTRATIVE

The National Provider System assigns a single, unique NPI to each provider (with subpart enumeration rules), collects and maintains provider information, deactivates NPIs when appropriate, reactivates on request, and never reassigns a deactivated NPI to another provider.

Notice Access Review PATIENT RIGHTS

A patient-rights concept involving Notice Access Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Audit Evidence PATIENT RIGHTS

A patient-rights concept involving Notice Audit Evidence. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Policy Review PATIENT RIGHTS

A patient-rights concept involving Notice Policy Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Risk Finding PATIENT RIGHTS

A patient-rights concept involving Notice Risk Finding. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Training Record PATIENT RIGHTS

A patient-rights concept involving Notice Training Record. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Incident Log PATIENT RIGHTS

A patient-rights concept involving Notice Incident Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Vendor Review PATIENT RIGHTS

A patient-rights concept involving Notice Vendor Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice PHI Handling PATIENT RIGHTS

A patient-rights concept involving Notice PHI Handling. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Security Control PATIENT RIGHTS

A patient-rights concept involving Notice Security Control. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Privacy Workflow PATIENT RIGHTS

A patient-rights concept involving Notice Privacy Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Retention Check PATIENT RIGHTS

A patient-rights concept involving Notice Retention Check. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Notice Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice User Provisioning PATIENT RIGHTS

A patient-rights concept involving Notice User Provisioning. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Encryption Review PATIENT RIGHTS

A patient-rights concept involving Notice Encryption Review. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Backup Test PATIENT RIGHTS

A patient-rights concept involving Notice Backup Test. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Contingency Task PATIENT RIGHTS

A patient-rights concept involving Notice Contingency Task. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Compliance Calendar PATIENT RIGHTS

A patient-rights concept involving Notice Compliance Calendar. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Evidence Packet PATIENT RIGHTS

A patient-rights concept involving Notice Evidence Packet. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice System Inventory PATIENT RIGHTS

A patient-rights concept involving Notice System Inventory. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Notice Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Claims Transaction PATIENT RIGHTS

A patient-rights concept involving Notice Claims Transaction. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Eligibility Workflow PATIENT RIGHTS

A patient-rights concept involving Notice Eligibility Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Patient Request PATIENT RIGHTS

A patient-rights concept involving Notice Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Workforce Attestation PATIENT RIGHTS

A patient-rights concept involving Notice Workforce Attestation. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Notice Exception Register PATIENT RIGHTS

A patient-rights concept involving Notice Exception Register. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

OCR (Office for Civil Rights) ENFORCEMENT

The HHS division that enforces HIPAA. Investigates complaints, conducts compliance reviews, provides technical assistance, and imposes penalties. Most investigations begin with patient complaints or breach reports, not random audits.

Guide: The OCR audit program

Omnibus Rule ENFORCEMENT

The 2013 final rule implementing HITECH Act provisions into HIPAA. Extended requirements directly to business associates, strengthened the breach notification standard (from "harm" to "probability of compromise"), and expanded patient rights. The reason BAs are directly subject to enforcement today.

Organized Health Care Arrangement (OHCA) 45 CFR § 160.103 PRIVACY RULE

A clinically integrated care setting in which individuals typically receive health care from more than one provider; an organized system of health care in which participating covered entities hold themselves out to the public as joint participants and engage in joint utilization review, quality assessment, or shared financial risk; or specified arrangements between group health plans and health insurance issuers or HMOs. OHCA members may share PHI for the arrangement's operations and may use a joint notice of privacy practices.

Object Security TECHNICAL SAFEGUARDS

A technical approach that applies access controls, labels, or encryption directly to files, records, or data objects. It can help protect PHI even when data moves across systems.

Offshore Vendor BUSINESS ASSOCIATES

A vendor that stores, processes, supports, or accesses PHI from outside the United States. Offshore arrangements require careful BAA terms, security review, and awareness of payer or state restrictions.

Operational Safeguard ADMINISTRATIVE

A day-to-day control that turns written policy into actual practice, such as access reviews, ticket approvals, log checks, badge procedures, or breach drills.

Out-of-Pocket Restriction 45 CFR § 164.522(a)(1)(vi) PATIENT RIGHTS

The mandatory restriction: when the individual or someone on their behalf (other than the plan) has paid for the item or service in full, the entity must honor a request not to disclose it to the health plan for payment or operations, unless disclosure is required by law.

Outsourced Coding 45 CFR § 160.103 BUSINESS ASSOCIATES

Coding vendors receive PHI to assign billing codes on the provider's behalf, a business associate function requiring a BAA.

Open Enrollment 45 CFR § 155.410 ADMINISTRATIVE

The Exchange enrollment provision: the initial open enrollment period and the annual open enrollment period during which qualified individuals may enroll in or change qualified health plans.

Open Notes 45 CFR Part 171 PATIENT RIGHTS

The common name for clinical note sharing driven by the information blocking rules: withholding electronic health information such as clinical notes can be information blocking under § 171.103 unless a regulatory exception applies.

Operational Resilience SECURITY RULE

An organization's ability to continue critical services during disruption. For healthcare, resilience connects contingency planning, backups, downtime procedures, and vendor readiness.

Opt-In Consent PRIVACY RULE

An affirmative permission model where a person actively agrees to a use or disclosure. HIPAA uses authorization for many non-TPO uses, while state law may impose opt-in rules.

Opt-Out Preference PATIENT RIGHTS

A patient's choice to decline certain communications or directory listings when permitted. Preferences should be documented and honored across relevant workflows.

Order Entry System TECHNICAL SAFEGUARDS

A system used to enter medications, labs, imaging, or service orders. Because it creates and transmits PHI, access, integrity, and audit controls matter.

Outage Procedure 45 CFR § 164.308(a)(7)(ii)(C) ADMINISTRATIVE

Steps for operating through a system outage, implementing the emergency mode operation specification for protection of ePHI during the event.

Outsourced Billing 45 CFR § 160.103 BUSINESS ASSOCIATES

A third party billing for a provider handles PHI for a covered function and is a business associate; billing is named in the definition.

Out-of-Band Verification TECHNICAL SAFEGUARDS

Confirming identity or request details through a separate communication channel. It reduces risk for password resets, portal invites, and sensitive disclosures.

Outbound Email Review TECHNICAL SAFEGUARDS

A control or process for checking messages before they leave the organization. It can catch misaddressed emails or attachments containing PHI.

Override Log TECHNICAL SAFEGUARDS

A record of when a user bypasses a normal restriction or alert. Override logs should be reviewed for appropriateness and potential privacy concerns.

Optical Character Recognition TECHNICAL SAFEGUARDS

Technology that converts scanned images into searchable text. OCR output can create new PHI repositories when medical records, IDs, or billing documents are indexed.

Object Storage TECHNICAL SAFEGUARDS

Cloud storage for files and unstructured data. Object buckets containing PHI need access policies, encryption, logging, and lifecycle controls.

Office Closure Procedure ADMINISTRATIVE

A process for securing records, devices, mail, voicemail, and systems during temporary or permanent closure. It supports continuity and privacy protection.

On-Call Access TECHNICAL SAFEGUARDS

Temporary or after-hours access needed for care, support, or incident response. On-call access should be role-limited and logged.

Online Intake Form TECHNICAL SAFEGUARDS

A web form used to collect patient or billing information. Forms collecting PHI need secure transport, storage, access controls, and vendor review.

Overdue Remediation SECURITY RULE

A risk, audit, or incident action that missed its due date. Tracking overdue items helps leadership prioritize unresolved HIPAA exposure.

OCR Access Review SECURITY RULE

An administrative safeguard concept involving OCR Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Audit Evidence ENFORCEMENT

A compliance oversight concept involving OCR Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

OCR Policy Review ADMINISTRATIVE

An administrative safeguard concept involving OCR Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving OCR Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Training Record ADMINISTRATIVE

An administrative safeguard concept involving OCR Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving OCR Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

OCR Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving OCR Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

OCR PHI Handling PRIVACY RULE

A privacy-rule concept involving OCR PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

OCR Security Control SECURITY RULE

An administrative safeguard concept involving OCR Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Privacy Workflow PRIVACY RULE

A privacy-rule concept involving OCR Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

OCR Retention Check ADMINISTRATIVE

An administrative safeguard concept involving OCR Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Disclosure Log PATIENT RIGHTS

A patient-rights concept involving OCR Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

OCR User Provisioning SECURITY RULE

An administrative safeguard concept involving OCR User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving OCR Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

OCR Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving OCR Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

OCR Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving OCR Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Compliance Calendar SECURITY RULE

An administrative safeguard concept involving OCR Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Evidence Packet SECURITY RULE

An administrative safeguard concept involving OCR Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR System Inventory ADMINISTRATIVE

An administrative safeguard concept involving OCR System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving OCR Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

OCR Claims Transaction SECURITY RULE

An administrative safeguard concept involving OCR Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving OCR Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Patient Request PATIENT RIGHTS

A patient-rights concept involving OCR Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

OCR Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving OCR Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

OCR Exception Register SECURITY RULE

An administrative safeguard concept involving OCR Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

P

50 TERMS

Patch Management TECHNICAL SAFEGUARDS

Identifying, testing, and applying software updates to fix known vulnerabilities. The Security Rule's requirement to protect against reasonably anticipated threats encompasses keeping systems updated. Unpatched software is a leading entry point for ransomware in healthcare. OCR has cited failure to patch in multiple enforcement actions.

Payment 45 CFR § 164.501 PRIVACY RULE

Activities of a health plan to obtain premiums or determine or fulfill its coverage and benefit responsibilities, and activities of a provider or plan to obtain or provide reimbursement for health care. Includes eligibility and coverage determinations, adjudication or subrogation of claims, risk adjusting, billing, claims management, collection activities, medical necessity and justification-of-charges review, utilization review (precertification, preauthorization, concurrent and retrospective review), and limited disclosures to consumer reporting agencies.

Person or Entity Authentication 45 CFR § 164.312(d) TECHNICAL SAFEGUARDS

The required standard to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Personal Representative 45 CFR § 164.502(g) PATIENT RIGHTS

A person with authority under applicable law to act on behalf of an individual in making health care decisions, or for a decedent's estate, must be treated as the individual for Privacy Rule purposes, subject to the abuse, neglect, and endangerment exception at § 164.502(g)(5).

Physical Safeguards 45 CFR § 164.304 SECURITY RULE

Physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Guide: Physical safeguards requirements

Plan Sponsor 45 CFR § 164.103 PRIVACY RULE

Defined as at section 3(16)(B) of ERISA: the employer, for a plan established by a single employer; the employee organization, for a plan maintained by one; or the association, committee, joint board of trustees, or similar group, for a multi-employer plan.

