Kyūdō

SOVEREIGNTY-GRADE AI · GRC

HIPAA Compliance Automation Guide

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · READ THIS FIRST

HIPAA is federal law. Automation is what makes it operable at scale.

HIPAA is unlike the other compliance regimes most organizations operate against. It is not a voluntary framework like NIST CSF, not a commercial standard like SOC 2 or ISO 27001, not a contractual requirement like CMMC. It is federal law, codified at 45 CFR Parts 160 and 164, enforced by the HHS Office for Civil Rights (OCR), with civil monetary penalties up to $2,134,831 per violation category per year (2026 adjusted) and criminal penalties up to ten years imprisonment for knowing violations of the most serious kind. There is no certification body. There is no audit firm that issues an opinion. There are OCR investigators, OCR audits, OCR resolution agreements, and — increasingly — state attorneys general bringing parallel actions under HIPAA's enforcement provisions.

HIPAA is also unlike those other regimes in another important way: it is currently bifurcated. The Security Rule that has governed regulated entities since 2003 (last meaningfully updated in 2013) remains the operative law in April 2026. But on January 6, 2025, OCR published a Notice of Proposed Rulemaking (NPRM) that would substantially overhaul the Security Rule — the first major rewrite in over a decade. As of April 2026, the NPRM remains on the OCR regulatory agenda for finalization in May 2026. If the rule is finalized as proposed, regulated entities will have 240 days from publication to comply with materially more prescriptive cybersecurity requirements: technology asset inventories, network maps, mandatory encryption, mandatory MFA, written verification from business associates, annual compliance audits, 72-hour disaster recovery, 15- to 30-day patch deployment SLAs.

This guide is built for organizations operating in this dual reality. Sections 2 and 3 cover what HIPAA requires today. Section 5 covers what the NPRM proposes. The recommendation throughout is unambiguous: prepare against the NPRM. Most of what the NPRM mandates was already implicitly required by the existing Security Rule's risk analysis obligation — OCR consistently cites the failure to implement these controls as evidence of inadequate risk analysis. Building toward the proposed standards now reduces both current OCR enforcement exposure and future remediation cost when the final rule arrives.

This guide is for the Microsoft 365 + Azure customer

HIPAA applies to any covered entity (health plans, health care clearinghouses, most health care providers) and any business associate (anyone who creates, receives, maintains, or transmits ePHI on behalf of a covered entity). This guide focuses on automation for organizations on the Microsoft 365 and Azure stack — the most common deployment pattern in U.S. healthcare.

Microsoft 365 includes a HIPAA Business Associate Agreement (BAA) by default for all U.S. tenants. Azure includes a BAA by default for the in-scope services listed in the Microsoft

> Online Services BAA. The BAA is necessary but not sufficient — it transfers the contractual obligation to Microsoft for the services Microsoft operates, but the customer remains responsible for configuration, access control, identity, monitoring, and every Security Rule safeguard that operates within the customer's tenant.

Sections of this guide: 1 establishes the regulatory landscape; 2 covers covered entities and business associates; 3 walks the current Security Rule by safeguard category; 4 covers the OCR-mandated Risk Analysis — the single most-cited deficiency in HIPAA enforcement; 5 covers the NPRM proposed changes; 6 covers Breach Notification; 7 maps each safeguard category to specific Microsoft Security stack signal sources; 8 is the Kyūdō continuous-readiness model. Appendices include the complete safeguard matrix, OCR enforcement priorities, and authoritative sources.

01 · FOUNDATIONS

The three rules, the two regulations, the one law.

HIPAA — the Health Insurance Portability and Accountability Act of 1996 — is the underlying statute. The operational compliance obligations come from a set of regulations promulgated by HHS: the Privacy Rule (45 CFR Part 164 Subpart E), the Security Rule (Subpart C), the Breach Notification Rule (Subpart D), and the Enforcement Rule (45 CFR Part 160 Subparts C–E). Together with the HITECH Act amendments of 2009 — which extended direct liability to business associates and substantially increased penalties — these constitute the operational HIPAA regime.

The current state of each rule

Rule	Current operational status (April 2026)
Privacy Rule (Subpart E)	In effect. The 2024 Reproductive Health Privacy Rule was vacated nationally by the U.S. District Court for the Northern District of Texas on June 18, 2025; the broader 2024 Privacy Rule changes related to Notice of Privacy Practices (NPP) for Part 2 alignment remain in effect with compliance required by February 16, 2026.
Security Rule (Subpart C)	In effect; last meaningfully revised in 2013 (HIPAA Omnibus Rule). Subject to the January 6, 2025 NPRM proposing substantial modifications. OCR regulatory agenda lists final rule for May 2026.
Breach Notification Rule (Subpart D)	In effect; 60-day notification window for breaches affecting 500 or more individuals; annual reporting for smaller breaches.

Rule	Current operational status (April 2026)
Enforcement Rule (Part 160)	In effect; civil penalty tiers updated annually for inflation. 2026 maximums: $137 per violation (Tier 1) up to $2,134,831 per violation category per year (Tier 4).
Part 2 alignment (42 CFR Part 2)	Final rule effective April 16, 2024; full compliance required by February 16, 2026 — already past as of this guide. Substance use disorder records now better aligned with HIPAA disclosure permissions.

Sources — HHS OCR Regulatory Initiatives page; 45 CFR Parts 160 and 164; HIPAA Journal HIPAA Updates 2026.

Why the NPRM matters even before finalization

The Security Rule NPRM is the most consequential pending change in U.S. healthcare cybersecurity regulation. If finalized, it would shift the Security Rule from a flexible, risk-based framework with 'required' and 'addressable' implementation specifications to a prescriptive framework where every implementation specification is mandatory. The proposed rule eliminates the addressable/required distinction entirely. It adds new standards — technology asset inventory, network mapping, patch management, compliance audits — that have no current Security Rule analog. It imposes specific time-bound obligations: terminate access within one hour of separation, restore critical systems within 72 hours, deploy critical patches within 15 days.

The bipartisan support for healthcare cybersecurity strengthening, the May 2026 finalization on the OCR agenda, and the consistency of the proposed requirements with NIST Cybersecurity Framework v2.0 and the HHS Cybersecurity Performance Goals all suggest the NPRM is more likely than not to be finalized in some form. Regulated entities that are sized and resourced to make material cybersecurity investments should plan against the NPRM, not against the current rule.

If the NPRM is finalized in May 2026

Effective date: 60 days after publication. Compliance date: 180 days after the effective date — 240 days from publication total. Business associate agreement transition: earlier of BAA renewal after the compliance date or one year after the effective date.

Practical implication: a May 2026 final rule means an effective date around July 2026, a compliance date around January 2027. Organizations not currently meeting the proposed standards should be in active remediation now — January 2027 is closer than it appears once you account for budget cycles, vendor procurement, and tenant configuration timelines.

