Insert Your Logo Here

${organizationName}

Subject: HIPAA Security Policy Template Policy #:
Title: Termination Policy and Procedure

HIPAA SECURITY POLICY TEMPLATE

Termination Policy and Procedure

With Workforce Offboarding, AI Tool Offboarding, Vendor Access, Privileged Access, and Audit Evidence Controls

Document Control Field	Template Entry
Organization Name	[Insert covered entity or business associate name]
Policy ID	HIPAA-SEC-WF-TERM-001
Version	1.0 Template
Prepared / Last Reviewed	May 12, 2026
Effective Date	[Insert effective date]
Policy Owner	[Security Officer / Compliance Officer]
Approved By	[Executive Leadership / Compliance Committee]
Applies To	Employees, volunteers, trainees, students, interns, contractors, temporary workforce, credentialed providers, consultants, vendors, business associate workforce users under direct control, and users or administrators of systems, AI tools, service accounts, integrations, or automations that create, receive, maintain, transmit, process, analyze, summarize, infer from, or store ePHI.
Template Classification	Policy and operating procedure template for customization before adoption.

Template Use Notice
This template is designed for HIPAA-regulated organizations and must be customized to match the organization's workforce model, systems, contracts, state law, medical staff bylaws, credentialing rules, union agreements, risk analysis, and legal requirements. It is not legal advice. Final language should be reviewed by the Security Officer, Privacy Officer, Human Resources, IT leadership, Compliance, and legal counsel before adoption.

Prepared for implementation, OCR audit readiness, workforce offboarding, AI governance, privileged access control, vendor access management, and evidence retention.

Contents

- 9. Training, Testing, Auditing, and Review
- 10. Appendices: Checklists, Forms, Logs, Notices, and Audit Tools
- 11. References Reviewed
- 12. Definitions

Navigation Tip
This document uses Microsoft Word heading styles so it can be navigated through the Word Navigation Pane. Replace all bracketed fields before adoption. Add the organization's system inventory and AI inventory before policy approval.

1. How to Use This Template

This document provides a comprehensive HIPAA Security policy and operating procedure for terminating, modifying, suspending, or transferring access to electronic protected health information (ePHI) and systems that can affect ePHI. It is written for use by covered entities, business associates, and healthcare organizations that need a practical offboarding control aligned with Security Rule safeguards, cybersecurity readiness, and AI governance.

- **Customize bracketed fields.** Replace bracketed placeholders with organization-specific titles, systems, timeframes, committees, and approval roles.
- **Attach the system inventory.** Add EHR/EMR, billing, claims, cloud, email, collaboration, remote access, identity, analytics, device management, SIEM, ticketing, AI, automation, and vendor portals used by the organization.
- **Map to the risk analysis.** Use the organization's HIPAA risk analysis to define stricter controls for high-risk terminations, privileged users, remote workforce members, AI developers, API owners, and vendors.
- **Adopt appendices as evidence.** The checklists, forms, logs, certifications, and audit scripts can be copied into a ticketing system or retained as policy implementation evidence.
- Treat AI tools as ePHI systems when they can access ePHI. Approved AI assistants, medical scribes, RPA bots, generative AI platforms, vector stores, model environments, and APIs must be included in offboarding.
- **Review with HR and legal counsel.** Coordinate the policy with employment law, contracts, collective bargaining agreements, medical staff bylaws, state law, professional licensing obligations, and litigation hold procedures.

Implementation Note
Do not rely on verbal confirmation that access was removed. Require ticket numbers, system reports, screenshots or exports, timestamps, system-owner sign-off, asset receipts, AI-owner transfer evidence, key-rotation records, and post-termination log review results.

Version	Date	Owner	Summary of Changes
1.0	May 12, 2026	[Security Officer]	Initial template created. Includes HIPAA Security Rule termination procedures, access control, device/media controls, vendor/business associate considerations, AI use and AI offboarding, privileged access and secrets rotation, audit evidence, and proposed-rule readiness notes.
[Insert]	[Insert]	[Insert]	[Insert revisions after legal, compliance, operational, and security review.]
1.1	May 18, 2026	[Security Officer / Privacy Officer / Legal]	Regulatory currency review completed. Added 42 CFR Part 2 final-rule handling, AI governance refinements, current-law versus proposed-rule status clarification, evidence requirements, regulatory currency gap analysis, Part 2 and AI checklists, and final change history record.

2. Policy Statement, Purpose, and Scope

2.1 Policy Statement

It is the policy of [Organization Name] to terminate, modify, suspend, or transfer workforce, contractor, vendor, privileged, service account, and AI-related access to ePHI and relevant information systems in a timely, documented, and risk-based manner when employment, assignment, role, contract, affiliation, authorization, credentialing, or other access arrangement ends or changes.

- Access to ePHI shall be limited to authorized workforce members, authorized business associate users, and authorized software programs with a current role-based need.
- No former workforce member or user shall retain access to ePHI, systems containing ePHI, AI tools that process ePHI, authentication credentials, tokens, prompt histories, model artifacts, physical access devices, organization devices, records, or exports after access is no longer authorized.
- High-risk, involuntary, security-sensitive, insider-threat, or privileged-access terminations shall be coordinated before notice where feasible and access shall be disabled before or at the time of notice.
- Access termination and modification actions shall be documented, verified, reviewed, and retained as evidence of compliance.
- AI-enabled systems, AI assistants, AI agents, medical scribe tools, transcription tools, RPA bots, API integrations, analytics workspaces, and model development environments that interact with ePHI shall be included in termination procedures.

Core Compliance Principle
Termination procedures are not only an HR task. They are a HIPAA Security Rule safeguard used to prevent unauthorized access to ePHI after a person, contractor, vendor, service account, AI agent, or technology asset no longer has a legitimate and approved need for access.

2.2 Purpose

- Prevent unauthorized access, use, disclosure, alteration, destruction, copying, export, forwarding, printing, query, model training, or retention of ePHI by former users or users whose roles have changed.
- Ensure timely coordination among Human Resources, supervisors, IT, Information Security, Privacy, Compliance, Legal, Facilities, vendor management, system owners, and AI governance owners.
- Define minimum actions for disabling accounts, revoking sessions, removing roles, recovering assets, preserving records, reviewing logs, rotating secrets, and transferring ownership of AI artifacts and automations.
- Support the organization's security management process, workforce security, information access management, access control, audit controls, physical safeguards, device/media controls, incident response, risk management, and documentation obligations.
- Improve readiness for OCR audits, breach investigations, litigation holds, third-party due diligence, cyber insurance reviews, and future HIPAA Security Rule amendments.

2.3 Scope

This policy applies to all workforce members, users, accounts, systems, applications, devices, media, physical access methods, cloud resources, APIs, AI-enabled technologies, and third-party access paths that create, receive, maintain, transmit, process, summarize, analyze, infer from, or store ePHI for or on behalf of [Organization Name].

Included Category	Examples
Workforce members	Employees, volunteers, trainees, students, interns, clinicians, credentialed providers, temporary staff, contractors, consultants, remote workers, and other persons whose work is under the organization's direct control.
Electronic information systems	EHR/EMR, patient portal, HIE, practice management, claims, billing, scheduling, pharmacy, lab, imaging/PACS, data warehouse, cloud storage, email, chat, secure messaging, fax, ticketing, VPN, VDI, IAM, MDM, EDR, SIEM, password vault, and identity platforms.

Included Category	Examples
AI and automation systems	AI documentation assistants, medical scribe tools, transcription/summarization tools, coding/claims AI, generative AI assistants, predictive algorithms, clinical decision support, intake/chatbots, RPA bots, AI agents, API integrations, model hosting, vector databases, embeddings, RAG systems, and AI governance platforms.
Physical access and assets	Badges, keys, smartcards, tokens, laptops, mobile devices, tablets, removable media, printers, scanners, copiers, dictation devices, telehealth equipment, paper records, paper notes, and security rooms.
Third-party access	Business associates, subcontractors, vendor support users, managed service providers, cloud providers, AI vendors, billing companies, consultants, temporary staffing agencies, and outsourced service providers.

2.4 Exclusions and Related Policies

This policy does not replace general HR separation procedures or employment law requirements. Employment records held by a covered entity in its role as employer are generally excluded from PHI under HIPAA; however, they may still be confidential and subject to other legal or organizational controls. When workforce records contain health information maintained for treatment, payment, healthcare operations, or plan administration, apply the appropriate privacy and security requirements.