Policies and Procedures 45 CFR §§ 164.316(a), 164.530(i) ADMINISTRATIVE

Both rules require implementing reasonable and appropriate written policies and procedures to comply with their standards, maintained in accordance with the documentation requirements and changed as needed.

Guide: Written HIPAA policies

Preemption (State Law) 45 CFR § 160.203 PRIVACY RULE

HIPAA standards preempt contrary state law, with exceptions: Secretary-granted exception determinations, state laws more stringent than the federal standard, public health reporting laws, and certain health plan reporting and audit laws. More stringent state privacy protections survive.

Guide: State privacy laws vs HIPAA

Privacy Officer 45 CFR § 164.530(a)(1)(i) ADMINISTRATIVE

A covered entity must designate, and document, a privacy official responsible for developing and implementing its privacy policies and procedures, plus a contact person or office for complaints and further information.

Guide: HIPAA compliance officer guide

Privacy Rule 45 CFR Part 164, Subpart E (§§ 164.500-164.534) PRIVACY RULE

The privacy standards for individually identifiable health information: permitted and required uses and disclosures, authorization requirements, individual rights (notice, access, amendment, accounting, restrictions), and administrative requirements.

Guide: Privacy Rule requirements

Protected Health Information (PHI) 45 CFR § 160.103 PRIVACY RULE

Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by FERPA, the student treatment records described at 20 U.S.C. 1232g(a)(4)(B)(iv), employment records held by a covered entity in its role as employer, and records of a person who has been deceased for more than 50 years.

Guide: PHI vs PII vs ePHI

Psychotherapy Notes 45 CFR § 164.501 PRIVACY RULE

Notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversation during a private, group, joint, or family counseling session, that are separated from the rest of the individual's medical record. Excludes medication prescription and monitoring, session start and stop times, treatment modalities and frequencies, clinical test results, and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Public Health Activities 45 CFR § 164.512(b) PRIVACY RULE

Permitted disclosures without authorization to public health authorities for preventing or controlling disease, injury, or disability, including reporting disease, births and deaths, child abuse or neglect, FDA-regulated product safety, communicable disease exposure, and workplace medical surveillance in stated circumstances.

Patient Portal TECHNICAL SAFEGUARDS

A secure online system that lets patients view records, send messages, request appointments, or pay bills. Portal access requires identity proofing, authentication, audit logging, and appropriate privacy controls.

Payment and Remittance Advice 45 CFR §§ 162.1601, 162.1602 ADMINISTRATIVE

The named HIPAA transaction pairing payment (EFT) with the explanation of payment (X12N 835 remittance advice).

Penetration Test 45 CFR §§ 164.308(a)(1)(ii)(A), 164.308(a)(8) SECURITY RULE

Not required by HIPAA. Testing results serve as evidence for the required risk analysis and the periodic technical evaluation standard.

Phishing 45 CFR § 164.308(a)(5) SECURITY RULE

Not named in the regulation. Phishing defenses fall under the security awareness and training standard, including the specification for guarding against, detecting, and reporting malicious software.

Possession Factor TECHNICAL SAFEGUARDS

An authentication factor based on something the user has, such as a hardware key, authenticator app, smart card, or security token. It is commonly paired with a password for MFA.

Premium Payment Transaction 45 CFR § 162.1702 ADMINISTRATIVE

The health plan premium payments transaction, conducted with the adopted ASC X12N 820 standard.

Password Manager 45 CFR § 164.308(a)(5)(ii)(D) TECHNICAL SAFEGUARDS

A tool commonly used to satisfy the addressable password management specification: procedures for creating, changing, and safeguarding passwords.

Patient Access API 45 CFR § 170.315(g)(10) PATIENT RIGHTS

Patient app access to records rides on the standardized API for patient and population services certification criterion; CMS program rules (Title 42) require payers to expose Patient Access APIs built on the same standards.

Patient Estimate 45 CFR § 149.610 ADMINISTRATIVE

The good faith estimate requirement: providers and facilities must give uninsured or self-pay individuals an estimate of expected charges for scheduled items and services, within the section's timeframes and content requirements.

Patient Matching PRIVACY RULE

The process of linking records to the correct individual. Matching errors can cause wrong-record access, disclosure, or clinical safety problems.

Portal Invitation PATIENT RIGHTS

A message inviting a patient to create portal access. It should verify destination details and avoid exposing more PHI than necessary.

Procedure Code 45 CFR § 162.1002 ADMINISTRATIVE

Procedures are reported with the adopted code sets: CPT-4 and HCPCS for physician and other health care services, ICD-10-PCS for inpatient hospital procedures, and CDT for dental services.

PHI Access Review PRIVACY RULE

A privacy-rule concept involving PHI Access Review. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Audit Evidence ENFORCEMENT

A compliance oversight concept involving PHI Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

PHI Policy Review ADMINISTRATIVE

An administrative safeguard concept involving PHI Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving PHI Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Training Record ADMINISTRATIVE

An administrative safeguard concept involving PHI Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving PHI Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

PHI Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving PHI Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

PHI 45 CFR § 160.103 PRIVACY RULE

Protected health information: individually identifiable health information transmitted or maintained in any form or medium (electronic, paper, or oral) by a covered entity or business associate, excluding FERPA education records, certain student treatment records, employment records held by an employer, and records of persons deceased more than 50 years.

PHI Security Control PRIVACY RULE

A privacy-rule concept involving PHI Security Control. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Privacy Workflow PRIVACY RULE

A privacy-rule concept involving PHI Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Retention Check ADMINISTRATIVE

An administrative safeguard concept involving PHI Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Disclosure Log PATIENT RIGHTS

A patient-rights concept involving PHI Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

PHI User Provisioning PRIVACY RULE

A privacy-rule concept involving PHI User Provisioning. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving PHI Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

PHI Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving PHI Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

PHI Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving PHI Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Compliance Calendar PRIVACY RULE

A privacy-rule concept involving PHI Compliance Calendar. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Evidence Packet PRIVACY RULE

A privacy-rule concept involving PHI Evidence Packet. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI System Inventory ADMINISTRATIVE

An administrative safeguard concept involving PHI System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving PHI Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

PHI Claims Transaction PRIVACY RULE

A privacy-rule concept involving PHI Claims Transaction. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Eligibility Workflow PRIVACY RULE

A privacy-rule concept involving PHI Eligibility Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

PHI Patient Request PATIENT RIGHTS

A patient-rights concept involving PHI Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

PHI Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving PHI Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

PHI Exception Register PRIVACY RULE

A privacy-rule concept involving PHI Exception Register. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Qualified Protective Order
45 CFR § 164.512(e)(1)(v) PRIVACY RULE

A court or tribunal order, or a stipulation, that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation and requires return or destruction of the PHI, including copies, at the end of the proceeding.

Quality Improvement
45 CFR § 164.501 PRIVACY RULE

Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, are the first-listed health care operations.

Quality Assurance Review
45 CFR § 164.501 ADMINISTRATIVE

Quality assessment activities are health care operations by definition, permitting use of PHI without authorization under § 164.506.

Query of Records
TECHNICAL SAFEGUARDS

A search or lookup of patient information in an EHR, HIE, or other system. Queries should be tied to a permitted purpose and captured in audit logs.

Queue Management
ADMINISTRATIVE

The workflow for routing access requests, amendment requests, incidents, claims, or privacy tasks to the right owner. Good queue management helps meet HIPAA deadlines and documentation expectations.

Qualified Service Organization Agreement
42 CFR § 2.11 (Title 42, not Title 45) PRIVACY RULE

Part 2's analog to a business associate agreement: the agreement by which a service organization receiving Part 2 records acknowledges it is bound by the Part 2 rules and will resist unauthorized efforts to obtain the records.

Quality Measure
ADMINISTRATIVE

A metric used to assess care, outcomes, safety, or performance. Measures may rely on PHI and should follow minimum necessary and reporting rules.

Query-Based Exchange
TECHNICAL SAFEGUARDS

A health information exchange model where one system searches another for patient records. Access should be tied to identity, purpose, consent rules, and audit logs.

Queued Transaction
TECHNICAL SAFEGUARDS

An electronic transaction waiting to be processed or transmitted. Queues containing PHI need access controls, retention rules, monitoring, and error handling.

Quick Response Procedure
ADMINISTRATIVE

A short incident procedure for urgent privacy or security events. It should identify first actions, escalation contacts, evidence preservation, and breach review triggers.

Quarantine Folder
TECHNICAL SAFEGUARDS

A controlled location where suspicious files, messages, or records are isolated for review. If PHI is present, access and retention still need safeguards.

Quarterly Access Review
TECHNICAL SAFEGUARDS

A scheduled review of user permissions. It helps detect excessive access, stale accounts, role drift, and termination failures before they create incidents.

Quarterly Compliance Review
ADMINISTRATIVE

A recurring review of training, incidents, risks, policies, BAAs, and evidence. It keeps HIPAA work from becoming a once-a-year scramble.

Quarterly Patch Cycle
TECHNICAL SAFEGUARDS

A recurring patch process for lower-risk updates. Critical vulnerabilities affecting ePHI systems may need faster handling outside the routine cycle.

Quarterly Vendor Review
BUSINESS ASSOCIATES

A recurring review of business associates and key vendors. It checks BAA status, incidents, security evidence, subcontractors, and service changes.

Questioned Disclosure
PRIVACY RULE

A disclosure that must be reviewed because its authority, recipient, or minimum necessary scope is unclear. It should be paused or escalated before release when possible.

Quorum for Compliance Committee
ADMINISTRATIVE

The minimum attendance needed for governance decisions to be valid. Defining quorum helps document oversight and accountability for privacy and security decisions.

Quota Management
TECHNICAL SAFEGUARDS

Controls that limit storage, message, or export volume. Quotas can reduce accidental bulk exposure of PHI and support monitoring for abnormal activity.

Quality Control Sample PRIVACY RULE

A limited record sample used to test process accuracy. Samples containing PHI should be minimized, protected, and destroyed when no longer needed.

Qualified Individual ADMINISTRATIVE

A person with appropriate role, authority, or expertise for a specific compliance task. Documentation should show why the individual was assigned.

Qualified Health Plan 45 CFR § 155.20 ADMINISTRATIVE

A health plan that has in effect a certification that it meets the standards of Part 156 Subpart C, issued or recognized by each Exchange through which the plan is offered.

Quality Reporting ADMINISTRATIVE

Submitting care quality or performance data to a payer, registry, or government program. Reports should use minimum necessary data and appropriate agreements.