02 · WHO IS COVERED

Covered entities, business associates, and the chain of liability.

HIPAA's regulatory perimeter is defined by the relationships between three categories of entity: covered entities (CEs), business associates (BAs), and subcontractors. Knowing which category you are in determines what you must do; knowing which category every party you exchange ePHI with is in determines what they must do, and what your contractual obligations to them are.

Covered entities

Three categories of organization are covered entities under HIPAA: health plans (insurers, HMOs, government health programs, employer-sponsored group health plans of more than 50 participants), health care clearinghouses (organizations that process nonstandard health information into a standard format), and most health care providers (anyone who furnishes, bills for, or receives payment for health care in the normal course of business AND transmits any health information in electronic form in connection with a HIPAA-standardized transaction).

The third category catches most providers because nearly all providers electronically submit claims, eligibility queries, or referrals to insurers. A solo practitioner who bills cash-only and never electronically transmits any standardized transaction is technically not a covered entity. Any provider that uses EDI for any HIPAA-standardized transaction — including any provider that uses a clearinghouse, any provider whose EHR submits claims, any provider whose practice management system queries eligibility — is a covered entity.

Business associates

A business associate is any person or entity (other than a member of the workforce) that creates, receives, maintains, or transmits protected health information on behalf of a covered entity, or that performs a function or activity involving the use or disclosure of PHI on behalf of a covered entity. The HITECH Act of 2009 made business associates directly liable for Security Rule compliance and most Privacy Rule provisions — BAs are no longer merely contractually obligated, they are regulated entities subject to OCR enforcement.

Common BA categories	Typical examples
Cloud service providers	Microsoft Azure / Microsoft 365 (with BAA), AWS (with BAA), Google Cloud (with BAA), specialized HIPAA-compliant hosting providers.
Software-as-a-Service vendors	Electronic health record vendors, practice management systems, telehealth platforms, billing services, scheduling tools, patient

Common BA categories	Typical examples
	engagement platforms.
Professional services	Medical billing companies, transcription services, claims processors, attorneys advising on patient matters, accountants with access to PHI.
IT services	Managed service providers with administrative access to ePHI systems, data destruction services, cybersecurity consultants performing risk assessments, MSSPs.
Health information exchanges	HIE operators, regional health information organizations, e-prescribing networks.
Conduits (NOT business associates)	Internet service providers, telecommunications carriers, postal services — entities that transmit PHI but do not access or store it for any purpose other than transmission.

Subcontractors and the chain

A subcontractor of a business associate that itself creates, receives, maintains, or transmits ePHI is also a business associate. The chain of liability extends as far as the chain of ePHI-handling. A covered entity that uses an EHR vendor (BA), where the EHR vendor uses a hosting provider (BA-of-BA), where the hosting provider uses a backup vendor (BA-of-BA-of-BA), creates a four-link chain in which every entity touching ePHI is regulated.

Each link requires a Business Associate Agreement (BAA) with the immediately upstream entity. The covered entity contracts with the EHR vendor; the EHR vendor contracts with the hosting provider; the hosting provider contracts with the backup vendor. OCR has stated that each link is independently liable; a breach at the backup vendor exposes all four entities to investigation, with potential liability allocated based on which entity's safeguards failed.

The Business Associate Agreement (BAA)

The BAA is the contractual mechanism that satisfies the covered entity's HIPAA obligation to obtain assurances that any business associate will appropriately safeguard ePHI. The BAA must contain specific provisions enumerated at 45 CFR §164.504(e), including:

- Permitted and required uses and disclosures of PHI by the business associate.
- Prohibition on the BA using or disclosing PHI other than as permitted by the agreement or required by law.
- Requirement that the BA implement appropriate safeguards (in particular, the Security Rule administrative, physical, and technical safeguards for ePHI).
- Requirement that the BA report to the CE any use or disclosure not provided for by the agreement, and any security incident.

- Requirement that the BA ensure any subcontractors that create, receive, maintain, or transmit ePHI agree to the same restrictions.
- Requirement that the BA make available its books and records relating to PHI use and disclosure to HHS for OCR investigations.
- Termination provisions including return or destruction of PHI at termination.

Microsoft, AWS, and Google Cloud each publish standard BAAs for their HIPAA-eligible services. These BAAs are typically non-negotiable for the standard service tiers — they incorporate the §164.504(e) provisions and limit Microsoft (or AWS/GCP) liability to the cloud service provider's defined BA scope. Customer responsibility for configuration, access, identity, and monitoring is explicit in these BAAs.

Three safeguard categories. Required and addressable specifications.

The current HIPAA Security Rule (45 CFR Part 164 Subpart C) organizes ePHI protections into three safeguard categories: administrative, physical, and technical. Each category contains a set of standards. Each standard contains one or more implementation specifications, classified as either Required (must be implemented as written) or Addressable (must be implemented if reasonable and appropriate for the entity's environment, or replaced with an equivalent measure, or affirmatively documented as not reasonable and appropriate).

The addressable/required distinction has been a source of confusion since 2003. The Security Rule does not say that addressable specifications are optional; it says they require either implementation or a documented alternative. Failing to implement an addressable specification without documenting why is a Security Rule violation. OCR has cited inadequate handling of addressable specifications — particularly the encryption specifications — in many enforcement actions. The NPRM proposes to eliminate this distinction entirely, making all implementation specifications mandatory.

Administrative safeguards (§164.308) — 9 standards

Administrative safeguards are the management activities that govern the conduct of the workforce in relation to ePHI. They are the most extensive of the three safeguard categories and are where most OCR enforcement actions concentrate.

Standard (§164.308)	Key implementation specifications
(a)(1) Security Management Process	Risk Analysis (Required); Risk Management (Required); Sanction Policy (Required); Information System Activity Review (Required). The four most-enforced specifications in the entire Security Rule.
(a)(2) Assigned Security Responsibility	Identify the security official responsible for development and implementation of policies and procedures. (Single specification, Required.)
(a)(3) Workforce Security	Authorization and/or Supervision (Addressable); Workforce Clearance Procedure (Addressable); Termination Procedures (Addressable).
(a)(4) Information Access Management	Isolating Health Care Clearinghouse Functions (Required, where applicable); Access Authorization (Addressable); Access Establishment and Modification (Addressable).

Standard (§164.308)	Key implementation specifications
(a)(5) Security Awareness and Training	Security Reminders (Addressable); Protection from Malicious Software (Addressable); Log-in Monitoring (Addressable); Password Management (Addressable).
(a)(6) Security Incident Procedures	Response and Reporting (Required).
(a)(7) Contingency Plan	Data Backup Plan (Required); Disaster Recovery Plan (Required); Emergency Mode Operation Plan (Required); Testing and Revision Procedures (Addressable); Applications and Data Criticality Analysis (Addressable).
(a)(8) Evaluation	Periodic technical and nontechnical evaluation of the Security Rule compliance posture. (Single specification, Required.)
(b)(1) Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement (Required) — the BAA requirement.