Related policies should include Information Access Management, Workforce Clearance, Sanction Policy, Security Awareness and Training, Password and MFA, Remote Access, Mobile Device and BYOD, Device and Media Controls, Incident Response, Vendor Management, Business Associate Agreement Management, AI Acceptable Use, Data Retention, Legal Hold, and Breach Notification.

If ePHI includes specially protected data such as substance use disorder treatment records, psychotherapy notes, reproductive health information, genetic information, sensitive minor records, or information subject to state-specific restrictions, the termination workflow should include additional access segmentation and system-specific controls applicable to those data sets.

2.5 Compliance Mapping Summary

Security Rule Area	Policy Implementation in This Template
Security management process	Requires documented access removal, log review, incident escalation, exception control, and risk-based treatment of high-risk separations.
Workforce security	Defines authorization, clearance, role change, suspension, and termination workflows for workforce members and workforce-like users.
Information access management	Requires removal, modification, review, and recertification of role-based access, privileged access, delegated access, shared workspaces, and software-program access.
Security incident procedures	Requires escalation when post-termination access, exfiltration, retained ePHI, personal AI use, or unusual activity is suspected.
Physical safeguards	Requires badge/key removal, facility access validation, asset return, workstation/device controls, and media sanitization.
Technical safeguards	Requires unique user disablement, session revocation, audit controls, authentication removal, transmission/access safeguards, and AI/API/token review.
Documentation requirements	Requires policy, procedure, action records, approvals, exceptions, evidence, and reviews to be retained in written or electronic form according to the retention schedule.

Security Rule Area	Policy Implementation in This Template
Business associate safeguards	Requires vendor-side access removal confirmation, subcontractor consideration, contract/BAA alignment, and AI vendor offboarding when ePHI is processed.

3. Governance and Responsibilities

Access termination requires coordinated action. No department should rely on another department's assumption that access has been removed. Each role below has specific responsibilities and must document completion of assigned tasks.

Role	Responsibilities
Human Resources / Credentialing	Initiate termination, transfer, leave, suspension, or status-change notification; classify termination type; provide effective date/time; notify IT/Security/Privacy/Facilities using the approved workflow; maintain HR separation records; notify Security immediately for involuntary, high-risk, or investigation-related events.
Supervisor / Department Manager	Identify systems, devices, records, files, physical areas, data repositories, shared workspaces, AI tools, automations, delegated access, vendor portals, and business processes used by the person; coordinate work handoff; certify that prior access is no longer needed; report suspected misconduct or data retention.
Security Officer	Own this policy; approve high-risk termination controls; oversee Security Rule documentation; determine whether security incident response is required; review exceptions; monitor trends; verify evidence retention.
Privacy Officer	Advise on PHI/ePHI, minimum necessary, patient privacy, breach risk assessment, special data categories, impermissible disclosure concerns, and communications involving PHI.
IT / Identity and Access Management	Disable or modify accounts; revoke sessions and tokens; remove groups and roles; rotate credentials; recover or wipe devices; disable VPN/remote access; preserve audit logs; transfer ownership of data, mailboxes, queues, AI agents, and automations; produce evidence of completion.
Information Security / SOC	Perform high-risk monitoring; review logs; investigate alerts; suspend suspicious accounts; preserve forensic evidence; coordinate incident response and breach analysis; review privileged and AI-related activity.
Facilities / Physical Security	Recover badges, keys, parking passes, smartcards, alarm codes, lockers, biometric access, physical tokens, and secure-area access; update physical access systems; escort high-risk terminations; preserve access logs if needed.
Legal / Compliance	Advise on legal hold, litigation preservation, employment law, contract obligations, regulator inquiries, breach notification, subpoenas, union requirements, and vendor or business associate issues.
Vendor Management / Procurement	Notify vendors and business associates when access must be removed; verify vendor-controlled accounts and support portals are disabled; update BAA/contract user lists; collect written confirmation.
AI Governance Owner / AI System Owner	Disable AI platform accounts; transfer AI artifacts; stop AI agents and automations; remove data connectors; revoke API keys; reassign model deployment ownership; verify prompt/output histories and vector stores containing ePHI remain under organizational control.
Workforce Member / Departing User	Return assets, records, keys, devices, tokens, documents, and media; certify that no ePHI, credentials, AI outputs, prompts, transcripts, files, screenshots, exports, backups, or copies are retained in personal accounts, personal devices, personal AI tools, or unauthorized storage.

Small Organization Note
The same person may hold several roles in a smaller organization. The key controls are timely notice, documented access removal, segregation of review where feasible, evidence retention, and independent verification that access no longer exists.

3.1 Escalation Authority

- The Security Officer may require immediate suspension of access when ePHI, patient safety, operational integrity, AI system integrity, privileged access, or regulatory compliance may be at risk.
- The Privacy Officer may require investigation or breach risk assessment when retained ePHI, impermissible disclosure, unauthorized AI use, or improper access is suspected.
- Legal may require evidence preservation or legal hold before account deletion, device wipe, email deletion, log destruction, or data transfer.
- Executive leadership may approve time-limited exceptions only when Security, Privacy, Legal, and the business owner document compensating controls and monitoring.

4. Policy Requirements

4.1 Mandatory Trigger Events

The termination or access modification procedure shall be initiated when any of the following events occur or are reasonably expected to occur:

- Employment, contract, volunteer status, internship, student placement, consulting arrangement, vendor support arrangement, credentialing status, medical staff affiliation, or temporary assignment ends.
- A workforce member transfers to a new department, changes duties, changes licensure/credentialing status, changes location, changes employment status, or no longer requires prior access.
- A workforce member goes on leave, suspension, administrative leave, medical leave, sabbatical, extended absence, or investigation leave and access is not required during the absence.
- A role is reduced, reassigned, narrowed, or time-limited so previous ePHI access is no longer minimum necessary.
- A security event, insider threat concern, suspected misconduct, policy violation, complaint, audit finding, or credentialing issue requires immediate access suspension or heightened monitoring.
- A business associate, subcontractor, vendor, consultant, temporary staffing agency, AI provider, or support user relationship ends or changes.
- An AI tool, AI agent, model environment, service account, script, API key, data connector, or automation changes owner or no longer has an approved business purpose.
- The organization's workforce clearance procedure determines that access to ePHI is no longer appropriate.

4.2 Termination Categories and Minimum Timing Standards

Category	Examples	Minimum Access Action	Target Timing
Scheduled voluntary termination	Resignation, retirement, planned end of assignment, planned contract end.	Plan offboarding in advance; remove nonessential access before final day; disable all ePHI access at the end of the final authorized work period.	No later than the end of final authorized work period; earlier where access is no longer needed.

Category	Examples	Minimum Access Action	Target Timing
Involuntary or high-risk termination	Termination for cause, hostile separation, suspected misconduct, insider threat, investigation, security-sensitive role.	Disable IdP/SSO, MFA, VPN, EHR, email, cloud, chat, AI, privileged access, remote sessions, device trust, and physical access before or at notice; preserve evidence.	Before notice when feasible; otherwise immediately at notice.
Immediate suspension / administrative leave	Investigation leave, license issue, compliance concern, urgent patient safety concern.	Suspend all access unless Security, Privacy, Legal, and HR approve limited access in writing; preserve logs and evidence.	Immediately when suspension begins.
Role change / transfer	Promotion, demotion, department transfer, temporary coverage ending, credential change.	Remove old role access before granting new access where feasible; revalidate least privilege and minimum necessary.	Before effective role change or same business day.
Contractor or vendor end	End of statement of work, temporary worker release, support account no longer needed.	Disable named/vendor access; revoke remote support; rotate shared credentials; verify subcontractor access removal where applicable.	No later than contract end or earlier when access no longer needed.
Privileged user, AI owner, developer, or administrator departure	System administrator, database admin, AI admin, data scientist, API owner, DevOps owner, integration owner.	Disable privileged and AI access; transfer artifacts; revoke API keys and tokens; rotate secrets; review pipelines, agents, notebooks, and admin logs.	Before notice for high-risk; otherwise before the final authorized work period ends.
Service account or automation owner change	Bot account, AI agent, RPA process, scheduled job, interface account.	Reassign owner, update credential custody, rotate secrets if known by departing user, validate logging and business approval.	Before owner departure or within approved change window.