Questionnaire Response PRIVACY RULE

A completed form from a patient, workforce member, or vendor. Responses may contain PHI, compliance evidence, or security information requiring protection.

Queue Monitoring ADMINISTRATIVE

Reviewing work queues for stuck claims, referrals, faxes, portal messages, or incidents. Queues containing PHI need timely handling and access limits.

Qualified Security Assessor SECURITY RULE

A professional role used in some security assessment programs. It is not a HIPAA-defined certification, but assessor evidence may support broader vendor or control review.

Qualified Access Review SECURITY RULE

An administrative safeguard concept involving Qualified Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Audit Evidence ENFORCEMENT

A compliance oversight concept involving Qualified Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Qualified Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Qualified Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Qualified Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Training Record ADMINISTRATIVE

An administrative safeguard concept involving Qualified Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Qualified Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Qualified Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Qualified Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Qualified PHI Handling PRIVACY RULE

A privacy-rule concept involving Qualified PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Qualified Security Control SECURITY RULE

An administrative safeguard concept involving Qualified Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Qualified Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Qualified Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Qualified Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Qualified Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Qualified User Provisioning SECURITY RULE

An administrative safeguard concept involving Qualified User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Qualified Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Qualified Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Qualified Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Qualified Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Qualified Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Qualified Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Evidence Packet SECURITY RULE

An administrative safeguard concept involving Qualified Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Qualified System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Qualified Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Qualified Claims Transaction SECURITY RULE

An administrative safeguard concept involving Qualified Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Qualified Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Patient Request PATIENT RIGHTS

A patient-rights concept involving Qualified Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Qualified Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Qualified Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Qualified Exception Register SECURITY RULE

An administrative safeguard concept involving Qualified Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Reasonable Cause
45 CFR § 160.401 ENFORCEMENT

An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the entity did not act with willful neglect.

Reasonable Diligence
45 CFR § 160.401 ENFORCEMENT

The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Recognized Security Practices
SECURITY RULE

A 2021 HITECH amendment requiring OCR to consider whether an entity had recognized security practices in place for the prior 12 months when determining fines. Includes NIST Cybersecurity Framework compliance and Section 405(d) of the Cybersecurity Act of 2015. Provides tangible incentive to adopt industry-standard security frameworks.

Record Retention
45 CFR §§ 164.316(b)(2)(i), 164.530(j)(2) ADMINISTRATIVE

Required documentation must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later. This is a documentation retention rule; HIPAA does not set medical record retention periods, which are state law.

Remediation Plan
45 CFR § 164.308(a)(1)(ii)(B) ADMINISTRATIVE

The documented plan for reducing identified risks; it implements the required risk management specification, which calls for measures sufficient to bring risk to a reasonable and appropriate level.

Required by Law (Disclosure)
45 CFR § 164.103 PRIVACY RULE

A mandate contained in law that compels a use or disclosure of PHI and is enforceable in a court of law. Includes court orders and court-ordered warrants; subpoenas or summonses issued by a court, grand jury, inspector general, or authorized administrative body; civil or authorized investigative demands; Medicare conditions of participation; and statutes or regulations requiring production of information, including when payment is sought under a government benefit program.

Required Implementation Specification
45 CFR § 164.306(d)(2) SECURITY RULE

A specification the regulation marks as required must be implemented as written. No assessment, alternative measure, or documentation substitute applies.

Guide: Addressable vs required

Research (HIPAA)
45 CFR § 164.501 PRIVACY RULE

A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Resolution Agreement
ENFORCEMENT

A formal settlement between OCR and an entity resolving a compliance investigation. Typically includes a monetary payment and a corrective action plan. Published on the HHS website as enforcement precedent.

Right of Access
45 CFR § 164.524 PATIENT RIGHTS

The individual's right to inspect and obtain a copy of PHI in a designated record set, excluding psychotherapy notes and litigation-prepared information; in the form and format requested if readily producible; within 30 days with one 30-day extension; for a reasonable, cost-based fee. The entity must also transmit copies to a third party the individual clearly designates in a signed writing.

Guide: Patient rights under HIPAA

Right to Amend
45 CFR § 164.526 PATIENT RIGHTS

The individual's right to have a covered entity amend PHI in a designated record set. The entity acts within 60 days (one 30-day extension) and either makes the amendment and notifies relevant parties, or issues a written denial explaining the basis and the individual's rights.

Right to Request Restrictions
45 CFR § 164.522(a) PATIENT RIGHTS

Individuals may request restrictions on uses and disclosures for treatment, payment, operations, and to persons involved in care. The entity need not agree, except it MUST agree when the disclosure would go to a health plan for payment or operations and the item or service was paid out of pocket in full.

Risk Analysis (SRA) 45 CFR § 164.308(a)(1)(ii)(A) SECURITY RULE

The required specification to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity.

Guide: How to conduct a risk assessment

Risk Management 45 CFR § 164.308(a)(1)(ii)(B) SECURITY RULE

The required specification to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Ransomware 45 CFR §§ 164.304, 164.402 SECURITY RULE

A ransomware encryption of ePHI is a security incident by definition (unauthorized access and interference with system operations), and under OCR guidance it is presumptively a breach of unsecured PHI unless the four-factor assessment demonstrates a low probability of compromise.

Guide: Ransomware: the first 72 hours

Reassociation 45 CFR § 162.1603 ADMINISTRATIVE

Matching an EFT payment to its corresponding 835 remittance advice by trace number, governed by the Phase III CORE 370 Reassociation Rule adopted as an operating rule.

Referral Authorization 45 CFR § 162.1302 ADMINISTRATIVE

The referral certification and authorization transaction, conducted with the adopted ASC X12N 278 standard.

Remote Access TECHNICAL SAFEGUARDS

Access to systems from outside the organization's controlled network. Remote access to ePHI should use MFA, encryption, device controls, logging, and clear workforce rules.

Request for Restriction 45 CFR § 164.522(a) PATIENT RIGHTS

The individual's ask to limit how PHI is used or shared. Optional for the entity to grant, except the mandatory self-pay restriction; once agreed, a restriction binds the entity except in emergencies.

Retaliation Prohibition 45 CFR §§ 164.530(g), 160.316 PATIENT RIGHTS

No intimidation, threats, coercion, discrimination, or other retaliatory action against individuals for exercising Privacy Rule rights, filing a complaint, participating in an investigation or hearing, or opposing an unlawful act or practice in good faith.

Role-Based Access Control (RBAC) 45 CFR § 164.308(a)(4) TECHNICAL SAFEGUARDS

A common method of satisfying information access management: access rights granted by job role, consistent with documented policies for authorizing access to ePHI.

Risk Acceptance 45 CFR §§ 164.308(a)(1)(ii)(B), 164.306(b) SECURITY RULE

A documented decision that a residual risk is at a reasonable and appropriate level, made using the flexibility factors: size, complexity, and capabilities; technical infrastructure; costs; and probability and criticality of the risks.

Risk Register 45 CFR § 164.308(a)(1)(ii)(B) SECURITY RULE

The working inventory of identified risks and their treatment. Not named in the rule, but the standard way entities document that risk management decisions were made and tracked.

Remote Wipe TECHNICAL SAFEGUARDS

A control that deletes managed data from a lost, stolen, or retired device. Remote wipe supports mobile and BYOD protection for ePHI.

Role Change Review 45 CFR § 164.308(a)(4)(ii)(C) ADMINISTRATIVE

Reviewing and modifying a user's right of access when duties change implements the addressable access establishment and modification specification.

Risk Access Review ADMINISTRATIVE

An administrative safeguard concept involving Risk Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Audit Evidence ENFORCEMENT

A compliance oversight concept involving Risk Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Risk Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Risk Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk 45 CFR § 164.308(a)(1)(ii) ADMINISTRATIVE

Not separately defined in the regulation. The Security Rule operationalizes risk through the required risk analysis and risk management specifications: assess threats and vulnerabilities to ePHI, then reduce them to a reasonable and appropriate level.

Risk Training Record ADMINISTRATIVE

An administrative safeguard concept involving Risk Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Risk Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Risk Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Risk Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Risk PHI Handling ADMINISTRATIVE

An administrative safeguard concept involving Risk PHI Handling. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Security Control ADMINISTRATIVE

An administrative safeguard concept involving Risk Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Privacy Workflow ADMINISTRATIVE

An administrative safeguard concept involving Risk Privacy Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Risk Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Risk Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Risk User Provisioning ADMINISTRATIVE

An administrative safeguard concept involving Risk User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Risk Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Risk Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Risk Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Risk Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Risk Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Compliance Calendar ADMINISTRATIVE

An administrative safeguard concept involving Risk Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Evidence Packet ADMINISTRATIVE

An administrative safeguard concept involving Risk Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Risk System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Risk Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Risk Claims Transaction ADMINISTRATIVE

An administrative safeguard concept involving Risk Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Eligibility Workflow ADMINISTRATIVE

An administrative safeguard concept involving Risk Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Patient Request PATIENT RIGHTS

A patient-rights concept involving Risk Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Risk Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Risk Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Risk Exception Register ADMINISTRATIVE

An administrative safeguard concept involving Risk Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

S

Safe Harbor (De-identification)
45 CFR § 164.514(b)(2) PRIVACY RULE

Remove 18 categories of identifiers of the individual and of the individual's relatives, employers, and household members, and have no actual knowledge that the remaining information could be used alone or in combination to identify the individual.

Guide: The 18 HIPAA identifiers

Safeguards
45 CFR §§ 164.530(c), 164.306(a) SECURITY RULE

The Privacy Rule requires appropriate administrative, technical, and physical safeguards to protect PHI from impermissible use or disclosure; the Security Rule's general rules require protecting the confidentiality, integrity, and availability of all ePHI against reasonably anticipated threats and impermissible uses.

Sale of PHI
45 CFR §§ 164.502(a)(5)(ii), 164.508(a)(4) PRIVACY RULE

A covered entity or business associate may not receive direct or indirect remuneration in exchange for PHI, except under an authorization stating that remuneration will result, or within listed exceptions including public health, research (cost-based), treatment and payment, sale of the business, business associate services, individual access fees, and disclosures required by law.

Sanctions Policy
45 CFR §§ 164.308(a)(1)(ii)(C), 164.530(e)(1) ADMINISTRATIVE

Both rules require appropriate sanctions against workforce members who fail to comply with the entity's security or privacy policies and procedures.

Security Awareness and Training
45 CFR § 164.308(a)(5)(i) ADMINISTRATIVE

The required standard to implement a security awareness and training program for all members of the workforce, including management. Its addressable specifications cover security reminders, protection from malicious software, log-in monitoring, and password management.