Physical safeguards (§164.310) — 4 standards

Physical safeguards protect electronic information systems and the buildings and equipment that contain them from natural and environmental hazards and unauthorized physical intrusion. For organizations operating primarily in cloud environments, most physical safeguards are inherited from the cloud provider's BAA — Microsoft, AWS, GCP physical security at the data center level satisfies these requirements for ePHI hosted in their environments.

Standard (§164.310)	Key implementation specifications
(a) Facility Access Controls	Contingency Operations (Addressable); Facility Security Plan (Addressable); Access Control and Validation Procedures (Addressable); Maintenance Records (Addressable).
(b) Workstation Use	Policies governing functions performed at workstations and physical attributes of workstation surroundings. (Single specification, Required.)
(c) Workstation Security	Physical safeguards for workstations that access ePHI. (Single specification, Required.)
(d) Device and Media Controls	Disposal (Required); Media Re-use (Required); Accountability (Addressable); Data Backup and Storage (Addressable).

Technical safeguards (§164.312) — 5 standards

Technical safeguards are the technology and the policies and procedures for its use that protect ePHI and control access to it. This is the safeguard category where Microsoft 365 and Azure capabilities map most directly — nearly every technical safeguard has a one-to-one mapping to specific Microsoft Security stack capabilities.

Standard (§164.312)	Key implementation specifications
(a)(1) Access Control	Unique User Identification (Required); Emergency Access Procedure (Required); Automatic Logoff (Addressable); Encryption and Decryption (Addressable).
(b) Audit Controls	Hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI. (Single specification, Required.)
(c)(1) Integrity	Mechanism to Authenticate Electronic Protected Health Information (Addressable).
(d) Person or Entity Authentication	Procedures to verify that a person or entity seeking access to ePHI is the one claimed. (Single specification, Required — though the proposed NPRM would substantially expand this with explicit MFA requirements.)
(e)(1) Transmission Security	Integrity Controls (Addressable); Encryption (Addressable). The pair of addressable encryption specifications has been the single most-cited area of confusion in the current rule, and the NPRM proposes to make encryption mandatory in both directions.

Organizational requirements and policies/procedures

§164.314 (Organizational Requirements) covers BAA contents and group health plan requirements. §164.316 (Policies and Procedures and Documentation Requirements) requires regulated entities to implement reasonable and appropriate policies and procedures to comply with the Security Rule, document them in writing, retain documentation for six years from the date of creation or last effective date (whichever is later), make documentation available to those persons responsible for implementing the procedures, and review and update documentation periodically.

OCR's #1 enforcement focus.

The Risk Analysis specification at §164.308(a)(1)(ii)(A) is the single most-cited deficiency in HIPAA enforcement history. OCR has made this explicit in resolution agreements going back more than a decade and continues to emphasize it in current Phase 3 audits, which began in March 2025. The required text reads: ‘Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.’

OCR's enforcement pattern is consistent. When investigating a breach, OCR will request the regulated entity's most recent Risk Analysis as a Day 1 evidence item. If the Risk Analysis is missing, outdated, incomplete, or fails to address the conditions that led to the breach, OCR cites that deficiency directly. In many high-dollar resolution agreements, the inadequate Risk Analysis is the gateway finding from which other findings flow — because if the entity had performed an adequate Risk Analysis, the controls necessary to prevent the breach would have been identified.

What an OCR-defensible Risk Analysis contains

OCR's 2024 Guidance on Risk Analysis (an extension of guidance originally published in 2010 and refined through enforcement actions) describes nine elements that an adequate Risk Analysis must include. None of these is optional — missing any one results in a finding.

Element	What it requires
1. Scope	Defined ePHI scope: every system, application, device, location, and process that creates, receives, maintains, or transmits ePHI. The scope must be comprehensive — OCR has consistently cited entities for scoping out specific systems that turned out to contain ePHI.
2. Data collection	Documentation of where ePHI is created, received, maintained, transmitted; including paper records (within the broader Risk Analysis even though the Security Rule technically governs only ePHI); inventories of devices, applications, network components, locations, removable media.
3. Threat identification	Identification of reasonably anticipated threats to ePHI: human (insider misuse, theft, loss), natural (fire, flood, environmental), technical (malware, vulnerabilities, configuration errors), and supply-chain (third-party breaches).
4. Vulnerability identification	Identification of vulnerabilities in policies, procedures, technical controls, training, and physical environment that could be exploited

Element	What it requires
	by identified threats.
5. Current security measures	Documentation of safeguards already in place: administrative, physical, technical. Required for the next step.
6. Likelihood determination	For each threat-vulnerability pair, an assessed likelihood (low/medium/high or quantitative) that the threat could exploit the vulnerability.
7. Impact determination	For each threat-vulnerability pair, an assessed impact (low/medium/high or quantitative) on confidentiality, integrity, and availability of ePHI.
8. Risk determination	Likelihood multiplied by impact; risks ranked; risk tolerance applied; high-risk items identified for treatment.
9. Documentation and periodic review	Written documentation of all eight prior elements; review and update as the environment changes; review at least every 12 months at minimum (the NPRM would make this explicit).

Source — HHS OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule, supplemented by OCR resolution agreements 2010–2025.

The five most common Risk Analysis failures

OCR resolution agreements consistently surface the same Risk Analysis failure modes. Avoiding these is the highest-leverage compliance investment any regulated entity can make.

- Scope is incomplete. The Risk Analysis covers the EHR but omits clinic systems, lab systems, mobile devices, removable media, paper records, voice recordings, fax, or particular application integrations. Discovered when an OCR investigation finds ePHI somewhere the Risk Analysis did not address.
- The analysis is a vulnerability scan or a control gap assessment, not a Risk Analysis. Vulnerability scanning addresses Element 4 (vulnerabilities) but not Elements 3, 6, 7, 8 — threat identification, likelihood, impact, risk determination. A vulnerability scan output is necessary input but not the Risk Analysis itself.
- The analysis is performed once and never updated. The 2003 Security Rule does not specify a frequency, but OCR has consistently treated stale Risk Analyses as inadequate. The NPRM would make this explicit by requiring annual updates.
- The analysis does not connect to the Risk Management process at §164.308(a)(1)(ii)(B). Identified risks must drive specific risk treatment decisions — either control implementation, risk acceptance with documented rationale, or risk transfer. Risk Analysis without Risk Management is a finding.
- The analysis fails to address third-party and business associate risk. The chain of ePHI-handling described earlier in this guide is in scope of the Risk Analysis. OCR has cited entities

for failing to assess the risk posed by their major business associates and the safeguards those business associates implement.