Template Timing Standard
HIPAA currently requires termination procedures but does not prescribe one universal minute-by-minute access removal timeframe for every termination event. This template establishes internal timing standards. The 2025 HIPAA Security Rule NPRM proposed a one-hour outer limit for terminating workforce access after an arrangement ends and a 24-hour notification requirement to certain other regulated entities; that proposed language should be treated as readiness planning unless finalized.

4.3 Required Offboarding Ticket or Workflow

- All terminations, suspensions, role changes, contractor ends, vendor access removals, and AI ownership changes shall be processed through an approved ticket, workflow, form, or case record.
- Email-only requests are not sufficient unless converted into an approved ticket or form before closure.
- The workflow must identify the user, role, department, manager, termination category, effective date/time, systems used, AI tools used, devices/assets issued, physical access, vendor portals, privileged access, service accounts, and whether the event is high-risk.
- The workflow must assign tasks to HR, supervisor, IT/IAM, Security, Privacy, Facilities, AI system owners, vendor management, and other system owners as applicable.
- The workflow must track timestamps, responsible persons, completed actions, evidence, exceptions, approvals, and final certification.
- The workflow must not be closed until electronic access, physical access, assets, AI artifacts, privileged access, secrets, and vendor access have been addressed or documented as approved exceptions.

4.4 Minimum Systems and Access to Review

Access Area	Examples to Review and Remove, Modify, Transfer, Revoke, or Rotate
Identity and authentication	IdP, SSO, MFA factors, passkeys, hardware tokens, smartcards, password reset access, authentication apps, delegated authentication, emergency/break-glass access, device trust, browser session trust.
Clinical and healthcare systems	EHR/EMR, patient portal, HIE, scheduling, care management, telehealth, pharmacy, lab/LIS, imaging/PACS, referrals, quality reporting, clinical registries.
Business and revenue cycle systems	Billing, coding, claims, clearinghouse portals, eligibility, prior authorization, collections, payment systems, accounting systems with ePHI, CRM systems with patient data.
Communication and collaboration	Email, secure messaging, chat, video, file shares, shared drives, cloud storage, intranet, fax, voicemail, call center, printers, scanners, copier address books, e-signature systems.
Remote access and network	VPN, VDI, RDP, SSH, privileged remote support, wireless access, firewall/VPN groups, third-party remote support tools, admin jump boxes, bastion hosts.
Devices and endpoints	Laptop, desktop, tablet, mobile phone, removable media, encrypted drives, BYOD work profile, MDM/EDR enrollment, browser profiles, cached credentials, local files, offline files.
Cloud, SaaS, and data platforms	Cloud console, SaaS apps, data warehouse, databases, backup portals, dashboards, BI/analytics, logs, secrets vaults, DevOps, code repositories, data lake storage.
AI and automation	AI assistants, scribe/transcription, predictive decision support, RPA bots, AI agents, model platforms, vector stores, prompt libraries, data connectors, API keys, notebooks, datasets, governance tools.
Physical access	Facility badge, keys, alarm code, secure rooms, medication rooms, server rooms, file rooms, parking, lockers, biometric access, printer/copier release access.
Vendor and business associate portals	Vendor support accounts, BA user accounts, subcontractor access, shared credentials, remote service accounts, support call-back lists, AI vendor dashboards.
Secrets and shared credentials	Database passwords, API keys, SSH keys, certificates, encryption keys, service account secrets, integration tokens, shared inbox passwords, shared AI API keys, local admin passwords.

4.5 Account Disablement, Transfer, and Preservation Requirements

- **Disable before deleting.** Accounts must be disabled before deletion unless records, logs, files, legal hold, business continuity, and audit requirements have been satisfied.
- **Revoke active sessions.** Revoke refresh tokens, OAuth grants, application passwords, MFA registrations, device trust, passkeys, API tokens, browser sync, and persistent sessions where technically feasible.
- **Remove roles and memberships.** Remove the user from security groups, EHR roles, distribution lists, shared mailboxes, delegated calendars, AI tool groups, project spaces, and privileged access groups.
- **Transfer ownership.** Transfer ownership of files, mailboxes, calendars, tasks, dashboards, work queues, repositories, automations, AI agents, prompt libraries, notebooks, datasets, vector stores, and model deployments before disabling or deleting accounts where needed for business continuity.

- **Preserve evidence.** Preserve audit logs, access history, relevant emails, files, prompt/output histories, notebooks, model artifacts, endpoint telemetry, and system records when an investigation, incident, litigation hold, audit, subpoena, complaint, or regulatory inquiry is possible.
- **Use named accounts.** Access to ePHI must be attributable to unique users or approved service accounts with named business and technical owners.

4.6 Confidentiality and Return of ePHI

- The workforce member must return all organization equipment, documents, records, badges, keys, tokens, smartcards, removable media, notes, printed reports, screenshots, exports, or copies containing PHI or ePHI.
- The workforce member must certify that no ePHI, credentials, proprietary prompts, AI outputs, model artifacts, datasets, downloads, screenshots, images, recordings, transcripts, or backups are retained in personal email, personal cloud storage, personal AI accounts, personal devices, external drives, messaging apps, or paper files.
- The organization may inspect, wipe, quarantine, lock, or forensically preserve organization-managed devices and approved BYOD work profiles according to policy, legal requirements, and consent agreements.
- Any suspected retention, forwarding, copying, printing, downloading, photographing, external sharing, or exfiltration of ePHI must be escalated to the Security Officer and Privacy Officer for investigation.

4.7 Shared Accounts and Emergency Access

- Shared accounts that access ePHI are prohibited unless approved by the Security Officer, risk assessed, technically necessary, and controlled with named check-out, MFA where feasible, logging, password rotation, and owner certification.
- If a terminated user knew any shared passwords, service credentials, encryption secrets, API keys, emergency credentials, administrator passwords, or AI platform keys, those secrets must be rotated immediately or according to a documented risk-based timetable approved by Security.
- Emergency access shall be provided only through the approved emergency access procedure to active authorized workforce members. A terminated person shall not be granted emergency access unless rehired or formally reauthorized under written policy.

4.8 Exceptions and Risk Acceptance

- Any request to delay access termination or allow continued access after termination, contract end, suspension, or role change must be documented and approved before access continues.
- Exceptions are not allowed for high-risk involuntary separations unless Legal, Security, and executive leadership jointly approve an alternative control in writing.
- Exceptions must identify the business need, ePHI involved, systems affected, duration, compensating controls, monitoring, responsible owner, approval signatures, and expiration date.
- Exceptions shall be time-limited and reviewed at least daily for high-risk cases and no less than weekly for other cases.
- A manager's preference, convenience, or lack of planning is not sufficient justification for continued ePHI access.

5. Termination and Access Revocation Procedures

Procedure Flow
1. HR or manager initiates event -> 2. Supervisor identifies access and risk -> 3. Security/IT prepares offboarding -> 4. Accounts and physical access are disabled -> 5. Devices and records are recovered -> 6. AI tools, agents, and automations are transferred or disabled -> 7. Logs are reviewed -> 8. Evidence is retained.

5.1 Standard Scheduled Termination Procedure

1. HR or the supervisor submits the termination workflow as soon as the separation date is known, preferably at least five business days before the last working day when feasible.
2. The supervisor identifies all systems, datasets, physical areas, devices, vendor portals, shared workspaces, AI tools, automations, delegated access, service accounts, and projects used by the workforce member.
3. IT/IAM prepares a deprovisioning plan and confirms whether the user has privileged access, service account ownership, API keys, delegated mailbox access, AI artifacts, or automation ownership requiring transfer.
4. The supervisor coordinates business handoff and confirms that continued access is not needed after the final authorized work period.
5. At the scheduled access removal time, IT disables SSO/IdP access, EHR access, network access, remote access, AI access, cloud/SaaS accounts, email access, chat access, and other assigned systems.
6. Facilities disables physical access and confirms return or replacement of badges, keys, smartcards, parking access, alarm codes, and physical tokens.
7. IT or the manager collects organization devices and media. For remote users, IT initiates return shipping, remote lock, encryption verification, or remote wipe as appropriate.
8. AI system owners transfer ownership of AI agents, prompt libraries, shared chats, notebooks, datasets, dashboards, model deployments, vector stores, and automations to an active authorized owner.
9. The supervisor collects written certification that no ePHI, credentials, AI artifacts, prompts, outputs, screenshots, exports, or copies are retained by the departing user.
10. Security reviews deprovisioning evidence, resolves exceptions, and performs post-termination log review according to risk level.
11. The workflow is closed only after all required tasks have completion evidence, owner sign-off, and exception approval if any access remains.