Guide: Building a training program

Security Incident
45 CFR § 164.304 SECURITY RULE

The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations, in an information system.

Guide: HIPAA incident management guide

Security Management Process
45 CFR § 164.308(a)(1)(i) SECURITY RULE

The required standard to implement policies and procedures to prevent, detect, contain, and correct security violations. Its four implementation specifications are risk analysis, risk management, sanction policy, and information system activity review.

Security Officer
45 CFR § 164.308(a)(2) ADMINISTRATIVE

The security official every covered entity and business associate must identify as responsible for developing and implementing security policies and procedures. In small practices this is often the same person as the Privacy Officer.

Guide: HIPAA compliance officer guide

Security Rule
45 CFR Part 164, Subpart C (§§ 164.302-164.318) SECURITY RULE

The security standards for the protection of electronic protected health information: general rules, administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and documentation requirements, applying to covered entities and business associates.

Guide: Security Rule implementation

Social Media
PRIVACY RULE

HIPAA does not specifically address social media, but the rules apply regardless of platform. Posting patient photos, sharing treatment details, or discussing identifiable patients on social media is a PHI disclosure requiring authorization. Even well-intentioned posts can violate HIPAA.

Guide: HIPAA social media compliance

Standard (Security Rule)
45 CFR § 160.103 SECURITY RULE

A rule, condition, or requirement describing products, systems, services, or practices: classification of components, specification of materials, performance, or operations, or delineation of procedures; or, with respect to the privacy of health information, a rule, condition, or requirement of Subpart E.

Standard Transactions
45 CFR §§ 162.103, 162.923 ADMINISTRATIVE

A transaction that complies with an adopted HIPAA standard. A covered entity conducting a covered transaction with another covered entity using electronic media must conduct it as a standard transaction.

State Attorney General ENFORCEMENT

Under the HITECH Act, state AGs can bring civil actions in federal court on behalf of residents affected by HIPAA violations. Provides an independent enforcement mechanism beyond OCR. Several state AGs have brought actions after large breaches.

Subcontractor 45 CFR § 160.103 BUSINESS ASSOCIATES

A person to whom a business associate delegates a function, activity, or service, other than as a member of the business associate's workforce. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate is itself a business associate.

Substance Use Disorder Records (42 CFR Part 2) 42 CFR Part 2 (Title 42, not Title 45) PRIVACY RULE

Records of federally assisted substance use disorder treatment programs carry protections beyond HIPAA: patient consent requirements for disclosure, limits on redisclosure, and restrictions on use in proceedings against the patient. Within Title 45, such records held by covered entities remain PHI as well.

Guide: OCR and Part 2 enforcement

Sanction Documentation 45 CFR § 164.530(e)(2) ADMINISTRATIVE

Sanctions applied to workforce members must be documented, and the documentation retained under § 164.530(j).

Secure Messaging 45 CFR § 164.312(e)(1) TECHNICAL SAFEGUARDS

Encrypted messaging platforms implement the transmission security standard when ePHI moves between parties over a network.

Guide: Texting patients under HIPAA

Security Questionnaire BUSINESS ASSOCIATES

A vendor or customer questionnaire used to evaluate safeguards, policies, incident response, and compliance posture. It supports due diligence but should be validated against evidence where possible.

Service Level Agreement (SLA) BUSINESS ASSOCIATES

A contract provision defining performance expectations such as uptime, response time, backup recovery, or incident notice. SLAs for PHI vendors should align with contingency and breach response needs.

Shared Responsibility BUSINESS ASSOCIATES

A model dividing security and compliance duties between an organization and its vendor, especially in cloud services. The customer remains responsible for its own configuration, access decisions, and policies.

SOC 2 Report BUSINESS ASSOCIATES

An independent report on a service organization's controls. SOC 2 can support vendor due diligence, but it is not a HIPAA certification and does not replace a BAA.

Secure File Transfer 45 CFR § 164.312(e)(1) TECHNICAL SAFEGUARDS

Encrypted file transfer implements the transmission security standard: guarding against unauthorized access to ePHI moving over an electronic communications network.

Security Exception SECURITY RULE

An approved deviation from a security requirement. Exceptions should be time-limited, risk-rated, and tied to compensating safeguards.

Segregation of Duties ADMINISTRATIVE

A control that separates responsibilities so one person cannot perform conflicting high-risk actions unchecked. It can reduce fraud, misuse, and admin abuse.

Sensitive Diagnosis PRIVACY RULE

A diagnosis that may carry additional stigma or legal protection. Access and disclosure should account for minimum necessary and any stricter state or federal rules.

Security Access Review SECURITY RULE

An administrative safeguard concept involving Security Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Audit Evidence ENFORCEMENT

A compliance oversight concept involving Security Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Security Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Security Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Security Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Training Record ADMINISTRATIVE

An administrative safeguard concept involving Security Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Security Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Security Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Security Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Security PHI Handling PRIVACY RULE

A privacy-rule concept involving Security PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Security 45 CFR § 164.304 SECURITY RULE

Security or security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Security Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Security Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Security Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Security Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Security User Provisioning SECURITY RULE

An administrative safeguard concept involving Security User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Security Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Security Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Security Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Security Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Security Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Security Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Evidence Packet SECURITY RULE

An administrative safeguard concept involving Security Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Security System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Security Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Security Claims Transaction SECURITY RULE

An administrative safeguard concept involving Security Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Security Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Patient Request PATIENT RIGHTS

A patient-rights concept involving Security Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Security Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Security Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Security Exception Register SECURITY RULE

An administrative safeguard concept involving Security Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

T

Technical Assistance
45 CFR § 160.304(b) ENFORCEMENT

The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the administrative simplification provisions.

Technical Safeguards
45 CFR § 164.304 TECHNICAL SAFEGUARDS

The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Guide: The three HIPAA safeguards

Telehealth
TECHNICAL SAFEGUARDS

Delivering healthcare services through electronic communications. HIPAA applies the same way as in-person care. ePHI must be protected during transmission and storage. Telehealth platforms must be HIPAA-compliant and covered by a BAA.

Guide: Telehealth HIPAA compliance

Termination (BAA)
45 CFR § 164.504(e)(1)(ii), (e)(2)(iii) BUSINESS ASSOCIATES

A covered entity that knows of a pattern of activity or practice of its business associate in material breach must take reasonable steps to cure or end the violation, and if unsuccessful, terminate the contract if feasible. The BAA itself must authorize termination for violation of a material term.

TPO (Treatment, Payment, Healthcare Operations)
45 CFR § 164.506 PRIVACY RULE

A covered entity may use or disclose PHI for its own treatment, payment, or health care operations without individual authorization, and for another entity's in stated circumstances. The three terms are defined at § 164.501.

Transaction
45 CFR § 160.103 ADMINISTRATIVE

The transmission of information between two parties to carry out financial or administrative activities related to health care, including health care claims or equivalent encounter information, payment and remittance advice, coordination of benefits, claim status, enrollment and disenrollment, eligibility, premium payments, referral certification and authorization, first report of injury, health claims attachments, EFT and remittance advice, and other transactions the Secretary may prescribe.

Transmission Security
45 CFR § 164.312(e)(1) TECHNICAL SAFEGUARDS

The required standard to implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.

Treatment
45 CFR § 164.501 PRIVACY RULE

The provision, coordination, or management of health care and related services by one or more health care providers, including coordination or management with a third party, consultation between providers relating to a patient, and referral of a patient from one provider to another.

Tabletop Exercise
45 CFR § 164.308(a)(7)(ii)(D) ADMINISTRATIVE

A discussion-based walkthrough used to satisfy the addressable testing and revision specification: periodic testing and revision of contingency plans.

Threat Assessment
45 CFR § 164.308(a)(1)(ii)(A) SECURITY RULE

Identifying reasonably anticipated threats is a component of the required risk analysis of risks and vulnerabilities to ePHI.

Tokenization
TECHNICAL SAFEGUARDS

Replacing sensitive values with tokens that have no useful meaning outside a controlled system. Tokenization may reduce exposure but does not automatically remove HIPAA obligations if re-identification remains possible.

Training Attestation
45 CFR § 164.530(b)(2)(ii) ADMINISTRATIVE

The documentation that required training was provided, retained in written or electronic form under § 164.530(j).

Transaction Standard
45 CFR §§ 162.103, 162.923 ADMINISTRATIVE

The adopted format specification for each named transaction; covered entities conducting those transactions electronically must use the adopted standard.

Telehealth Platform
BUSINESS ASSOCIATES

Software used to provide remote care. If it creates, receives, maintains, or transmits PHI for a covered provider, HIPAA safeguards and often a BAA are required.

Third-Party Administrator 45 CFR § 160.103 BUSINESS ASSOCIATES

A TPA processing or administering claims for a health plan is a business associate; claims processing or administration is the first activity listed in the business associate definition.

Ticketing System TECHNICAL SAFEGUARDS

A support system used to track requests and incidents. If tickets include PHI, the system needs access controls, retention rules, and user guidance.

Treatment Relationship 45 CFR § 164.501 PRIVACY RULE

The Privacy Rule distinguishes direct treatment relationships, where the provider delivers care and results to the individual, from indirect ones, where care is based on another provider's orders and results flow through that provider.

Trusted Contact 45 CFR § 164.510(b) PATIENT RIGHTS

A person the individual identifies for involvement in care or notification; disclosures to them are limited to PHI directly relevant to that involvement, with the individual given the opportunity to agree or object when practicable.

Transport Layer Security 45 CFR § 164.312(e) TECHNICAL SAFEGUARDS

TLS is a standard technology used to meet the transmission security standard and its encryption specification for ePHI in transit.

Termination Checklist 45 CFR § 164.308(a)(3)(ii)(C) ADMINISTRATIVE

The operational artifact implementing the addressable termination procedures specification: terminating access to ePHI when employment or another workforce arrangement ends.

Token Vault TECHNICAL SAFEGUARDS

A controlled store that maps tokens back to sensitive values. A token vault protecting PHI-derived values needs strong access control and monitoring.

Trace Number 45 CFR § 162.1603 ADMINISTRATIVE

The adopted CAQH CORE operating rules include the Phase III CORE 370 EFT and ERA Reassociation Rule, which uses the trace number to let providers match the EFT payment to its 835 remittance advice.

Training Exception ADMINISTRATIVE

A documented reason a workforce member missed, delayed, or received alternate training. Exceptions should be tracked until resolved.

Transmission Log TECHNICAL SAFEGUARDS

A record of messages or files sent between systems. Logs help prove when PHI was sent, where it went, and whether delivery failed.