Risk Analysis as continuous process

In the conventional pattern, Risk Analysis is an annual document produced by a consultant, filed in a SharePoint folder, and not consulted again until the next annual cycle. The continuous-readiness pattern treats Risk Analysis as a live process: the asset inventory updates as the environment changes, threat intelligence feeds into threat identification, control state from Microsoft Defender for Cloud and Sentinel updates the safeguard inventory in real time, and the residual risk register is queryable rather than static. The annual document becomes a snapshot of an ongoing process, not a one-time deliverable.

This is the operational difference between an organization that survives an OCR investigation and one that does not. When OCR requests the Risk Analysis on Day 1 of an investigation, the continuous-readiness organization produces a document that is current, comprehensive, and traceable to specific control implementations. The conventional organization produces a document that was last updated 14 months ago and does not reflect three of the systems involved in the breach.

What the proposed Security Rule update would change.

On January 6, 2025, OCR published the most substantial proposed revision to the HIPAA Security Rule since the 2013 Omnibus Rule. The NPRM — 'HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information' — proposes to transform the Security Rule from a flexible, risk-based framework into a more prescriptive cybersecurity standard. Public comment closed March 7, 2025, with over 4,500 comments submitted, including substantial industry pushback on cost and feasibility. The OCR regulatory agenda lists final rule publication for May 2026.

The proposed changes are substantial enough that even with industry-driven softening in a final rule, regulated entities should plan against the proposal. The NPRM is consistent with the NIST Cybersecurity Framework v2.0, the HHS Cybersecurity Performance Goals, and modern industry practice — the technical content is largely uncontroversial. Industry opposition has focused on the cost and timeline, not on whether the practices are appropriate.

The five most consequential proposed changes

1. Elimination of the addressable/required distinction

Under the NPRM, every implementation specification becomes mandatory. The flexibility that has historically allowed regulated entities to document why an addressable specification is not reasonable and appropriate goes away — entities will be required to implement every specification, with flexibility remaining only in how the specification is implemented, not whether. This is the single most fundamental shift in the proposed rule.

2. New mandatory standards

New standard	What it requires
Technology asset inventory	Written inventory of all electronic information systems and technology assets that may affect the confidentiality, integrity, or availability of ePHI. Identification, version, person accountable, location. Reviewed and updated at least every 12 months.
Network map	Diagram illustrating the movement of ePHI throughout the regulated entity's electronic information systems. Reviewed and updated at least every 12 months.
Patch management	Written policies and procedures for applying patches and updates. Critical patches deployed within 15 days; high-risk patches within 30 days. Documented exceptions process.

New standard	What it requires
Compliance audit	Audit of compliance with each Security Rule standard and implementation specification at least every 12 months.
Verification by business associates	Annual written verification from each business associate that it has implemented the required technical safeguards.

3. Mandatory encryption

ePHI must be encrypted at rest and in transit using cryptographic mechanisms that meet specified standards. The current rule's addressable encryption specifications become mandatory. Limited exceptions are permitted (for example, for compatibility with legacy systems used by small specialty practices) but require documentation and equivalent compensating controls.

4. Mandatory MFA

Multi-factor authentication for all access to ePHI, with phishing-resistant methods preferred. The proposed rule does not strictly require phishing-resistant MFA but explicitly favors it; SMS-based MFA is permitted but discouraged. This effectively requires deployment of FIDO2, Windows Hello, certificate-based authentication, or comparable phishing-resistant methods for the regulated workforce.

5. Specific time-bound obligations

Obligation	Time limit
Terminate former employee's access after separation	Within 1 hour of termination.
Business associate report on contingency plan activation	Within 24 hours.
Restoration of critical electronic systems and data after a loss	Within 72 hours.
Deploy critical-severity patches	Within 15 days.
Deploy high-severity patches	Within 30 days.
Annual review and update of risk analysis, asset inventory, network map, policies and procedures	At least every 12 months.

What to do now

The NPRM has not been finalized as of April 2026. The current Security Rule remains the operative law. But the practical recommendation for any regulated entity that is not already operating at the proposed standard is to begin implementing now. Three reasons: first, OCR has

consistently treated the absence of these practices as evidence of inadequate Risk Analysis under the current rule — implementing them improves current compliance posture. Second, the 240-day compliance window after final rule publication is short enough that organizations starting implementation post-finalization will struggle to meet it. Third, the NPRM aligns with NIST CSF v2.0 and current industry practice — if your organization is investing in cybersecurity at all, building toward the NPRM is consistent with where the practice is moving regardless of the rule's final form.

Recognized security practices safe harbor

The HITECH Act amendment of January 2021 (Public Law 116-321) requires OCR to consider whether a regulated entity has adequately demonstrated that it had, for the 12 months prior to a breach, recognized security practices in place. Recognized security practices include the NIST Cybersecurity Framework, the HICP (HHS Cybersecurity Practices for the Health Industry, an HSCC publication aligned to NIST CSF), and other comparable security programs.

If OCR determines that the entity has had recognized security practices in place for the prior 12 months, it must mitigate fines and other remedies. This is a meaningful enforcement-period safe harbor: organizations that demonstrably implement NIST CSF v2.0 (with documentation of the implementation) are positioned for materially lower OCR penalties even when breaches occur. Recognized security practices also align directly with what the NPRM would require — the same investments support both the current safe harbor and future compliance.

60 days. Three audiences. The OCR portal.

The Breach Notification Rule (45 CFR Part 164 Subpart D) requires regulated entities to notify affected individuals, HHS OCR, and (for breaches affecting 500 or more individuals in a single state) prominent media outlets, when unsecured PHI is breached. The rule applies to all unsecured PHI — PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through encryption that meets HHS guidance, or through destruction. Encrypted PHI that is breached is not subject to notification under HIPAA; this is the practical reason encryption is, despite its current addressable status, the most important Security Rule control to implement.

The three audiences

Audience	Trigger and timing	Method
Affected individuals	Without unreasonable delay and no later than 60 calendar days after discovery of the breach. ‘Discovery’ is the first day on which the breach is known, or, by exercising reasonable diligence, would have been known.	Written notification by first-class mail, or email if the individual has agreed to electronic notice. Substitute notice (web posting + media) for individuals whose contact information is insufficient.
HHS OCR	For breaches affecting ≥500 individuals: contemporaneously with individual notification (within the 60-day window). For breaches affecting <500 individuals: annual log submitted within 60 days after the end of the calendar year.	OCR breach reporting portal at hhs.gov/ocr/breach-portal. Contains structured fields for breach details, affected population, types of PHI, security measures, mitigation actions.
Media	For breaches affecting 500 or more individuals in a single state or jurisdiction: notify prominent media outlets serving the state/jurisdiction. Same 60-day window.	Press release; coordination with public relations counsel. Subject to public disclosure of breach details.