5.2 Involuntary, High-Risk, or Security-Sensitive Termination Procedure

- **Coordinate quietly before notice.** HR, Legal, Security, IT, Facilities, the supervisor, and AI system owner shall coordinate before the termination meeting. Do not alert the individual before access controls are ready unless required by law or approved by Legal.
- **Disable first.** Disable IdP/SSO, VPN, EHR, cloud, email, chat, AI, privileged access, remote sessions, device trust, and physical access before or at the time of notice.
- **Preserve evidence.** Preserve relevant logs, endpoint telemetry, email, file activity, access history, AI prompt/output history, API usage, DLP alerts, badge logs, and device images when a security or privacy concern exists.
- **Recover assets and escort.** Recover badges, keys, devices, tokens, and paper/electronic records. Use an escort, remote lock, or remote wipe where appropriate.
- **Rotate secrets.** Rotate passwords, shared credentials, API keys, SSH keys, certificates, service account secrets, local admin credentials, and AI integration keys known to or controlled by the user.
- **Review activity.** Security shall review recent access, exports, downloads, printing, email forwarding, file sharing, AI prompts/outputs, cloud sharing, remote access, and physical access logs based on risk level.
- **Escalate incidents.** If unauthorized access, data exfiltration, malware, sabotage, retained ePHI, personal AI disclosure, or impermissible disclosure is suspected, activate the Security Incident Response and Breach Risk Assessment procedures.

High-Risk Control	Required Action	Evidence
Pre-notice access lock	Disable SSO/IdP, privileged access, remote access, EHR, email, cloud, and AI access before or during notice.	Timestamped IAM report, ticket, screenshot, or system export.
Session revocation	Terminate active sessions and revoke refresh tokens, OAuth grants, device trust, and application passwords.	IdP/session revocation log.

High-Risk Control	Required Action	Evidence
Endpoint containment	Lock, isolate, wipe, recover, or preserve devices as appropriate.	MDM/EDR action record or forensic chain of custody.
AI/API containment	Revoke AI seats, API keys, agents, connectors, notebooks, data pipelines, and model deployment rights.	AI admin export, key rotation record, owner transfer record.
Physical access removal	Disable badge, alarm code, secure room access, parking access, and keys; recover or rekey when needed.	Access control report, key receipt, rekey record.
Log review	Review activity based on risk: last 7, 30, or 90 days; expand scope if suspicious activity is found.	Log review checklist and findings.

5.3 Role Change, Transfer, Leave, or Suspension Procedure

- HR or the supervisor submits a role-change, transfer, leave, or suspension workflow before the effective date or immediately when the change is unplanned.
- The supervisor identifies old access that is no longer minimum necessary and new access required for the new role.
- IT removes old access before granting new access where feasible. Old department groups, EHR roles, shared drives, delegated mailbox access, dashboards, vendor portals, and AI tools must be removed or modified.
- For leave or suspension, access is suspended unless the Security Officer, Privacy Officer, Legal, and HR approve limited continued access in writing.
- AI agents, dashboards, reports, notebooks, prompt libraries, and automations owned by the workforce member must be transferred to an active owner or suspended.
- The supervisor and IT certify completion and retain evidence in the access management system.

5.4 Data Handoff, Legal Hold, and Business Continuity

- Before disabling accounts, determine whether email, files, calendars, clinical work queues, patient messages, claims, tickets, dashboards, AI agents, automations, or model artifacts must be transferred to an active authorized owner.
- Access to a former workforce member's mailbox, files, or work product shall be granted only through approved procedures, documented authorization, and minimum necessary access.
- Legal hold must be applied before deletion or alteration of relevant data when litigation, investigation, employment dispute, security incident, breach investigation, audit, subpoena, or regulatory inquiry is reasonably anticipated.
- If the former workforce member managed critical systems or AI automations, verify that patient care, billing, claims, prescriptions, lab results, on-call coverage, security monitoring, and incident response capabilities continue without unauthorized access.

5.5 Post-Termination Monitoring

Timeframe	Monitoring Activity	Responsible Role	Evidence
Day 0	Verify that all known electronic, physical, remote, privileged, vendor, and AI access is disabled, modified, transferred, or documented as approved exception.	IT/IAM, Facilities, AI System Owner	Completed checklist, account export, badge report.
Day 1	Review failed logins, remote access attempts, email forwarding, cloud sharing, EHR access, VPN/VDI, AI/API usage, and endpoint check-in.	Security / SOC	Log review record and findings.

Timeframe	Monitoring Activity	Responsible Role	Evidence
Day 7	Confirm no orphaned access, active sessions, shared links, delegated mailboxes, external shares, active API keys, or running AI agents remain.	IT/IAM, Security, AI Owner	Audit results and remediation records.
Day 30	Review a sample of terminations for SLA compliance, evidence completeness, exceptions, and unresolved access.	Security Officer / Compliance	Monthly termination access audit.
Quarterly	Reconcile HR active roster to system access lists, privileged access lists, vendor users, and AI system users.	Security, HR, IT	Access review attestation.

6. AI Use and AI Offboarding Requirements

AI use creates additional termination risk because ePHI may be stored or reflected in prompt histories, outputs, transcripts, model training data, embeddings, vector stores, notebooks, cached files, data connectors, AI agents, and API integrations. This policy treats AI-enabled systems that interact with ePHI as part of the ePHI environment for access management, audit, termination, and incident response purposes.

6.1 AI Use Baseline Controls

- Workforce members may use AI tools with ePHI only when the tool is approved, risk assessed, covered by appropriate agreements where required, configured for organizational control, and included in access management and audit procedures.
- Workforce members shall not input, paste, upload, dictate, screen-share, photograph, or otherwise provide PHI/ePHI to public or personal AI tools unless the tool has been approved for that purpose by [Organization Name].
- AI tools that create, receive, maintain, transmit, process, summarize, analyze, or store ePHI must use named accounts, role-based access, MFA where feasible, logging, approved retention settings, vendor review, incident reporting, and a documented system owner.
- AI outputs containing individually identifiable health information are treated as PHI/ePHI and must be protected, retained, disclosed, and disposed of according to organizational policy.
- AI systems must be included in inventory, risk analysis, business associate review where applicable, access review, offboarding, incident response, and audit procedures.

6.2 AI Offboarding Risk Scenarios

Risk Scenario	Potential Harm	Required Control
Terminated user still has access to an AI assistant or scribe account.	The former user may view or generate summaries of patient data, transcripts, or clinical notes.	Disable AI account, revoke sessions, remove from groups, review prompt/output history.
AI agent continues running under the former user's identity or API key.	Automated access to ePHI may continue without an accountable active owner.	Stop or reassign agent, rotate API key, update owner, validate logs and data connectors.
Prompt history contains patient identifiers or clinical details.	Former user or vendor support staff could retain or view PHI.	Ensure prompt/output history remains under organization control; restrict, export, retain, or delete according to policy and legal hold.
Former user owns a vector database, embeddings, notebook, fine-tuned model, or dataset.	ePHI or derived data may be retained outside approved ownership and access controls.	Transfer ownership; review data lineage; apply retention or secure destruction; remove user rights.

Risk Scenario	Potential Harm	Required Control
Former user had access to AI vendor admin console.	User could change retention settings, view logs, export data, alter connectors, or grant access.	Remove admin role, rotate secrets, review admin actions, verify no unknown users or connectors.
AI tool is connected to email, EHR, shared drive, or ticketing system.	Terminated user's delegated OAuth tokens or connectors may remain active.	Revoke OAuth grants, remove connector permissions, validate data source access through system owner.
Personal AI account was used improperly with PHI.	Possible unauthorized disclosure and loss of control over PHI.	Escalate as security incident/privacy event; investigate scope; preserve evidence; conduct breach risk assessment as needed.