Treatment Exception 45 CFR § 164.502(b)(2)(i) PRIVACY RULE

The minimum necessary standard does not apply to disclosures to, or requests by, a health care provider for treatment.

Training Access Review ADMINISTRATIVE

An administrative safeguard concept involving Training Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Audit Evidence ENFORCEMENT

A compliance oversight concept involving Training Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Training Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Training Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Training Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training 45 CFR §§ 164.530(b), 164.308(a)(5) ADMINISTRATIVE

The Privacy Rule requires training the workforce on privacy policies as necessary for their functions and documenting it; the Security Rule requires a security awareness and training program for the entire workforce including management.

Training Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Training Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Training Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Training Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Training PHI Handling ADMINISTRATIVE

An administrative safeguard concept involving Training PHI Handling. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Security Control ADMINISTRATIVE

An administrative safeguard concept involving Training Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Privacy Workflow ADMINISTRATIVE

An administrative safeguard concept involving Training Privacy Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Training Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Training Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Training User Provisioning ADMINISTRATIVE

An administrative safeguard concept involving Training User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Training Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Training Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Training Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Training Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Training Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Compliance Calendar ADMINISTRATIVE

An administrative safeguard concept involving Training Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Evidence Packet ADMINISTRATIVE

An administrative safeguard concept involving Training Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Training System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Training Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Training Claims Transaction ADMINISTRATIVE

An administrative safeguard concept involving Training Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Eligibility Workflow ADMINISTRATIVE

An administrative safeguard concept involving Training Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Patient Request PATIENT RIGHTS

A patient-rights concept involving Training Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Training Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Training Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Training Exception Register ADMINISTRATIVE

An administrative safeguard concept involving Training Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique User Identification
45 CFR § 164.312(a)(2)(i) TECHNICAL SAFEGUARDS

The required specification to assign a unique name or number for identifying and tracking user identity.

Unsecured PHI
45 CFR § 164.402 SECURITY RULE

Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through a technology or methodology specified by the Secretary in guidance. Under that guidance, PHI is secured only by encryption meeting the guidance or by destruction; anything else that is lost or impermissibly disclosed triggers breach analysis.

Use (of PHI)
45 CFR § 160.103 PRIVACY RULE

With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of the information WITHIN the entity that maintains it. Movement outside the entity is a disclosure.

Unauthorized Access
45 CFR § 164.304 PRIVACY RULE

Within the definition of security incident: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Unique Identifier
45 CFR §§ 162.406, 162.605 ADMINISTRATIVE

The adopted HIPAA identifiers: the NPI for health care providers and the EIN for employers. No standard unique patient identifier has ever been adopted.

Unstructured Data
SECURITY RULE

Information that does not live in a neatly defined database field, such as PDFs, scanned records, emails, images, notes, and attachments. Unstructured PHI is often missed in risk analysis.

Upcoding
ADMINISTRATIVE

Billing for a higher-level service than was actually provided. It is primarily a fraud and billing compliance issue, but related records and investigations may involve PHI.

User Provisioning
45 CFR § 164.308(a)(4)(ii)(B), (C) TECHNICAL SAFEGUARDS

Granting and documenting access implements the addressable access authorization and access establishment and modification specifications: policies for granting access to ePHI and for establishing, documenting, reviewing, and modifying a user's right of access.

Utilization Review
45 CFR § 164.501 PRIVACY RULE

Named within the definition of payment: utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review.

Unavailability Event
SECURITY RULE

A disruption that prevents access to ePHI or critical systems. It should trigger downtime procedures, contingency plan review, and possible incident documentation.

Unencrypted Device
45 CFR § 164.402 TECHNICAL SAFEGUARDS

A device holding ePHI not encrypted per the HHS guidance holds unsecured PHI; its loss or theft is presumptively a breach unless the four-factor assessment shows a low probability of compromise.

Unified Audit Log
TECHNICAL SAFEGUARDS

A centralized log source that combines events across systems. It helps investigations by connecting identity, device, application, and data-access activity.

Unique User ID Review
TECHNICAL SAFEGUARDS

A check that each workforce member has an individual account instead of shared credentials. Unique IDs support accountability and audit controls.

Unstructured PHI Repository
SECURITY RULE

A folder, shared drive, inbox, or archive containing PHI outside core clinical systems. These repositories are often missed in access reviews and retention plans.

Unsupported Software
SECURITY RULE

Software no longer receiving security updates. Unsupported systems that handle ePHI create risk and usually require upgrade, isolation, or documented compensating controls.

Urgent Care Record PRIVACY RULE

Documentation created during urgent care visits. It is PHI when held by a covered provider and should flow into access, amendment, billing, and retention workflows.

User Acceptance Testing TECHNICAL SAFEGUARDS

Testing performed before a system goes live. For ePHI systems, testing should avoid live PHI unless safeguards and approvals are in place.

User Behavior Analytics TECHNICAL SAFEGUARDS

Security monitoring that detects unusual access patterns. It can help identify snooping, compromised accounts, or abnormal ePHI exports.

Usability Risk SECURITY RULE

A risk created when confusing workflows cause privacy or security mistakes. Poorly designed systems can lead to wrong-patient disclosure, misrouting, or improper access.

Unique Device Identifier 45 CFR § 164.514(b)(2)(i)(M) ADMINISTRATIVE

Device identifiers and serial numbers are a listed safe harbor category to remove. (UDI is also an FDA labeling term; the HIPAA hook is the identifier list.)

Unapproved Application SECURITY RULE

Software used without review or approval. If it stores or transmits PHI, it can create shadow IT risk and missing BAA exposure.

Undeliverable Notice 45 CFR § 164.404(d)(2) ADMINISTRATIVE

When contact information is insufficient or out of date: for fewer than 10 unreachable individuals, an alternative written, phone, or other means; for 10 or more, a conspicuous 90-day website posting or major print or broadcast media notice, plus a toll-free number active for at least 90 days.

Unified Endpoint Management TECHNICAL SAFEGUARDS

A platform for managing laptops, phones, tablets, and other endpoints. UEM can enforce encryption, patches, passcodes, and remote wipe.

Unknown Recipient PRIVACY RULE

A recipient whose identity or authority has not been verified. PHI should not be disclosed until the recipient and purpose are confirmed.

User Deprovisioning 45 CFR § 164.308(a)(3)(ii)(C) TECHNICAL SAFEGUARDS

Removing access for departing or role-changed users; the addressable specification requires procedures for terminating access to ePHI when the employment or other arrangement ends.

Unique Access Review SECURITY RULE

An administrative safeguard concept involving Unique Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Audit Evidence ENFORCEMENT

A compliance oversight concept involving Unique Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Unique Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Unique Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Unique Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Training Record ADMINISTRATIVE

An administrative safeguard concept involving Unique Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Unique Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Unique Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Unique Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Unique PHI Handling PRIVACY RULE

A privacy-rule concept involving Unique PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Unique Security Control SECURITY RULE

An administrative safeguard concept involving Unique Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Unique Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Unique Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Unique Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Unique Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Unique User Provisioning SECURITY RULE

An administrative safeguard concept involving Unique User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Unique Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Unique Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Unique Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Unique Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Unique Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Unique Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Evidence Packet SECURITY RULE

An administrative safeguard concept involving Unique Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Unique System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Unique Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Unique Claims Transaction SECURITY RULE

An administrative safeguard concept involving Unique Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Unique Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Patient Request PATIENT RIGHTS

A patient-rights concept involving Unique Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Unique Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Unique Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Unique Exception Register SECURITY RULE

An administrative safeguard concept involving Unique Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Vendor Management
45 CFR §§ 164.502(e)(1), 164.504(e), 164.308(b) BUSINESS ASSOCIATES

The regulatory core of vendor management: a covered entity may disclose PHI to a business associate only with satisfactory assurances, documented in a BAA, that the vendor will appropriately safeguard the information.

Guide: Our vendor management process

Voluntary Compliance
45 CFR § 160.304(a) ENFORCEMENT

The Secretary will, to the extent practicable and consistent with the enforcement provisions, seek the cooperation of covered entities and business associates in obtaining compliance.

Valid Authorization
45 CFR § 164.508(c) PRIVACY RULE

Core elements: a specific and meaningful description of the information; the persons authorized to make the disclosure; the recipients; the purpose; an expiration date or event; and the individual's signature and date. Required statements cover the right to revoke, treatment or payment conditioning rules, and redisclosure risk. It must be in plain language, and the individual gets a copy.

Vendor Risk Assessment
BUSINESS ASSOCIATES

A review of a vendor's access to PHI, security controls, subcontractors, breach history, and contractual obligations. It helps determine whether a BAA and additional safeguards are required.

Guide: Risk assessing business associates

Version Control
ADMINISTRATIVE

A process for managing changes to policies, procedures, forms, and technical configurations. Version control helps prove which document was in effect at a given time.

Virtual Private Network (VPN)
45 CFR § 164.312(e) TECHNICAL SAFEGUARDS

A VPN tunnel is a common technical measure satisfying the transmission security standard for ePHI crossing open networks.

Vulnerability Scan
45 CFR § 164.308(a)(1)(ii)(A) SECURITY RULE

Not named in the rule; automated scanning is a standard input to the required risk analysis, which must identify technical vulnerabilities affecting ePHI.

Guide: HIPAA vulnerability scanning requirements

Vacated Account
45 CFR § 164.308(a)(3)(ii)(C) TECHNICAL SAFEGUARDS

An account still active after its owner has left, a direct failure of the termination procedures specification calling for ePHI access to end when the workforce arrangement ends.

Validation Rule
TECHNICAL SAFEGUARDS

A rule that checks transaction, form, or data quality before processing. Validation reduces rejected claims, data errors, and misrouted PHI.

Value-Based Care
ADMINISTRATIVE

Payment and delivery models that reward quality, outcomes, or efficiency. Data sharing for these programs often involves PHI and healthcare operations.

Variance Report
ADMINISTRATIVE

A report documenting an exception from expected policy, process, or security behavior. Variance tracking supports investigation and corrective action.

Vaulted Secret
TECHNICAL SAFEGUARDS

A password, key, token, or certificate stored in a controlled secrets vault. Vaulting reduces exposure of credentials that protect ePHI systems.

Vendor Access Review
BUSINESS ASSOCIATES

A review of third-party accounts, portals, integrations, and support access. It helps confirm vendors still need access and that access matches the BAA and contract.

Vendor Breach Notice
45 CFR § 164.410 BUSINESS ASSOCIATES

A business associate must notify the covered entity of a breach of unsecured PHI without unreasonable delay and no later than 60 days from discovery, identifying to the extent possible each individual affected and providing information the covered entity needs for its own notices.