The four-factor risk assessment

Not every impermissible use or disclosure of PHI triggers breach notification. The Breach Notification Rule allows regulated entities to perform a four-factor risk assessment to determine

whether the impermissible use or disclosure compromises the security or privacy of the PHI such that breach notification is required. If the entity demonstrates a low probability that the PHI has been compromised, notification is not required.

The four factors at 45 CFR §164.402(2):

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

The risk assessment must be documented. If the entity proceeds without notification on the basis of a low-probability determination, the documentation of that determination must be retained for six years. OCR will request it during any subsequent investigation.

Business associate breach reporting

When a breach occurs at a business associate, the business associate must report the breach to the covered entity. The covered entity is then responsible for notifying affected individuals, HHS, and (if applicable) media. The 60-day clock for the covered entity begins on the day the business associate provides notice to the covered entity, not on the day the BA discovered the breach.

The NPRM proposes to tighten this further — a business associate would be required to notify the covered entity within 24 hours of activating its contingency plan (a separate trigger from breach notification). This provides covered entities earlier visibility into security events that may eventually be determined to be breaches.

OCR public breach disclosure

OCR maintains a public breach reporting portal that lists breaches affecting 500 or more individuals (the ‘Wall of Shame’). Breaches reported to OCR are publicly visible at hhs.gov/ocr/breach-portal. The public listing includes the regulated entity name, the type of breach, the location of the breach, the number of individuals affected, the date of submission, and — once the OCR investigation closes — the resolution. This is a non-trivial reputational consequence of any reportable breach.

07 · MICROSOFT SECURITY STACK MAPPING

From safeguard to native Microsoft signal.

This section maps each HIPAA Security Rule safeguard category to the specific Microsoft Security stack capabilities that implement or evidence it for organizations on Microsoft 365 and Azure. The mapping is ordered to mirror the Security Rule structure: administrative, physical, technical. Both current rule citations and NPRM-anticipated requirements are addressed.

Microsoft 365 BAA and the customer responsibility model

Microsoft 365 Commercial includes a BAA by default for U.S. customers. Microsoft Azure includes a BAA covering the in-scope services listed in the Microsoft Online Services BAA. The BAA addresses Microsoft's responsibilities as a business associate — the physical safeguards Microsoft operates at its data centers, the underlying platform safeguards, and the contractual obligations.

Customer responsibility includes: tenant configuration, identity (Entra ID), Conditional Access, encryption keys (where customer-managed), data classification (Purview), workload-level network controls, monitoring (Sentinel), incident response, and the Risk Analysis itself. The BAA does not transfer these responsibilities to Microsoft — it allocates which party is responsible for what.

Administrative safeguards (§164.308)

Standard / Spec	Primary Microsoft signal source
(a)(1)(ii)(A) Risk Analysis	Microsoft Purview Compliance Manager HIPAA assessment template; Microsoft Defender for Cloud Secure Score with NIST 800-66 baseline; documented Risk Analysis referencing these signal sources for current state of safeguards.
(a)(1)(ii)(B) Risk Management	Risk register in Microsoft Purview Compliance Manager (or equivalent); risk treatment decisions linked to specific Defender for Cloud recommendations and Sentinel detection rules.
(a)(1)(ii)(D) Information System Activity Review	Microsoft Sentinel ingestion of Entra ID audit logs, M365 Unified Audit Log, Azure Activity Log; documented log review cadence; analyst review records.
(a)(2) Assigned Security Responsibility	Documented designation of Security Official; Entra ID role assignment for the designated official with appropriate administrative scope.
(a)(3) Workforce Security	Microsoft Entra ID lifecycle workflows; HRIS-to-Entra provisioning evidence; documented separation procedures with within-1-hour

Standard / Spec	Primary Microsoft signal source
	deprovisioning (NPRM-anticipated).
(a)(4) Information Access Management	Entra ID Governance access packages; Entra Privileged Identity Management for privileged role assignments; access review evidence.
(a)(5) Security Awareness and Training	Microsoft Defender for Office 365 Attack Simulation Training; Microsoft Viva Learning completion records; LMS exports per individual.
(a)(6) Security Incident Procedures	Documented IR plan; Microsoft Sentinel SOAR playbooks; Sentinel incident records demonstrating documented procedures in operation.
(a)(7) Contingency Plan	Azure Backup evidence with documented retention and restore-test results; Azure Site Recovery test failover evidence; documented DR runbooks.
(a)(8) Evaluation	Microsoft Purview Compliance Manager HIPAA assessment with completion evidence; documented periodic evaluation; mock OCR audit records (recommended even though not strictly required).
(b) BAA contracts	Inventory of business associates with signed BAAs; documented BA review cadence.

Physical safeguards (§164.310)

For workloads operating in Microsoft 365 and Azure, the data-center-level physical safeguards are inherited from Microsoft's BAA. The customer's physical safeguards are limited to facilities where workforce members access ePHI and any on-premises infrastructure. The Microsoft Service Trust Portal provides Customer Assurance Service documents for Microsoft data center physical security.

Standard / Spec	Primary Microsoft signal source
(a) Facility Access Controls	Inherited from Microsoft via the Service Trust Portal for cloud-hosted workloads; on-premises facility access procedures and visitor logs for customer-operated facilities.
(b) Workstation Use	Documented workstation use policy; Intune device configuration profiles; documented procedures for remote and BYOD access.
(c) Workstation Security	Microsoft Intune compliance policies (encryption required, antivirus required, screen lock); BitLocker enforcement; conditional access requiring compliant device.
(d) Device and Media Controls	Intune device lifecycle (enrollment, configuration, retirement); BitLocker encryption for all endpoints; documented disposal

Standard / Spec	Primary Microsoft signal source
	procedures for retired hardware (NIST SP 800-88 alignment).

Technical safeguards (§164.312)

Technical safeguards are where Microsoft 365 and Azure deliver the densest evidence per safeguard. The five standards map cleanly to specific Entra ID, Defender, Sentinel, and Purview capabilities.