6.3 AI Offboarding Procedure

12. Identify whether the workforce member used or administered AI-enabled systems, including approved enterprise AI, EHR AI modules, clinical decision support, scribe/transcription tools, coding/claims AI, data science platforms, AI APIs, AI agents, chatbots, RPA bots, and developer/model environments.
13. Disable the user's AI application accounts and remove group memberships, admin roles, model deployment privileges, data science workspace access, and AI governance roles.
14. Revoke active sessions, OAuth grants, browser extensions, connected app permissions, API tokens, secret vault entries, API keys, service credentials, and model hosting tokens associated with the user.
15. Transfer ownership of prompt libraries, shared chats, model artifacts, notebooks, datasets, vector stores, dashboards, automations, RPA bots, AI agents, and data connectors to an active authorized owner.
16. Review prompt/output histories, transcripts, model logs, export logs, data connector logs, and API usage for ePHI access, unusual downloads, unusual external sharing, or post-notice activity.
17. Stop or reassign any AI automation running under the user's identity. Validate that no scheduled jobs, data pipelines, agents, or bots continue to use the user's credentials.
18. Verify AI vendor portals and subcontractor environments have removed the user if vendor-managed access exists.
19. Document completion, evidence, exceptions, and follow-up actions in the offboarding workflow.

6.4 AI-Specific System Inventory Fields

Inventory Field	Description
AI tool name and owner	Product/service name, business owner, technical owner, privacy owner, and security owner.
Purpose and data types	Authorized use case, ePHI data elements, special data categories, minimum necessary limits, source systems.
Access model	Named users, groups, admin roles, service accounts, APIs, SSO/MFA status, vendor support access.
Data storage and retention	Prompt/output retention, transcripts, logs, training/fine-tuning restrictions, deletion capabilities, export controls.
Connectors and integrations	EHR, email, shared drive, chat, ticketing, data warehouse, APIs, RAG/vector store, workflow automations.
Vendor/BAA status	Vendor risk review, BAA or contract status, subcontractor involvement, security incident reporting obligations.
Audit and monitoring	Available logs, admin audit, prompt/API logs, export logs, DLP, SIEM integration, review cadence.

Inventory Field	Description
Offboarding actions	Required steps to disable user, revoke token, transfer owner, stop agent, rotate keys, preserve/delete histories.

AI Rule of Thumb
If a user can access ePHI through an AI tool, the AI tool must be listed in the offboarding checklist. If a user owns an automation or key that can access ePHI, that automation or key must be transferred, disabled, or rotated.

7. Contractor, Vendor, Business Associate, and Third-Party Access Termination

Vendor and contractor access must be governed with the same discipline as workforce access. Access must be tied to named users whenever possible, reviewed against business need, documented, and removed when the engagement ends or when the individual no longer needs access.

- The business owner must notify vendor management and IT when a contract, statement of work, support relationship, AI vendor arrangement, or specific user access ends.
- The organization must request and retain written confirmation that the vendor, business associate, or subcontractor disabled the named user's access to ePHI and related systems.
- If the vendor uses AI or automation to process ePHI, the termination notice must require removal of the user from AI tools, AI support environments, model development environments, prompt/output stores, support queues, customer data environments, and subcontractor systems.
- If shared credentials or support tokens were known to the vendor user, rotate those credentials and verify no active sessions remain.
- If the vendor relationship ends, follow the BAA and contract terms for return or destruction of PHI, data retention, breach reporting, security incident reporting, contingency notification, subcontractor controls, and transition support.
- Vendor access reviews must be performed periodically and compared against current contracts, named users, support tickets, remote access logs, and business owner attestations.

Third-Party Access Area	Termination Control	Evidence
Named vendor account	Disable named account in organization and vendor systems.	System export, vendor confirmation.
Remote support access	Disable VPN, support portal, remote desktop, PAM, jump host, and callback access.	Access report, PAM log, ticket.
Shared vendor credential	Rotate credential, revoke sessions, update vault owner, document who knew it.	Vault rotation record.
AI vendor workspace	Remove user, revoke admin rights, preserve prompt/output logs if required, confirm subcontractor removal.	AI vendor admin export, written confirmation.
Data return/destruction	Confirm return, destruction, retention limitation, or transition according to BAA/contract.	Certificate, contract record, legal approval.
Security incident concern	Open incident, preserve logs, notify Privacy/Legal, conduct breach analysis as needed.	Incident ticket, investigation record.

8. Documentation, Evidence, Retention, and Legal Hold

The organization shall maintain written or electronic documentation of this policy, procedures, required actions, approvals, exceptions, security incidents, risk assessments, and access termination evidence. Documentation shall be retained according to the HIPAA Security Rule documentation requirements and the organization's record retention schedule.

8.1 Required Evidence

Evidence Type	Examples
Workflow/ticket record	Termination ticket, role change ticket, suspension record, vendor access removal request, AI offboarding task, high-risk coordination note.
Access removal proof	IdP/SSO deactivation export, EHR role removal report, VPN disabled report, MDM wipe confirmation, cloud account status, AI admin portal export.
System owner certification	Supervisor certification, IT certification, AI owner transfer certification, vendor confirmation, facilities access removal confirmation.
Asset return evidence	Laptop return receipt, mobile device return, key/badge return, token return, media log, remote wipe confirmation.
Secret rotation records	API key rotation, password vault update, certificate/key change, service account credential rotation, shared credential rotation.
Monitoring and audit logs	Post-termination login attempts, EHR access review, AI/API usage review, email forwarding review, file sharing review, DLP alert review.
Exception approvals	Risk acceptance form, compensating controls, expiration date, executive approval, Security/Privacy/Legal approval if required.
Incident response records	Security incident ticket, investigation notes, breach risk assessment, mitigation steps, communications, lessons learned.

8.2 Documentation Retention

- Maintain this policy and related procedures for at least six years from the date of creation or the date when the document last was in effect, whichever is later, unless a longer period is required by law, contract, litigation hold, or organizational policy.
- Maintain required action records, assessments, access termination evidence, security incident records, exception records, access reviews, and owner certifications in written or electronic form.
- Make the policy and procedure available to persons responsible for implementation, including HR, Security, IT, Facilities, Privacy, Compliance, Vendor Management, AI owners, and system owners.
- Review and update documentation periodically and when environmental or operational changes affect ePHI security, including new systems, AI tools, vendors, remote work methods, identity platforms, role structures, or legal changes.
- **Legal hold overrides routine deletion.** Do not delete or alter accounts, logs, devices, email, AI prompt/output histories, or files that are subject to preservation instructions.

8.3 Evidence Quality Standards

Evidence Standard	Requirement

Evidence Standard	Requirement
Timestamped	Evidence should show when the action occurred or when the report was generated.
Attributable	Evidence should identify the system, user/account, reviewer, and person who completed the action.
Complete	Evidence should cover all assigned systems, not only the IdP or EHR.
Readable	Screenshots and exports must be legible, organized, and linked to the termination record.
Tamper resistant	Where feasible, logs and evidence should be retained in systems with access controls and change history.
Reviewable	Evidence should allow an auditor to determine whether access was removed within the policy timeframe.

9. Training, Testing, Auditing, and Review

9.1 Training Requirements

- HR, supervisors, IT, Facilities, Security, Privacy, Compliance, Vendor Management, and AI system owners shall be trained on their termination responsibilities.
- Workforce members shall receive security awareness training that includes confidentiality after termination, password safeguards, reporting lost/stolen devices, prohibition on retaining ePHI, and responsible AI use.
- Managers shall be trained to report terminations and role changes promptly and to identify all access, devices, AI tools, automations, shared workspaces, and vendor portals used by the workforce member.
- Privileged users, AI developers, analysts, and administrators shall receive additional training on API keys, service accounts, AI artifacts, prompt/output retention, data connectors, model ownership, and secure handoff.
- Vendor owners shall be trained to request vendor-side removal and retain written confirmation when named users, support accounts, or subcontractor users no longer need access.

9.2 Testing and Auditing

Audit Area	Minimum Test
HR-to-IAM reconciliation	Compare HR active roster to active user accounts in IdP, EHR, VPN, cloud, email, AI platforms, and major vendor portals. Investigate exceptions.
Termination SLA	Sample terminated users and verify access removal occurred within approved policy timeframes or documented approved exceptions.
Evidence completeness	Verify each sampled termination has ticket, system access evidence, physical access evidence, asset return, AI review where applicable, and final certification.
Privileged access	Verify privileged accounts, admin roles, break-glass access, service account ownership, API keys, and shared secrets were removed, reassigned, or rotated.
AI offboarding	Verify AI accounts, prompt histories, agents, vector stores, notebooks, data connectors, and API keys were disabled, transferred, retained, or deleted according to policy.