Vendor Exit Plan
BUSINESS ASSOCIATES

A plan for ending a vendor relationship while protecting PHI. It should cover data return, deletion, transition support, access shutdown, and evidence.

Verbal Disclosure
45 CFR § 160.103 PRIVACY RULE

Health information is defined to include information that is oral, not just recorded. Speaking PHI to an unauthorized listener is a disclosure exactly as handing over a document would be.

Virtual Waiting Room TECHNICAL SAFEGUARDS

A telehealth or scheduling feature that queues patients before a visit. It should limit exposure of names, visit reasons, and other PHI to unauthorized users.

Voice Mail Policy PRIVACY RULE

Rules for leaving messages that may include patient information. Policies should define what can be said, when authorization is needed, and how preferences are honored.

Vendor Due Diligence 45 CFR § 164.502(e)(1) BUSINESS ASSOCIATES

Vetting behind the required satisfactory assurances that a vendor receiving PHI will appropriately safeguard it; the assurances themselves must be documented in the BAA.

Vendor Management Program 45 CFR §§ 164.502(e)(1), 164.504(e) BUSINESS ASSOCIATES

The program wrapper around the BAA requirements: identify vendors handling PHI, obtain satisfactory assurances in a compliant BAA, and act on known violations.

Vaccination Record 45 CFR § 164.512(b)(1)(vi) PRIVACY RULE

A covered entity may disclose proof of immunization to a school required by law to have it, with the agreement of a parent, guardian, or other person in loco parentis, or of the individual if an adult or emancipated minor. The agreement may be oral but must be documented.

Vendor Contact Register BUSINESS ASSOCIATES

A maintained list of vendor security, privacy, legal, and support contacts. Current contacts matter during incidents and BAA reviews.

Vendor Evidence Package BUSINESS ASSOCIATES

A set of documents supporting vendor security and compliance review, such as policies, reports, diagrams, attestations, and incident history.

Video Visit Recording PRIVACY RULE

A recording of a telehealth encounter. If retained, it is PHI and needs consent review, access controls, retention rules, and secure storage.

Virtual Desktop TECHNICAL SAFEGUARDS

A remotely delivered desktop environment. Virtual desktops accessing ePHI still need authentication, logging, clipboard controls, and endpoint safeguards.

Vendor Audit Evidence BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Audit Evidence. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Policy Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Policy Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Risk Finding BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Risk Finding. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Training Record BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Training Record. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Incident Log BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Incident Log. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor 45 CFR § 160.103 BUSINESS ASSOCIATES

HIPAA has no vendor category. A vendor that creates, receives, maintains, or transmits PHI for a covered entity is a business associate; one that never touches PHI is outside the rule.

Vendor PHI Handling BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor PHI Handling. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Security Control BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Security Control. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Privacy Workflow BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Privacy Workflow. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Retention Check BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Retention Check. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Vendor Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Vendor User Provisioning BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor User Provisioning. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Encryption Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Encryption Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Backup Test BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Backup Test. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Contingency Task BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Contingency Task. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Compliance Calendar BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Compliance Calendar. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Evidence Packet BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Evidence Packet. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor System Inventory BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor System Inventory. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Vendor Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Vendor Claims Transaction BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Claims Transaction. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Eligibility Workflow BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Eligibility Workflow. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Patient Request PATIENT RIGHTS

A patient-rights concept involving Vendor Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Vendor Workforce Attestation BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Workforce Attestation. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Exception Register BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Exception Register. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Vendor Monitoring Rule BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Vendor Monitoring Rule. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Wall of Shame (HHS Breach Portal)
45 CFR § 164.408 ENFORCEMENT

Breaches affecting 500 or more individuals must be reported to the Secretary contemporaneously with individual notice, and HITECH requires HHS to post them publicly. Breaches under 500 are logged and reported within 60 days after the end of the calendar year.

Willful Neglect
45 CFR § 160.401 ENFORCEMENT

Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. Willful neglect triggers the highest penalty tiers and mandatory investigation.

Workforce
45 CFR § 160.103 ADMINISTRATIVE

Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the entity's direct control, whether or not they are paid by it.

Workforce Training
45 CFR §§ 164.530(b), 164.308(a)(5) ADMINISTRATIVE

Train all workforce members on privacy policies and procedures as necessary and appropriate for their functions: each new member within a reasonable period, and retraining after material changes. The Security Rule separately requires a security awareness and training program. Training must be documented.
Guide: Essential training topics

Workstation Security
45 CFR § 164.310(c) TECHNICAL SAFEGUARDS

The required standard to implement physical safeguards for all workstations that access ePHI, restricting access to authorized users.

Workstation Use
45 CFR § 164.310(b) TECHNICAL SAFEGUARDS

The required standard for policies and procedures specifying the proper functions to be performed, the manner of performance, and the physical attributes of the surroundings of workstations that access ePHI.

Workforce Clearance Procedure
45 CFR § 164.308(a)(3)(ii)(B) ADMINISTRATIVE

The addressable specification to implement procedures to determine that a workforce member's access to ePHI is appropriate.

Workforce Member
45 CFR § 160.103 ADMINISTRATIVE

Any person within the workforce definition: employees, volunteers, trainees, and others under the entity's direct control in the performance of work, paid or unpaid.

Written Acknowledgment
45 CFR § 164.520(c)(2)(ii) PRIVACY RULE

The signed receipt of the Notice of Privacy Practices a direct treatment provider must make a good faith effort to obtain at first service delivery, or document the attempt.

Web Portal
TECHNICAL SAFEGUARDS

An online system where patients, staff, or partners access information. Portals handling PHI need authentication, session controls, encryption, logging, and support procedures.

Webhook
TECHNICAL SAFEGUARDS

An automated message sent from one system to another when an event occurs. Webhooks carrying PHI require secure transport, authentication, logging, and recipient controls.

Weekly Backup Check
TECHNICAL SAFEGUARDS

A recurring confirmation that backups completed and failures were resolved. Backup checks support contingency planning and reduce recovery surprises.

Whistleblower Disclosure
45 CFR § 164.502(j)(1) PRIVACY RULE

A covered entity is not in violation when a workforce member or business associate, in good faith believing the entity engaged in unlawful conduct or care that endangers patients, discloses PHI to a health oversight agency, public health authority, accreditation organization, or an attorney retained to evaluate the whistleblower's options.

White-Glove Onboarding
ADMINISTRATIVE

A guided implementation process for a practice, vendor, or client. For HIPAA, onboarding should include PHI flow mapping, access roles, BAAs, training, and evidence setup.

Workstation Inventory
TECHNICAL SAFEGUARDS

A list of desktops, laptops, tablets, and shared terminals that access ePHI. Inventory supports patching, encryption, location tracking, and disposal controls.

Workstation Use Policy 45 CFR § 164.310(b) TECHNICAL SAFEGUARDS

The written policy implementing the workstation use standard: what workstations that access ePHI may be used for, how, and in what physical surroundings.

Wrong-Patient Error PRIVACY RULE

A documentation, access, or disclosure error involving the wrong individual. It can create patient safety risk and may require privacy incident review.

Wearable Device Data PRIVACY RULE

Information from watches, sensors, or trackers. It may become PHI when collected or maintained by a covered entity or business associate for care or payment.

Workforce Training Log 45 CFR § 164.530(b)(2)(ii) ADMINISTRATIVE

The record proving who was trained and when; the rule requires documenting that training has been provided.

Wrong Recipient Disclosure 45 CFR § 164.402 PRIVACY RULE

Sending PHI to the wrong person is an impermissible disclosure, presumed to be a breach unless the four-factor assessment demonstrates a low probability that the PHI has been compromised.

Website Tracking Pixel PRIVACY RULE

A small tracking technology embedded in a webpage. On healthcare sites, pixels can create privacy risk if they transmit visit or patient-context data.

Whitelisted Domain TECHNICAL SAFEGUARDS

A domain approved for communication, integration, or file exchange. Whitelisting should be paired with verification and ongoing vendor review.

Wireless Intrusion Detection TECHNICAL SAFEGUARDS

Monitoring that detects unauthorized or suspicious wireless activity. It can help protect networks supporting ePHI systems.

Workflow Audit ADMINISTRATIVE

A review of how information moves through a business process. Workflow audits can reveal unnecessary PHI exposure, missing safeguards, and inefficient handoffs.

Workgroup Permission TECHNICAL SAFEGUARDS

Access granted to a shared group rather than an individual. Workgroup permissions should be reviewed so membership changes do not silently expand PHI access.

Workforce Access Review ADMINISTRATIVE

An administrative safeguard concept involving Workforce Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Audit Evidence ENFORCEMENT

A compliance oversight concept involving Workforce Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Workforce Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Workforce Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Workforce Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Training Record ADMINISTRATIVE

An administrative safeguard concept involving Workforce Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Workforce Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Workforce Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Workforce Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Workforce PHI Handling ADMINISTRATIVE

An administrative safeguard concept involving Workforce PHI Handling. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Security Control ADMINISTRATIVE

An administrative safeguard concept involving Workforce Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Privacy Workflow ADMINISTRATIVE

An administrative safeguard concept involving Workforce Privacy Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Workforce Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Workforce Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Workforce User Provisioning ADMINISTRATIVE

An administrative safeguard concept involving Workforce User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Workforce Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Workforce Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Workforce Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Workforce Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Workforce Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Compliance Calendar ADMINISTRATIVE

An administrative safeguard concept involving Workforce Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Evidence Packet ADMINISTRATIVE

An administrative safeguard concept involving Workforce Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Workforce System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Workforce Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Workforce Claims Transaction ADMINISTRATIVE

An administrative safeguard concept involving Workforce Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Eligibility Workflow ADMINISTRATIVE

An administrative safeguard concept involving Workforce Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Patient Request PATIENT RIGHTS

A patient-rights concept involving Workforce Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Workforce Exception Register ADMINISTRATIVE

An administrative safeguard concept involving Workforce Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Workforce Monitoring Rule ADMINISTRATIVE

An administrative safeguard concept involving Workforce Monitoring Rule. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

X

X12 45 CFR § 162.920 ADMINISTRATIVE

The ASC X12 standards and Technical Reports Type 3 adopted for HIPAA transactions are incorporated by reference at § 162.920, which lists each adopted X12 implementation specification.

X12N 45 CFR § 162.920 ADMINISTRATIVE

The insurance subcommittee of ASC X12 whose Technical Reports Type 3 (TR3s) define most adopted HIPAA transaction standards, incorporated by reference at § 162.920.

X.509 Certificate TECHNICAL SAFEGUARDS

A digital certificate used to support identity verification and encrypted communication. Certificates can help secure APIs, portals, VPNs, and other systems that transmit ePHI.