Standard / Spec	Primary Microsoft signal source
(a)(1) Access Control — Unique User ID	Entra ID user identity inventory; documented procedure for unique identifier issuance; service account inventory with identity provenance.
(a)(1) Access Control — Emergency Access	Entra ID break-glass account documentation; PIM emergency access procedures; documented activation criteria.
(a)(1) Access Control — Automatic Logoff	Entra ID session policies; Microsoft Intune device configuration profile enforcing screen lock; M365 sign-in frequency policy.
(a)(1) Access Control — Encryption / Decryption	Microsoft Purview sensitivity labels enforcing encryption; M365 customer key (Service Encryption); Azure Storage encryption with customer-managed keys; Azure SQL TDE.
(b) Audit Controls	Microsoft Sentinel ingestion of Entra ID audit and sign-in logs, M365 Unified Audit Log, Azure Activity Log, Defender XDR investigations; documented retention aligned to 6-year requirement; immutable storage for retention period.
(c)(1) Integrity — Authenticate ePHI	Azure Storage immutable blob retention; Microsoft Purview audit for change records; documented integrity verification procedure for backups (NPRM aligned).
(d) Authentication — NPRM mandates MFA	Entra ID Conditional Access policies enforcing MFA for ALL ePHI system access; phishing-resistant MFA (FIDO2, Windows Hello, certificate-based) preferred over SMS; sign-in logs filtered by authentication method.
(e)(1) Transmission — Integrity Controls	TLS 1.2+ enforcement on all M365 and Azure services; certificate management in Azure Key Vault; documented configuration of integrity-protected protocols.
(e)(1) Transmission — Encryption	TLS 1.2+ enforced for M365; Microsoft Purview sensitivity labels with encryption for ePHI in email and documents; Microsoft 365 Message Encryption; SMTP TLS 1.2 enforcement.

NPRM-anticipated additions

Proposed standard	Primary Microsoft signal source
Technology asset inventory	Microsoft Defender Vulnerability Management software inventory; Azure Resource Graph queries; Microsoft Purview Data Map for data assets; consolidated inventory in a Knowledge Graph.
Network map	Azure Network Watcher topology; NSG flow logs; private endpoint topology; documented data flow diagram derived from Azure Resource Graph and M365 connector inventory.
Patch management	Microsoft Update for Business / Intune update rings; Azure Update Manager; Defender Vulnerability Management remediation tracking; SLA evidence (15-day critical, 30-day high).
Compliance audit	Microsoft Purview Compliance Manager improvement-action history; documented annual compliance audit referencing Compliance Manager state plus targeted control testing.
BA verification	Annual written verification process; vendor risk management workflow; documented evidence of receipt and review of each BA's verification.

HIPAA at scale requires automation. Manual will not survive the NPRM.

HIPAA has always been a high-volume compliance regime. A mid-sized regional hospital system has thousands of workforce members, hundreds of applications, dozens of business associates, multiple facilities, ten thousand or more devices, and millions of records of ePHI flowing through the environment annually. The Security Rule's risk-based flexibility was the regulatory accommodation that made compliance feasible for that complexity. The NPRM, by contrast, proposes prescriptive standards with annual review cycles, technology asset inventories, network maps, written verification from every business associate, and 15- to 30-day patch SLAs. At scale, none of that is achievable through manual processes.

This is the operational reality the title of this guide reflects. ‘HIPAA Compliance Automation’ is not a marketing phrase — it is a feasibility statement. The regulated entity that maintains HIPAA compliance through quarterly Risk Analysis updates, annual policy reviews, and ad-hoc evidence collection will fail to meet the NPRM's requirements when finalized. The regulated entity that has operationalized continuous monitoring, automated evidence capture, and machine-queryable Risk Analysis will satisfy the NPRM as a byproduct of how it operates.

Pattern 1 — Risk Analysis as a live graph

In the conventional pattern, the Risk Analysis is a Word document or spreadsheet produced annually by a consultant. It captures the state of the environment at one point in time, lists threats and vulnerabilities, ranks risks, and is filed. When the environment changes — a new EHR module, a new business associate, a new clinical application — the Risk Analysis is not updated until the next annual cycle. By the time of the next OCR audit, the document is months out of sync with reality.

In the continuous-readiness pattern, the Risk Analysis is a view over a Knowledge Graph. Every ePHI-handling system is a node. Every threat is a node. Every vulnerability is a node. Every safeguard is a node. The relationships between them are edges. When a new system is provisioned in Azure, it joins the graph automatically through Azure Resource Graph integration. When a new business associate signs a BAA, the BA enters the graph with its own subgraph of safeguards. The Risk Analysis is rendered as needed — for OCR, for the annual cycle, for an investigation — from the live graph state, not assembled from stale documents.

Pattern 2 — Evidence-on-demand for OCR

OCR investigations have a predictable pattern. The investigator requests Day 1 evidence: the most recent Risk Analysis, the Information System Activity Review records, the BAA inventory, the IR plan, the access management documentation. The conventional regulated entity

scrambles to assemble these from various locations, often discovering during assembly that documents are out of date or missing. The 30-day OCR response window becomes a fire drill.

The continuous-readiness pattern reads Microsoft signal continuously — Entra ID for identity, Defender XDR for threats, Sentinel for activity review, Purview for data classification. Evidence is captured at execution time, hashed, timestamped, and indexed. When OCR asks ‘produce the access reviews for ePHI systems for the past 12 months,’ the answer is a query over evidence already collected, not a screenshot exercise that begins after the question is asked. The 30-day response window becomes adequate.

> **One control set, every framework**
> The Secure Controls Framework (SCF) anchors the Kyūdō Knowledge Graph as the meta-framework substrate. SCF includes 1,470+ controls across 80+ frameworks. HIPAA Security Rule maps to SCF; SCF maps to NIST CSF v2.0, NIST SP 800-53, NIST SP 800-66 (the HIPAA implementation guidance), HITRUST, SOC 2, ISO 27001, and the rest. A single Microsoft Defender for Cloud configuration baseline, a single Sentinel detection record, a single Purview DLP policy execution attests against every framework where the SCF crosswalk holds. For healthcare organizations operating against HIPAA plus SOC 2 plus HITRUST plus state breach laws plus contractual obligations to payers, this is what makes a multi-framework portfolio operable.

Pattern 3 — NPRM compliance as a graph extension

If the NPRM is finalized in May 2026, the technology asset inventory, network map, patch management, compliance audit, and BA verification requirements all need to be operationalized inside the 240-day compliance window. Built manually, this is a multi-quarter program. Built as extensions of an existing Knowledge Graph, this is configuration: the asset inventory is a query, the network map is a topology rendering, the patch SLA is a Sentinel detection, the compliance audit is a graph traversal, the BA verification is a workflow that fires annually.

The architectural question is whether your governance platform is a static document store or a queryable graph. Document stores require manual programs to satisfy NPRM requirements. Graphs satisfy NPRM requirements through schema extensions. The question to ask vendors evaluating GRC platforms in 2026: ‘Can your platform render a current technology asset inventory and network map for OCR on demand, or do those need to be produced by separate processes?’

Pattern 4 — Sovereignty as architecture

HIPAA's most consequential architectural property is that ePHI cannot move through systems without a BAA. Most SaaS GRC platforms are business associates of their customers — they handle ePHI-adjacent metadata (control state, evidence pointers, sometimes raw logs) and require BAAs themselves. This adds a regulated entity to the chain. The continuous-readiness pattern inverts this: the governance layer deploys inside the customer's own Azure tenant or AWS account. Microservices run in customer-owned AKS clusters with private endpoints, system-

assigned managed identities, and customer-managed encryption keys. No ePHI or ePHI-adjacent data crosses the tenant boundary. The governance platform is not a separate business associate.