Audit Area	Minimum Test
Vendor access	Verify vendor/business associate users were removed and confirmations retained.
Post-termination activity	Review failed logins, EHR access, VPN, email, cloud file access, AI/API usage, and badge attempts after termination.
Exception management	Verify exceptions were approved, time-limited, monitored, and closed.

9.3 Policy Review and Maintenance

- The Security Officer shall review this policy at least annually and after material changes to systems, workforce structure, AI tools, vendor relationships, laws, regulations, OCR guidance, risk analysis results, or security incidents.
- The organization shall update system-specific offboarding lists whenever new ePHI systems, AI tools, cloud services, vendors, integrations, or access methods are introduced.
- The Compliance Committee or equivalent governance body shall review trends in termination exceptions, failed access attempts, delayed deprovisioning, missing evidence, and AI offboarding gaps.
- Audit results must be tracked to remediation plans with responsible owners, target dates, completion evidence, and risk acceptance where remediation is delayed.

9.4 Proposed-Rule Readiness Addendum

Planning Only
This addendum is included for planning only. It should not be represented as final regulatory text. The organization should review final rules before changing compliance statements or asserting that proposed requirements are legally effective.

Readiness Topic	Suggested Preparatory Action
One-hour access termination objective	Configure ticketing, IAM automation, HR notifications, and high-risk workflows so workforce access can be terminated promptly and measured against a one-hour readiness target if a final rule requires it.
24-hour notification to other regulated entities	Identify circumstances where a workforce member uses another covered entity's or business associate's ePHI systems and prepare a notification template.
Required written documentation	Centralize written policies, procedures, plans, access change records, AI offboarding records, and evidence.
Annual compliance audits	Use Appendix N as a starting audit script and expand testing to all Security Rule safeguards.
Asset inventory and network map	Ensure systems, AI tools, APIs, service accounts, data flows, and vendor portals used during offboarding are included in the inventory and network map.
MFA and encryption	Validate MFA for workforce, privileged, remote, cloud, vendor, and AI access and encryption for ePHI at rest and in transit.
Vulnerability scanning and penetration testing	Include IAM, remote access, AI platforms, cloud consoles, and ePHI repositories in scanning/testing scope.

Readiness Topic	Suggested Preparatory Action
Network segmentation and technical controls	Segment critical ePHI systems and AI environments; remove extraneous software and disable unneeded access paths.

10. Appendices: Checklists, Forms, Logs, Notices, and Audit Tools

Appendix Use
The appendices are designed to be copied into a ticketing system or used as paper/electronic forms. Keep completed forms with the termination record and Security Rule documentation.

Appendix A - Termination Event Intake Form

Field	Entry
Workforce member / account name	_____
User ID(s)	_____
Job title / department	_____
Manager / business owner	_____
Termination or change type	Voluntary / Involuntary / Transfer / Leave / Suspension / Contractor / Vendor / AI owner change
Last authorized work date/time	_____
Effective access removal date/time	_____
High-risk? Yes / No	_____
Privileged access? Yes / No	_____
AI tools or automations used? Yes / No	_____
Remote user? Yes / No	_____
Legal hold needed? Yes / No	_____
Incident suspected? Yes / No	_____
HR ticket number	_____
IT/Security ticket number	_____

Appendix B - Workforce Termination Offboarding Checklist

Status	Task / Control	Owner	Evidence / Notes
[ ]	HR submitted termination workflow with effective date/time and termination category.	HR	

Status	Task / Control	Owner	Evidence / Notes
[ ]	Supervisor identified all systems, devices, shared workspaces, AI tools, automations, privileged rights, and vendor portals used by the workforce member.	Supervisor	
[ ]	High-risk determination completed and Security/Legal notified if applicable.	HR / Security	
[ ]	IdP/SSO account disabled or scheduled for disablement.	IT/IAM	
[ ]	EHR/EMR and clinical system access disabled.	System Owner	
[ ]	VPN/VDI/RDP/remote access disabled and active sessions revoked.	IT/IAM	
[ ]	Email, chat, cloud storage, shared drives, secure messaging, and delegated access removed or transferred.	IT/IAM	
[ ]	AI accounts, AI agents, prompt libraries, notebooks, API keys, and AI data connectors disabled, transferred, or rotated.	AI Owner / IT	
[ ]	Privileged access, admin roles, service account ownership, password vault access, and API secrets reviewed and removed or rotated.	Security / IT	
[ ]	Vendor portals, clearinghouse portals, billing/coding systems, and third-party support access removed.	Vendor Owner / IT	
[ ]	Badge, keys, smartcards, tokens, alarm codes, and physical access removed.	Facilities	
[ ]	Laptop, mobile device, tablet, removable media, paper records, and organization property returned, locked, or wiped.	IT / Manager	
[ ]	Mailbox, files, calendars, tasks, dashboards, work queues, and patient messages transferred according to approval.	Supervisor / IT	
[ ]	Workforce member signed confidentiality and no-retention certification.	HR / Manager	
[ ]	Post-termination log review completed.	Security	
[ ]	All exceptions documented and approved, or no exceptions exist.	Security Officer	
[ ]	Final closure certification completed.	Security / IT / HR	

Appendix C - Emergency / High-Risk Termination Checklist

Status	Task / Control	Owner	Completion Time / Evidence
[ ]	HR/Legal/Security/IT pre-termination coordination completed.	HR / Legal / Security	

Status	Task / Control	Owner	Completion Time / Evidence
[ ]	SSO/IdP disabled before or at notice.	IT/IAM	
[ ]	EHR/EMR, VPN, email, cloud, chat, AI, and privileged access disabled.	IT/IAM / System Owners	
[ ]	Active sessions, OAuth grants, device trust, MFA factors, passkeys, and tokens revoked.	IT/IAM	
[ ]	Devices isolated, recovered, locked, wiped, or forensically preserved.	Security / IT	
[ ]	Shared credentials, API keys, AI tokens, certificates, local admin passwords, and service account secrets rotated.	Security / IT	
[ ]	Physical access disabled and security escort arranged if onsite.	Facilities / HR	
[ ]	Email forwarding, external sharing, DLP alerts, downloads, printing, EHR access, AI prompt/API logs reviewed.	Security / Privacy	
[ ]	Security incident opened if suspicious activity or unauthorized ePHI access is suspected.	Security Officer	
[ ]	Privacy Officer notified for potential impermissible use/disclosure or breach risk assessment.	Security / Privacy	
[ ]	Evidence preserved under legal hold or incident response process if needed.	Legal / Security	

Appendix D - Role Change, Transfer, Leave, or Suspension Checklist

Status	Task / Control	Owner	Evidence / Notes
[ ]	Old role access identified and reviewed for removal.	Supervisor / IT	
[ ]	New role access approved based on minimum necessary and role-based access.	Supervisor / System Owner	
[ ]	Old EHR roles, shared drive groups, dashboards, queues, distribution lists, and vendor portals removed.	IT / System Owners	
[ ]	AI tools, agents, notebooks, prompts, and automations transferred or modified.	AI Owner	
[ ]	Access suspended for leave or investigation unless approved exception exists.	IT / HR / Security	
[ ]	Post-change access review completed.	Security / Supervisor	

Appendix E - Contractor, Vendor, and Business Associate Termination Checklist

Status	Task / Control	Owner	Evidence / Notes
[ ]	Business owner notified vendor management and IT of end date/time.	Business Owner	
[ ]	Named vendor users disabled in organization systems.	IT/IAM	
[ ]	Vendor-controlled accounts disabled and written confirmation obtained.	Vendor Manager	
[ ]	Remote support tools, VPN, vendor portals, admin consoles, and support groups disabled.	IT / Vendor Manager	
[ ]	Shared support credentials, API tokens, certificates, and secrets rotated.	Security / IT	
[ ]	AI vendor access, AI support logs, model environments, and subcontractor access reviewed and removed.	AI Owner / Vendor Manager	
[ ]	Return/destruction of PHI/ePHI verified if relationship ended.	Privacy / Legal / Vendor Manager	
[ ]	BAA/security incident reporting obligations reviewed.	Compliance / Legal	