XML Payload TECHNICAL SAFEGUARDS

Structured data encoded in XML for exchange between systems. XML payloads containing PHI require the same access, transmission, logging, and retention safeguards as other ePHI.

XDR (Extended Detection and Response) TECHNICAL SAFEGUARDS

Security technology that correlates alerts across endpoints, networks, email, cloud, and identity systems. XDR can improve detection and response for threats to ePHI.

XDM (Cross-Enterprise Document Media Interchange) TECHNICAL SAFEGUARDS

A health information exchange profile for moving clinical documents using physical or electronic media. When documents identify patients, HIPAA safeguards still apply.

XDS (Cross-Enterprise Document Sharing) TECHNICAL SAFEGUARDS

A health information exchange profile for sharing clinical documents across organizations. Access controls, audit trails, and permitted-purpose rules remain important when PHI is exchanged.

X12 270 Eligibility Inquiry 45 CFR § 162.1202 ADMINISTRATIVE

The adopted standard for the eligibility for a health plan inquiry: ASC X12N 270, with NCPDP standards for retail pharmacy.

X12 271 Eligibility Response 45 CFR § 162.1202 ADMINISTRATIVE

The adopted standard for the eligibility for a health plan response: ASC X12N 271.

X12 276 Claim Status Request 45 CFR § 162.1402 ADMINISTRATIVE

The adopted standard for the health care claim status request: ASC X12N 276.

X12 277 Claim Status Response 45 CFR § 162.1402 ADMINISTRATIVE

The adopted standard for the health care claim status response: ASC X12N 277.

X12 278 Referral Authorization 45 CFR § 162.1302 ADMINISTRATIVE

The adopted standard for the referral certification and authorization transaction: ASC X12N 278, with NCPDP standards for retail pharmacy.

X12 820 Premium Payment 45 CFR § 162.1702 ADMINISTRATIVE

The adopted standard for the health plan premium payments transaction: ASC X12N 820.

X12 834 Enrollment Transaction 45 CFR § 162.1502 ADMINISTRATIVE

The adopted standard for enrollment and disenrollment in a health plan: ASC X12N 834.

X12 835 Remittance Advice 45 CFR § 162.1602 ADMINISTRATIVE

The adopted standard for the health care payment and remittance advice transaction: ASC X12N 835.

X12 837 Claim 45 CFR § 162.1102 ADMINISTRATIVE

The adopted standard for the health care claims or equivalent encounter information transaction: the ASC X12N 837 professional, institutional, and dental implementations, plus the NCPDP standards for retail pharmacy drug claims.

XACML Policy TECHNICAL SAFEGUARDS

An access-control policy language used to express authorization rules. It can support fine-grained decisions for systems that manage sensitive health data.

XDR Alert Triage SECURITY RULE

The process of reviewing correlated security alerts from an XDR platform. Triage should determine scope, affected systems, PHI exposure, and escalation needs.

XHTML Clinical Document TECHNICAL SAFEGUARDS

A web-compatible document format sometimes used in clinical exchange contexts. If it identifies a patient, it should be treated as PHI.

XML Encryption TECHNICAL SAFEGUARDS

A standard for encrypting XML content. It can protect structured healthcare payloads, but key management and transport security remain necessary.

X12 999 Acknowledgment ADMINISTRATIVE

A standard acknowledgment used to report whether a transaction file was received and syntactically accepted. It supports transaction troubleshooting.

X12 Companion Guide 45 CFR § 162.915 ADMINISTRATIVE

Companion guides operate under trading partner agreements, which may not change a data element or segment definition, condition, or use, add elements or segments, use unadopted codes, or change the meaning or intent of the adopted implementation specification.

X12 Trading Partner 45 CFR §§ 160.103, 162.915 ADMINISTRATIVE

A party exchanging standard transactions under a trading partner agreement (defined at § 160.103 as an agreement related to the exchange of information in electronic transactions); § 162.915 limits what such agreements may modify.

XDR Playbook SECURITY RULE

A documented response workflow for alerts from extended detection and response tools. Playbooks should include PHI exposure checks and escalation criteria.

XML Schema Validation TECHNICAL SAFEGUARDS

Checking an XML payload against an expected schema. Validation helps reject malformed healthcare data before it disrupts workflows or exposes information.

X12 Access Review SECURITY RULE

A healthcare transaction standard term related to X12 Access Review. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Audit Evidence ENFORCEMENT

A healthcare transaction standard term related to X12 Audit Evidence. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Policy Review ADMINISTRATIVE

A healthcare transaction standard term related to X12 Policy Review. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Risk Finding ADMINISTRATIVE

A healthcare transaction standard term related to X12 Risk Finding. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Training Record ADMINISTRATIVE

A healthcare transaction standard term related to X12 Training Record. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Incident Log TECHNICAL SAFEGUARDS

A healthcare transaction standard term related to X12 Incident Log. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Vendor Review BUSINESS ASSOCIATES

A healthcare transaction standard term related to X12 Vendor Review. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 PHI Handling PRIVACY RULE

A healthcare transaction standard term related to X12 PHI Handling. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Security Control SECURITY RULE

A healthcare transaction standard term related to X12 Security Control. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Privacy Workflow PRIVACY RULE

A healthcare transaction standard term related to X12 Privacy Workflow. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Retention Check ADMINISTRATIVE

A healthcare transaction standard term related to X12 Retention Check. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Disclosure Log PATIENT RIGHTS

A healthcare transaction standard term related to X12 Disclosure Log. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 User Provisioning SECURITY RULE

A healthcare transaction standard term related to X12 User Provisioning. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Encryption Review TECHNICAL SAFEGUARDS

A healthcare transaction standard term related to X12 Encryption Review. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Backup Test TECHNICAL SAFEGUARDS

A healthcare transaction standard term related to X12 Backup Test. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Contingency Task ADMINISTRATIVE

A healthcare transaction standard term related to X12 Contingency Task. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Compliance Calendar SECURITY RULE

A healthcare transaction standard term related to X12 Compliance Calendar. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Evidence Packet SECURITY RULE

A healthcare transaction standard term related to X12 Evidence Packet. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 System Inventory ADMINISTRATIVE

A healthcare transaction standard term related to X12 System Inventory. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Authorization Workflow PATIENT RIGHTS

A healthcare transaction standard term related to X12 Authorization Workflow. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Claims Transaction SECURITY RULE

A healthcare transaction standard term related to X12 Claims Transaction. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Eligibility Workflow SECURITY RULE

A healthcare transaction standard term related to X12 Eligibility Workflow. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Patient Request PATIENT RIGHTS

A healthcare transaction standard term related to X12 Patient Request. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Workforce Attestation ADMINISTRATIVE

A healthcare transaction standard term related to X12 Workforce Attestation. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

X12 Exception Register SECURITY RULE

A healthcare transaction standard term related to X12 Exception Register. In a HIPAA program, it helps teams understand how eligibility, claims, remittance, enrollment, or payment data moves between covered entities, clearinghouses, and payers.

Y

Year-End Risk Review ADMINISTRATIVE

A scheduled review of risk analysis results, unresolved remediation items, incidents, vendor changes, and policy updates before the next compliance cycle.

Yielded Access TECHNICAL SAFEGUARDS

Access temporarily delegated or transferred to another authorized person, such as coverage during leave. It should be documented and removed when the need ends.

YubiKey TECHNICAL SAFEGUARDS

A hardware security key commonly used as a possession factor for MFA. Hardware keys can reduce phishing risk for systems that access ePHI.

Youth Health Records PATIENT RIGHTS

Health records involving minors. HIPAA usually treats a parent or guardian as the personal representative, but exceptions can apply for minor consent, abuse, or state law.

Year-to-Date Deductible ADMINISTRATIVE

The amount of deductible a member has accumulated during the plan year. It appears in eligibility and benefits workflows and is PHI when tied to a person.

Yearly BAA Review BUSINESS ASSOCIATES

A scheduled review of business associate agreements and vendor relationships. It helps catch missing contracts, outdated contacts, and changed PHI workflows.

Yearly Policy Review 45 CFR §§ 164.306(e), 164.308(a)(8) ADMINISTRATIVE

The rule sets no annual cycle; it requires security measures to be reviewed and modified as needed to continue reasonable and appropriate protection, and periodic evaluation against the standards.

Yearly Risk Analysis 45 CFR § 164.308(a)(1)(ii)(A) SECURITY RULE

The risk analysis requirement itself states no frequency; HHS guidance treats it as an ongoing process, and annual refresh is common practice rather than regulatory text.

Yellow Alert ADMINISTRATIVE

An internal status for elevated concern that does not yet meet incident severity. Defined alert levels help workforce members escalate privacy or security issues consistently.

Yield Management in Scheduling PRIVACY RULE

Operational management of appointment capacity. Scheduling data can reveal care relationships and should be handled as PHI when linked to patients.

Youth Consent Rule 45 CFR § 164.502(g)(3) PATIENT RIGHTS

When state or other law lets a minor consent to their own care, the parent is not automatically the personal representative for that care; state law controls parental access, and where state law is silent, the provider has documented discretion.

Youth Portal Access PATIENT RIGHTS

Patient portal access for minors and guardians. It needs careful configuration because adolescent consent, proxy access, and state law can conflict.

Youth Privacy Exception 45 CFR § 164.502(g)(3), (g)(5) PATIENT RIGHTS

Parental access can be limited when the minor lawfully consented to the care, when confidentiality was agreed, or when the provider reasonably believes the personal representative situation involves abuse, neglect, or endangerment.

YAML Configuration TECHNICAL SAFEGUARDS

A structured configuration format often used for infrastructure and applications. YAML files should not store PHI or secrets unless protected by strong controls.

YARA Rule TECHNICAL SAFEGUARDS

A malware detection rule used by security teams. YARA can support detection of threats targeting systems that process or store ePHI.

Year-End Access Cleanup TECHNICAL SAFEGUARDS

A scheduled removal of stale users, excessive roles, and abandoned groups. Cleanup supports least privilege before the next compliance cycle.

Year-End Vendor Attestation BUSINESS ASSOCIATES

A documented request for key vendors to confirm controls, incidents, subcontractors, and contact details. It supports ongoing business associate oversight.

Youth Behavioral Health Record PATIENT RIGHTS

Mental or behavioral health documentation involving a minor. Access and disclosure may be affected by minor consent, state law, and safety concerns.

Youth Immunization Record 45 CFR § 164.512(b)(1)(vi) PRIVACY RULE

Proof of immunization may go to a school legally required to have it with a documented agreement from a parent, guardian, person acting in loco parentis, or the emancipated or adult individual.