Pattern 5 — Auditor-defensible AI

AI in healthcare GRC is an immediate area of OCR scrutiny. The 2025 NPRM specifically addresses AI in its preamble; OCR has signaled in current Phase 3 audits that AI-generated risk analyses, AI-generated policies, and AI-generated breach risk assessments will receive heightened review. The continuous-readiness pattern requires AI that survives an OCR investigator's question: every AI-produced explanation, mapping, or recommendation must have a source, a confidence level, and a re-performable result.

In Kyūdō, AI is layered. Deterministic functions handle scoring, state transitions, breach four-factor risk assessment, BA chain traversal, and the Risk Analysis structure. AI functions handle explanation, draft policy generation, control-mapping suggestions, and natural-language traversal of the Knowledge Graph. The two layers never share a trust contract: the deterministic engine produces the answer, AI produces the prose. When OCR asks ‘how was this risk score derived?’ the answer is a graph traversal — not a model output.

Where this leaves you

If you are a covered entity or business associate operating today against the current Security Rule, this guide is a working reference. Walk the safeguards. Build or update your Risk Analysis. Identify gaps. Implement remediation. Pay particular attention to encryption, MFA, and the Risk Analysis itself — these are OCR's enforcement priorities.

If you anticipate operating under the finalized NPRM, the architecture this section describes is the direction the practice must move. The marginal cost of maintaining HIPAA compliance, supporting OCR audits, and adding the cross-framework coverage healthcare organizations also operate against (SOC 2, ISO 27001, NIST CSF, HITRUST, state breach laws) should approach zero. If it does not, the bottleneck is the architecture.

Kyūdō is the platform that makes that architecture available to regulated organizations running Microsoft 365 and Azure. The next step, if useful, is a deployment workshop in your tenant. The architecture brief is one click. The conversation is one email.

—

If this is useful, the next step is concrete

Architecture briefing — a 30-minute walkthrough of the Kyūdō deployment in your Azure tenant: Risk Analysis automation, Microsoft signal mapping, evidence-on-demand for OCR, and the sovereignty model. → hello@kyudo.ai

HIPAA readiness workshop — 90 minutes walking the Security Rule safeguards against your current state, with a documented gap report and 90-day remediation plan ahead of the NPRM. → kyudo.ai/workshop

Trust packet — our HIPAA architecture commitments, BAA template, NPRM readiness statement, data-residency model, and the Microsoft estate dependency map. Available on request.

APPENDIX A · SAFEGUARD MATRIX

The Security Rule at a glance.

The Appendix A matrix from 45 CFR Part 164 Subpart C, in compact form. R = Required; A = Addressable. The NPRM proposes to eliminate the R/A distinction — every specification becomes Required.

Standard	Implementation specification	R/A
Administrative — Security Management Process §164.308(a)(1)	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Administrative — Assigned Security Responsibility §164.308(a)(2)	(no separate spec; the standard itself)	R
Administrative — Workforce Security §164.308(a)(3)	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A
Administrative — Information Access Management §164.308(a)(4)	Isolating Health Care Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A
Administrative — Security Awareness and Training §164.308(a)(5)	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A

Standard	Implementation specification	R/A
Administrative — Security Incident Procedures §164.308(a)(6)	Response and Reporting	R
Administrative — Contingency Plan §164.308(a)(7)	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedures	A
	Applications and Data Criticality Analysis	A
Administrative — Evaluation §164.308(a)(8)	(no separate spec; the standard itself)	R
Administrative — BA Contracts §164.308(b)(1)	Written Contract or Other Arrangement	R
Physical — Facility Access Controls §164.310(a)	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A
Physical — Workstation Use §164.310(b)	(no separate spec)	R
Physical — Workstation Security §164.310(c)	(no separate spec)	R
Physical — Device and Media Controls §164.310(d)	Disposal	R
	Media Re-use	R
	Accountability	A
	Data Backup and Storage	A
Technical — Access Control §164.312(a)(1)	Unique User Identification	R
	Emergency Access Procedure	R

Standard	Implementation specification	R/A
	Automatic Logoff	A
	Encryption and Decryption	A
Technical — Audit Controls §164.312(b)	(no separate spec)	R
Technical — Integrity §164.312(c)(1)	Mechanism to Authenticate ePHI	A
Technical — Person or Entity Authentication §164.312(d)	(no separate spec)	R
Technical — Transmission Security §164.312(e)(1)	Integrity Controls	A
	Encryption	A

APPENDIX B · OCR ENFORCEMENT PRIORITIES

Where investigations actually focus.

OCR's enforcement priorities are visible from the resolution agreements published since 2010. The enforcement actions cluster around a small set of recurring deficiencies. Investing in these specific areas produces the largest enforcement-risk reduction per dollar spent.

OCR enforcement priority	What OCR cites
1. Risk Analysis	Inadequate, incomplete, missing, or out-of-date Risk Analysis. The single most-cited deficiency. Often a gateway finding from which other findings flow.
2. Risk Management	Risks identified in Risk Analysis but not mitigated. Risk Analysis without Risk Management is a finding.
3. Encryption	Failure to encrypt ePHI at rest or in transit, particularly on portable devices and removable media. Even though the current rule is addressable, OCR has consistently treated unencrypted ePHI as unreasonable.
4. Access controls	Failure to terminate access promptly upon separation; failure to apply least-privilege access; shared accounts; lack of audit logging on privileged access.
5. Audit Controls / Information System Activity Review	Missing or inadequate audit logs; failure to actually review the logs; no documented procedure for review.
6. Workforce training	Untrained workforce; no documented training records; training not refreshed.
7. Business Associate Agreements	Missing BAAs for identified business associates; BAAs that lack required §164.504(e) provisions; BAAs not updated.
8. Breach Notification	Late notification beyond the 60-day window; incomplete notification; failure to notify HHS; failure to notify media for ≥500-individual breaches in a single state.
9. Disposal and Media Re-use	Improper disposal of devices and media containing ePHI; ePHI recovered from sold or donated equipment.
10. Right of Access (Privacy Rule)	OCR's Right of Access Initiative since 2019 has produced over 50 enforcement actions for failure to provide patients access to their PHI within 30 days. While Privacy Rule, this directly affects ePHI

OCR enforcement priority	What OCR cites
	handling.

Penalty tiers (2026 inflation-adjusted)

Tier	Culpability standard	Penalty range per violation
Tier 1	Did not know and would not have known by exercising reasonable diligence	$137 to $68,928
Tier 2	Reasonable cause and not willful neglect	$1,379 to $68,928
Tier 3	Willful neglect, corrected within 30 days	$13,785 to $68,928
Tier 4	Willful neglect, not corrected	$68,928 to $2,134,831

Source — 45 CFR §160.404, with annual inflation adjustments. Annual cap per violation category: $2,134,831. Penalties may be aggregated across violation categories; multi-million-dollar settlements are common.