Appendix F - AI Tool and Automation Offboarding Form

Field	Entry
AI tool / platform name	_____
AI system owner	_____
Departing user	_____
User role in AI system	_____
Does AI tool process ePHI? Yes / No	_____
BAA/vendor review status	_____
Prompt/output retention setting	_____
API keys or service accounts involved	_____
Data connectors involved	_____
Vector store / embeddings involved	_____

Appendix F1 - AI Offboarding Checklist

Status	Task / Control	Owner	Evidence / Notes
[ ]	AI application user account disabled and sessions revoked.	AI Owner / IT	
[ ]	AI admin role, workspace role, model deployment role, and project role removed.	AI Owner	
[ ]	Prompt history, output history, transcripts, and chat histories reviewed for ePHI and retained/deleted according to policy.	AI Owner / Privacy	
[ ]	Ownership of shared prompts, prompt libraries, AI agents, chatbots, RPA bots, and automations transferred.	AI Owner	
[ ]	Notebooks, datasets, vector databases, embeddings, retrieval indexes, fine-tuning files, and model artifacts transferred or secured.	AI Owner / Data Owner	
[ ]	API keys, service credentials, OAuth grants, connected app permissions, and data connectors revoked or rotated.	Security / IT	
[ ]	Automated jobs, agents, model pipelines, and scheduled workflows stopped or reassigned to an approved service account.	AI Owner / IT	
[ ]	Vendor/subcontractor AI access removed and confirmation retained if applicable.	Vendor Manager	
[ ]	AI/API logs reviewed for unusual access, exports, sharing, or post-termination activity.	Security / AI Owner	
[ ]	No personal AI account, personal storage, or personal device retention detected or reported.	Supervisor / Security	

Appendix G - Privileged Access and Secrets Rotation Checklist

Privileged Item	Action Required	Owner	Evidence
Admin account	Disable, remove roles, revoke sessions, confirm no active login.	IT/IAM	PAM/IAM export.
Break-glass credential	Confirm user did not know credential or rotate immediately.	Security	Vault rotation record.
API key / token	Revoke or rotate; update integration owner; review usage logs.	Security / DevOps	Key rotation record.
Service account owner	Reassign owner; validate purpose, least privilege, logging, and expiration.	IT / System Owner	Owner transfer record.
SSH key / certificate	Remove authorized keys; revoke certificates; rotate secrets.	IT / Security	Certificate/key record.
Database credential	Remove user, rotate shared credentials, review query logs.	DBA / Security	DB export / vault log.
AI platform key	Revoke or rotate; confirm no agents use old key.	AI Owner / Security	AI admin log.

Privileged Item	Action Required	Owner	Evidence
Code repository	Remove access; rotate deploy keys; review recent commits and secrets.	DevOps / Security	Repository audit log.

Appendix H - Asset Return and Media Sanitization Log

Asset / Media	Asset ID / Serial	Returned?	Action	Date / Owner / Evidence
Laptop	[Insert]	Yes / No / N/A	Returned / locked / wiped / forensic hold	[Insert]
Mobile phone / tablet	[Insert]	Yes / No / N/A	Returned / wiped / BYOD profile removed	[Insert]
Removable media	[Insert]	Yes / No / N/A	Returned / sanitized / destroyed	[Insert]
Badge / key / token / smartcard	[Insert]	Yes / No / N/A	Returned / disabled / replaced	[Insert]
Paper records / notes	[Insert]	Yes / No / N/A	Returned / shredded / archived	[Insert]
Other	[Insert]	Yes / No / N/A	[Insert]	[Insert]

Appendix I - Post-Termination Audit Log

Review Date	System / Log Source	Review Period	Findings	Reviewer / Evidence
[Insert]	IdP/SSO failed logins and sessions	[Insert]	[Insert]	[Insert]
[Insert]	EHR/EMR access log	[Insert]	[Insert]	[Insert]
[Insert]	VPN/remote access log	[Insert]	[Insert]	[Insert]
[Insert]	Email forwarding / external sharing / cloud download log	[Insert]	[Insert]	[Insert]
[Insert]	AI prompt/API/agent activity log	[Insert]	[Insert]	[Insert]
[Insert]	Badge/physical access attempt log	[Insert]	[Insert]	[Insert]
[Insert]	DLP/EDR/SIEM alerts	[Insert]	[Insert]	[Insert]

Appendix J - Confidentiality and No-Retention Certification

I certify that I have returned all organization property and have not retained any PHI/ePHI, credentials, files, screenshots, reports, notes, messages, recordings, transcripts, AI prompts, AI outputs, model artifacts, datasets, downloads, backups, or copies in any personal account, personal device, external storage, paper file, personal AI tool, or unauthorized system. I understand that confidentiality obligations continue after my employment, assignment, contract, or access authorization ends.

Field	Entry
Workforce member / user	_____
Department / organization	_____
Date	_____
Signature	_____
Witness / HR representative	_____
Notes / exceptions	_____

Appendix K - Exception / Risk Acceptance Form

Use this form only when access cannot be removed within the required timeframe or when a temporary deviation from this policy is requested. Exceptions must be approved before access continues unless emergency circumstances make prior approval impossible.

Field	Entry
Requestor	_____
Workforce member or account	_____
System / access affected	_____
Reason for exception	_____
ePHI involved	_____
Risk rating	_____
Compensating controls	_____
Monitoring plan	_____
Start date/time	_____
Expiration date/time	_____
Approvers: Security Officer, Privacy Officer, Legal, Executive Owner	_____
Final closure evidence	_____

Appendix L - Business Associate / Vendor Access Termination Notice Template

Subject: Access Termination Required for [Name / User ID]

Dear [Vendor / Business Associate Contact],

[Organization Name] requests immediate termination or modification of access for the individual/account listed below. This request applies to all systems, support portals, remote access tools, AI-enabled systems, AI support environments, data repositories, subcontractor systems, and any other environment through which the individual/account may access, create, receive, maintain, transmit, process, summarize, analyze, or store PHI/ePHI on behalf of [Organization Name].

User / Account: [Insert]

Effective Date/Time: [Insert]

Systems / Services: [Insert]

Action Required: Disable access / remove role / rotate credentials / transfer ownership / confirm destruction or return of data as applicable.

Please confirm in writing by [deadline] that access has been terminated or modified, active sessions have been revoked, relevant credentials or API keys have been rotated where applicable, and any subcontractor access has been addressed. If you identify any security incident, unauthorized access, retained PHI/ePHI, or inability to complete this request, notify [Security/Privacy Contact] immediately according to the applicable agreement.

Thank you,

[Name / Title / Contact Information]

Appendix M - Supervisor Exit Certification

I certify that I have identified, to the best of my knowledge, the systems, applications, files, devices, physical access methods, AI tools, automations, vendor portals, and ePHI repositories used by the workforce member listed below. I have coordinated handoff of active work and have reported any known or suspected unauthorized access, copying, forwarding, printing, downloading, or retention of ePHI.

Field	Entry
Workforce member	_____
Supervisor name	_____
Department	_____
Date	_____
Signature	_____
Notes / exceptions	_____

Appendix N - Compliance Audit Test Script

Control Objective	Sample Test Steps	Pass Criteria	Evidence

Control Objective	Sample Test Steps	Pass Criteria	Evidence
Terminations are reported timely	Select a sample of terminated workforce members from HR records. Compare HR termination date/time to access termination ticket creation date/time.	Ticket was created before or at required policy timeframe.	HR export, ticket report.
Access is removed timely	For each sample, compare termination effective time to system deactivation timestamps in IdP, EHR, VPN, email/cloud, and AI tools.	Access disabled within policy SLA or approved exception exists.	System exports/screenshots.
Evidence is complete	Review checklist and required forms for each sample.	Evidence includes HR request, IT actions, physical access removal, asset return, AI review where applicable, and final certification.	Checklist packet.
Privileged access is controlled	Identify sampled users with admin rights. Verify privileged roles, service accounts, API keys, and shared secrets were removed or rotated.	No active admin rights or unrotated secrets remain.	PAM export, vault log, key rotation record.
AI access is controlled	For users with AI access, review AI account status, prompt/output history retention, agent ownership, API key status, and data connector status.	AI access disabled; AI artifacts transferred or secured; API keys revoked/rotated.	AI admin report, logs.
Vendor access is controlled	Sample vendor users or terminated contractors. Verify organization and vendor-side access removal confirmation.	Vendor access removed and documented.	Vendor confirmation, portal export.
Post-termination activity is reviewed	Review failed logins and access attempts after termination.	No successful post-termination access; suspicious activity escalated.	Log review record.
Exceptions are governed	Review exceptions associated with samples.	Exceptions approved, time-limited, monitored, and closed.	Exception form, monitoring evidence.