Youth Proxy Access 45 CFR § 164.502(g)(3) PATIENT RIGHTS

Portal proxy access for parents tracks personal representative status: full access while the parent is the minor's personal representative, restricted for minor-consented services where state law limits parental access.

Yearly Training Plan ADMINISTRATIVE

A schedule for required and role-specific privacy or security training. It should account for new hires, annual refreshers, and policy changes.

Youth Access Restriction PATIENT RIGHTS

A limit on access to a minor's records based on consent rules, safety concerns, or law. Restrictions should be configured consistently across portals and workflows.

Youth Confidential Visit PRIVACY RULE

A visit where a minor may have confidentiality rights under state law. Records and portal access should reflect the applicable privacy rule.

Youth Record Segmentation TECHNICAL SAFEGUARDS

Separating sensitive minor records or data elements so access can be managed correctly. Segmentation helps avoid inappropriate proxy disclosure.

Youth Release Authorization PATIENT RIGHTS

An authorization involving a minor's records. Validity depends on who may sign under HIPAA, state law, and the service involved.

Year-End Access Review SECURITY RULE

An administrative safeguard concept involving Year-End Access Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Audit Evidence ENFORCEMENT

A compliance oversight concept involving Year-End Audit Evidence. It helps organizations prepare for complaints, audits, investigations, corrective action, and documentation requests.

Year-End Policy Review ADMINISTRATIVE

An administrative safeguard concept involving Year-End Policy Review. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Risk Finding ADMINISTRATIVE

An administrative safeguard concept involving Year-End Risk Finding. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Training Record ADMINISTRATIVE

An administrative safeguard concept involving Year-End Training Record. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Incident Log TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Year-End Incident Log. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Year-End Vendor Review BUSINESS ASSOCIATES

A vendor and business associate oversight concept involving Year-End Vendor Review. It helps covered entities track third-party responsibilities, contract expectations, PHI handling, and follow-up evidence.

Year-End PHI Handling PRIVACY RULE

A privacy-rule concept involving Year-End PHI Handling. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Year-End Security Control SECURITY RULE

An administrative safeguard concept involving Year-End Security Control. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Privacy Workflow PRIVACY RULE

A privacy-rule concept involving Year-End Privacy Workflow. It helps teams decide when PHI may be used, disclosed, limited, corrected, retained, or shared.

Year-End Retention Check ADMINISTRATIVE

An administrative safeguard concept involving Year-End Retention Check. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Disclosure Log PATIENT RIGHTS

A patient-rights concept involving Year-End Disclosure Log. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Year-End User Provisioning SECURITY RULE

An administrative safeguard concept involving Year-End User Provisioning. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Encryption Review TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Year-End Encryption Review. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Year-End Backup Test TECHNICAL SAFEGUARDS

A technical safeguard or security operations concept involving Year-End Backup Test. It helps protect ePHI through controlled access, monitoring, encryption, logging, or system configuration.

Year-End Contingency Task ADMINISTRATIVE

An administrative safeguard concept involving Year-End Contingency Task. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Compliance Calendar SECURITY RULE

An administrative safeguard concept involving Year-End Compliance Calendar. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Evidence Packet SECURITY RULE

An administrative safeguard concept involving Year-End Evidence Packet. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End System Inventory ADMINISTRATIVE

An administrative safeguard concept involving Year-End System Inventory. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Authorization Workflow PATIENT RIGHTS

A patient-rights concept involving Year-End Authorization Workflow. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Year-End Claims Transaction SECURITY RULE

An administrative safeguard concept involving Year-End Claims Transaction. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Eligibility Workflow SECURITY RULE

An administrative safeguard concept involving Year-End Eligibility Workflow. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Patient Request PATIENT RIGHTS

A patient-rights concept involving Year-End Patient Request. It helps covered entities handle individual requests, disclosures, notices, or corrections consistently while protecting PHI.

Year-End Workforce Attestation ADMINISTRATIVE

An administrative safeguard concept involving Year-End Workforce Attestation. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Year-End Exception Register SECURITY RULE

An administrative safeguard concept involving Year-End Exception Register. It helps healthcare organizations document policies, workforce responsibilities, risk decisions, and compliance evidence.

Z

50 TERMS

Zero Trust Architecture SECURITY RULE

A security model that continuously verifies users, devices, access, and context rather than assuming internal network traffic is trusted. It can support least privilege and stronger ePHI protection.

Zero-Day Vulnerability SECURITY RULE

A software flaw unknown to the vendor or without an available patch. Organizations should use layered safeguards, monitoring, and incident response to reduce exposure.

Zombie Account 45 CFR § 164.308(a)(3)(ii)(C) TECHNICAL SAFEGUARDS

A forgotten active account belonging to a departed user; evidence the termination procedures specification is not operating.

Zeroization TECHNICAL SAFEGUARDS

Securely erasing keys or sensitive data from memory or storage. Zeroization supports disposal, media reuse, and incident containment.

ZIP Code Identifier 45 CFR § 164.514(b)(2)(i)(B) PRIVACY RULE

Safe harbor requires removing all geographic subdivisions smaller than a state, except the initial three digits of a ZIP code when the three-digit area contains more than 20,000 people; for areas of 20,000 or fewer, the three digits become 000.

Zone-Based Firewall TECHNICAL SAFEGUARDS

A firewall design that applies rules between network zones. It can isolate ePHI systems from guest, administrative, or vendor networks.

Zero Standing Privilege TECHNICAL SAFEGUARDS

A privileged access model where elevated rights are not continuously assigned. Users request time-limited privilege when needed, reducing account compromise risk.

ZTNA TECHNICAL SAFEGUARDS

Zero Trust Network Access, a model that grants application access based on identity, device posture, and context. It can replace broad VPN access for ePHI systems.

Zoned Backup Storage TECHNICAL SAFEGUARDS

Backup storage separated by trust level, geography, or function. Zoning can protect clean backups from ransomware and administrative mistakes.

Zip File Handling TECHNICAL SAFEGUARDS

Rules for creating, sending, receiving, scanning, and extracting compressed files. ZIP archives containing PHI need encryption, recipient verification, and malware controls.

Zero-Touch Provisioning TECHNICAL SAFEGUARDS

Automated device setup that applies security settings before first use. It can help enforce encryption, passcodes, and managed apps on devices accessing ePHI.

Zone Transfer SECURITY RULE

A DNS operation that can expose domain records if misconfigured. Attackers can use exposed records to map healthcare systems and target services.

Zombie Vendor Account 45 CFR §§ 164.308(a)(3)(ii)(C), 164.504(e)(2)(ii)(J) BUSINESS ASSOCIATES

A vendor account that outlived the vendor relationship. Termination procedures and the BAA obligation to return or destroy PHI at contract termination both point at closing it.

Z-Score Outlier PRIVACY RULE

A statistical signal that a value is unusual compared with a population. In healthcare analytics, small or unusual groups may increase re-identification risk.

Zero-Day Response Plan SECURITY RULE

A plan for responding when a critical vulnerability has no patch. It should define monitoring, isolation, compensating controls, vendor contact, and leadership escalation.

Zero Trust Segmentation SECURITY RULE

A segmentation approach that limits access between users, workloads, and applications based on identity and context. It reduces lateral movement toward ePHI systems.

Zone Isolation TECHNICAL SAFEGUARDS

Separating systems into controlled zones so a compromise in one area does not automatically expose ePHI elsewhere.

Zip Bomb TECHNICAL SAFEGUARDS

A malicious compressed file that expands massively when opened. Email and upload workflows should scan archives before they reach systems handling PHI.

Zonal Recovery SECURITY RULE

Restoring systems by network, application, or business zone after an incident. Zonal recovery can prioritize critical care and ePHI access functions.

Zero-Privilege Baseline TECHNICAL SAFEGUARDS

A starting access model where users receive no permissions until a role-based need is approved. It supports least privilege for ePHI systems.

Zero Trust Policy Engine TECHNICAL SAFEGUARDS

A component that evaluates identity, device, context, and policy before granting access. It supports finer control than broad network trust.

Zero-Day Advisory SECURITY RULE

A notice about a newly discovered vulnerability without a complete fix. Advisories should trigger risk review for affected ePHI systems.

Zipped Record Export PRIVACY RULE

A compressed package of records produced for transfer or release. Exports containing PHI should be encrypted, verified, and tracked.

Zone-Based Access TECHNICAL SAFEGUARDS

Access that changes based on network, device, location, or trust zone. It can reduce exposure when users connect from unmanaged environments.

Zonal Incident Containment SECURITY RULE

Containing an incident within a defined network or application zone. It helps preserve critical clinical functions and limit ePHI exposure.

Zero Trust Access Review TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Access Review. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Audit Evidence ENFORCEMENT

A security operations term for Zero Trust Audit Evidence. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Policy Review TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Policy Review. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Risk Finding TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Risk Finding. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Training Record TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Training Record. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Incident Log TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Incident Log. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Vendor Review BUSINESS ASSOCIATES

A security operations term for Zero Trust Vendor Review. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust PHI Handling TECHNICAL SAFEGUARDS

A security operations term for Zero Trust PHI Handling. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Security Control TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Security Control. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Privacy Workflow TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Privacy Workflow. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Retention Check TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Retention Check. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Disclosure Log PATIENT RIGHTS

A security operations term for Zero Trust Disclosure Log. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust User Provisioning TECHNICAL SAFEGUARDS

A security operations term for Zero Trust User Provisioning. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Encryption Review TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Encryption Review. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Backup Test TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Backup Test. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Contingency Task TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Contingency Task. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Compliance Calendar TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Compliance Calendar. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Evidence Packet TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Evidence Packet. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust System Inventory TECHNICAL SAFEGUARDS

A security operations term for Zero Trust System Inventory. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Authorization Workflow PATIENT RIGHTS

A security operations term for Zero Trust Authorization Workflow. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Claims Transaction TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Claims Transaction. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Eligibility Workflow TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Eligibility Workflow. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Patient Request PATIENT RIGHTS

A security operations term for Zero Trust Patient Request. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Workforce Attestation TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Workforce Attestation. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

Zero Trust Exception Register TECHNICAL SAFEGUARDS

A security operations term for Zero Trust Exception Register. It supports HIPAA safeguards by reducing implicit trust, limiting access to ePHI, and documenting how systems are protected and reviewed.

A term is the easy part.

Knowing what it obligates your practice to do is the real work.
That is what One Guy Consulting is for.

oneguyconsulting.com · hello@oneguyconsulting.com