APPENDIX C · AUTHORITATIVE SOURCES

Where to verify and go deeper.

Primary regulation

- HIPAA — Public Law 104-191 (1996); HITECH Act — Public Law 111-5 (2009).
- 45 CFR Part 160 — General Administrative Requirements (Enforcement Rule, definitions, applicability).
- 45 CFR Part 164 Subpart A — General provisions.
- 45 CFR Part 164 Subpart C — Security Rule (§§164.302–164.318).
- 45 CFR Part 164 Subpart D — Breach Notification Rule (§§164.400–164.414).
- 45 CFR Part 164 Subpart E — Privacy Rule.

OCR guidance

- HHS OCR website (hhs.gov/hipaa) — the authoritative repository for guidance, enforcement actions, and rulemaking status.
- Guidance on Risk Analysis Requirements under the HIPAA Security Rule — OCR (originally 2010, updated through enforcement actions).
- HIPAA Security Rule NPRM (90 Federal Register 898, January 6, 2025) — the proposed rule under consideration for May 2026 finalization.
- OCR Resolution Agreements and Civil Money Penalties — hhs.gov/hipaa/for-professionals/compliance-enforcement; the operational record of OCR enforcement priorities.
- OCR Breach Reporting Portal — hhs.gov/ocr/breach-portal; the public record of breaches affecting 500 or more individuals.

NIST publications

- NIST SP 800-66 Revision 2 — Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide (February 2024). Maps each Security Rule standard to NIST SP 800-53 controls and provides implementation guidance.
- NIST Cybersecurity Framework v2.0 (CSWP 29, February 2024) — the recognized security practice framework relevant to the HITECH safe harbor.
- NIST SP 800-30 Revision 1 — Guide for Conducting Risk Assessments. The methodological reference for Security Rule Risk Analysis.
- NIST SP 800-53 Revision 5.2 — Security and Privacy Controls. Underlying control catalog for SP 800-66 mappings.
- NIST SP 800-88 Revision 1 — Guidelines for Media Sanitization.

HSCC and industry resources

- Health Sector Coordinating Council (HSCC) — 405(d) Aligning Health Care Industry Security Approaches publications, including HICP (Health Industry Cybersecurity Practices).
- HHS Cybersecurity Performance Goals (CPGs) — voluntary, NIST CSF-aligned goals released January 2024; recognized security practices for HITECH safe harbor.
- HITRUST CSF — industry-recognized control framework that incorporates HIPAA, NIST, and other authority documents; used by many health systems for vendor assessment and self-attestation.

Microsoft documentation

- Microsoft Online Services BAA — the standard agreement covering Microsoft 365, Dynamics 365, and Azure HIPAA-eligible services.
- Microsoft Service Trust Portal — published assessments, audit reports, and Customer Assurance Service documents for Microsoft cloud services.
- Microsoft Purview Compliance Manager — HIPAA assessment template with improvement actions mapped to Microsoft 365 and Azure.
- Microsoft HIPAA/HITECH guidance — docs.microsoft.com/azure/compliance/offerings/offering-hipaa-hitech.

APPENDIX D · GLOSSARY

Terms used in this guide.

Term	Definition
Addressable specification	An implementation specification that the regulated entity must implement if reasonable and appropriate, replace with an equivalent measure if not, or document why neither is appropriate. The NPRM proposes to eliminate this category.
Administrative safeguards	§164.308 — administrative actions, policies, and procedures that govern the workforce in relation to ePHI.
BA / Business Associate	Any person or entity, other than a workforce member, that creates, receives, maintains, or transmits PHI on behalf of a covered entity. Directly liable under HIPAA since the HITECH Act.
BAA / Business Associate Agreement	The contract required at §164.504(e) between a covered entity and a business associate, or between a BA and its subcontractor BAs.
Breach	An impermissible use or disclosure of PHI that compromises its security or privacy. Subject to the four-factor risk assessment at §164.402(2) for low-probability determinations.
Breach Notification Rule	45 CFR Part 164 Subpart D — the rule governing notification to individuals, HHS, and (for ≥500) media when unsecured PHI is breached.
CE / Covered Entity	Health plans, health care clearinghouses, and most health care providers — the three categories directly regulated by HIPAA.
ePHI	Electronic Protected Health Information — PHI in electronic form. The exclusive subject matter of the Security Rule.
HHS	U.S. Department of Health and Human Services. The federal agency with HIPAA rulemaking and enforcement authority.
HIPAA	Health Insurance Portability and Accountability Act of 1996. The underlying statute.
HITECH Act	Health Information Technology for Economic and Clinical Health Act of 2009. Extended direct liability to business associates and substantially increased penalties.
HITRUST	An industry-driven control framework that incorporates HIPAA, NIST,

Term	Definition
	and other authority documents. Widely used in health system vendor risk programs.
NPRM	Notice of Proposed Rulemaking. The procedural step before a final rule. The 2025 Security Rule NPRM is the subject of Section 5.
OCR / Office for Civil Rights	The HHS office responsible for HIPAA enforcement. Conducts investigations, audits, and resolution agreements.
Part 2	42 CFR Part 2 — the federal regulation governing substance use disorder records. Aligned with HIPAA via the 2024 final rule (compliance February 16, 2026).
PHI	Protected Health Information — individually identifiable health information held by a covered entity or business associate. ePHI is the electronic subset.
Physical safeguards	§164.310 — physical measures, policies, and procedures protecting ePHI systems and the buildings/equipment that contain them.
Privacy Rule	45 CFR Part 164 Subpart E — the rule governing the use and disclosure of PHI.
Recognized security practices	The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, or the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015. Implementing them for the prior 12 months provides a HITECH safe harbor for OCR penalty mitigation.
Required specification	An implementation specification that the regulated entity must implement as written, with no flexibility to substitute an alternative. The NPRM proposes that all specifications become Required.
Risk Analysis	§164.308(a)(1)(ii)(A) — the foundational Security Rule requirement for an accurate and thorough assessment of risks and vulnerabilities to ePHI. OCR's #1 enforcement focus.
Security Rule	45 CFR Part 164 Subpart C — the regulation governing administrative, physical, and technical safeguards for ePHI.
Subcontractor BA	A subcontractor of a business associate that itself creates, receives, maintains, or transmits ePHI. Independently regulated as a BA.
Technical safeguards	§164.312 — the technology and policies and procedures that protect ePHI and control access to it.

Term	Definition
Unsecured PHI	PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through encryption or destruction meeting HHS guidance. The trigger for Breach Notification Rule applicability.