Appendix O - System and AI Inventory Template

System / Tool	Owner	ePHI? Y/N	Access Method	Offboarding Action	Evidence Source
EHR / EMR	[Insert]	Y	SSO / local account / role	Disable account or role; review audit log	[Report name]
Patient Portal	[Insert]	Y	[Insert]	[Insert]	[Insert]
VPN / Remote Access	[Insert]	Y	SSO / MFA / device trust	Disable, revoke sessions, remove device trust	[Insert]
Email / Cloud Storage	[Insert]	Y	SSO / delegated access	Disable, transfer ownership, review forwarding/shares	[Insert]
AI Assistant / Scribe	[Insert]	Y/N	SSO / local / API	Disable user, review prompt/output history, transfer artifacts	[Insert]
AI Agent / RPA Bot	[Insert]	Y/N	Service account / API key	Stop/transfer agent, rotate key, update owner	[Insert]
Vendor Portal	[Insert]	Y/N	Named account / shared account	Disable named user or rotate shared credential	[Insert]
Physical Access System	[Insert]	N	Badge / key / code	Disable badge/code; recover key	[Insert]

Appendix P - Security Incident Escalation Quick Reference

Trigger	Immediate Action
Former workforce member successfully logs in after termination.	Open security incident, disable access, preserve logs, review scope, notify Privacy Officer, investigate potential breach.
Terminated user attempted multiple logins.	Confirm account disabled, block IP/session as needed, review MFA/device trust, monitor for related attempts.
Evidence of ePHI download, print, export, email forwarding, or cloud sharing before termination.	Preserve logs and files, notify Security/Privacy/Legal, conduct investigation and breach risk assessment as needed.
AI prompt/output history includes PHI in personal or unapproved AI tool.	Open privacy/security investigation, preserve evidence, identify PHI involved, notify Legal/Privacy, mitigate vendor/account access.
API key or service account under former user remains active.	Revoke/rotate immediately, review activity, assign new owner, update automation, document incident if unauthorized access occurred.
Device not returned or remote worker unresponsive.	Disable access, remote lock/wipe if authorized, track asset, review logs, escalate to HR/Legal/Security.

Appendix Q - Implementation Project Plan

Step	Implementation Action	Owner	Target Date
1	Customize organization name, policy ID, approvers, definitions, and related policy references.	[Security / Compliance]	[Insert]
2	Build or update the HR-to-IAM offboarding workflow with required fields and evidence attachments.	[HR / IT]	[Insert]
3	Attach system inventory and identify all ePHI systems, AI systems, vendor portals, privileged access platforms, and service accounts.	[IT / Security / AI Owner]	[Insert]
4	Configure high-risk termination workflow with pre-notice access removal, evidence preservation, device containment, and legal hold steps.	[HR / Legal / Security]	[Insert]
5	Train HR, supervisors, IT, Security, Facilities, Privacy, Compliance, Vendor Management, and AI owners.	[Training / Compliance]	[Insert]
6	Run a tabletop test using a voluntary termination, high-risk termination, vendor termination, and AI owner departure scenario.	[Security Officer]	[Insert]
7	Complete first access termination audit and remediation plan.	[Compliance / Audit]	[Insert]

11. References Reviewed

The following sources were reviewed to develop this template. The organization should verify current law, final rules, OCR guidance, state requirements, and contract obligations before adoption.

- **eCFR 45 CFR § 160.103 - Definitions:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103
- **eCFR 45 CFR § 164.306 - Security standards: General rules:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306
- **eCFR 45 CFR § 164.308 - Administrative safeguards:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308
- **eCFR 45 CFR § 164.310 - Physical safeguards:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.310
- **eCFR 45 CFR § 164.312 - Technical safeguards:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312
- **eCFR 45 CFR § 164.314 - Organizational requirements:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.314
- **eCFR 45 CFR § 164.316 - Policies, procedures, and documentation requirements:** https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316
- **HHS OCR Summary of the HIPAA Security Rule:** https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- **HHS OCR Security Rule Guidance Material:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- **HHS OCR HIPAA Audit Protocol:** https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
- **HHS OCR HIPAA Security Rule NPRM Fact Sheet:** https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html
- **Federal Register - HIPAA Security Rule To Strengthen the Cybersecurity of ePHI, Proposed Rule, Jan. 6, 2025:** https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
- **NIST SP 800-66 Rev. 2 - Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide:** https://csrc.nist.gov/pubs/sp/800/66/r2/final
- **NIST AI Risk Management Framework and Generative AI Profile:** https://www.nist.gov/itl/ai-risk-management-framework

Final Customization Reminder
Before adoption, replace bracketed fields, add organization-specific system names and AI tools, confirm timing standards with Legal/HR, attach the system and AI inventory, align with the risk analysis, and approve through the organization's governance process.

12. Definitions

This glossary section is placed at the end of the policy so an organization may keep it here, consolidate it into a master policy glossary, or remove it during final template customization.

Term	Definition for This Policy
Access	The ability or permission to read, create, receive, maintain, transmit, modify, delete, export, print, copy, download, query, analyze, summarize, infer from, administer, or otherwise interact with ePHI or a system that contains or can reach ePHI.
AI-enabled system	Any software, service, model, agent, assistant, automation, predictive algorithm, machine learning tool, generative AI tool, transcription/summarization system, RPA bot, chatbot, or analytics tool that uses AI techniques to process, generate, classify, predict, summarize, recommend, search, or automate work.
AI artifact	Prompt history, output history, transcript, agent configuration, custom instruction, workflow, model, fine-tuning data, embedding, vector database, retrieval index, notebook, dataset, evaluation record, API response, model deployment, or export created by or used with an AI-enabled system.
Business associate	A person or entity, other than a workforce member, that creates, receives, maintains, or transmits PHI on behalf of a covered entity, or provides certain services involving PHI.
ePHI	Electronic protected health information. PHI that is created, received, maintained, or transmitted in electronic media.
Emergency termination	A termination, suspension, or access removal triggered by suspected misconduct, security incident, insider threat, unauthorized access, data exfiltration, immediate risk to ePHI, involuntary separation, or urgent operational need.
Former workforce member	A person whose employment, assignment, contract, authorization, credentialing, training relationship, volunteer service, or other arrangement with the organization has ended or been suspended.
Least privilege	The security principle that users and software programs are granted only the minimum access necessary to perform currently authorized duties.
Minimum necessary	The HIPAA Privacy Rule concept that uses, disclosures, and requests for PHI should be limited to the minimum amount needed to accomplish the intended purpose unless an exception applies.
PHI	Protected health information, including individually identifiable health information maintained or transmitted by a covered entity or business associate, except for specific exclusions such as employment records held by a covered entity in its role as employer.
Privileged access	Administrative, elevated, break-glass, service account, root, database, security, audit, API, integration, developer, model deployment, or support access that can change systems, controls, data flows, logs, or access rights.
Service account / bot account	A non-human account used by applications, automations, integrations, AI agents, scripts, or services. Service accounts must have named business owners, technical owners, approved purpose, credential rotation, and logging.
Termination procedures	Documented steps to remove, suspend, modify, transfer, rotate, or disable access to ePHI, systems, facilities, devices, media, AI tools, and credentials when employment, assignment, access authorization, or role changes end or no longer justify access.
User	A person, account, service account, API client, software program, bot, or automation with authorized access to an information system or ePHI.

Term	Definition for This Policy
Workforce	Employees, volunteers, trainees, and other persons whose work for a covered entity or business associate is under the direct control of that entity or business associate, whether paid or unpaid.

Regulatory Currency Analysis / 42 CFR Part 2 / AI Governance / HIPAA Security Rule NPRM Readiness / Change History Record

This addendum documents the regulatory currency review performed to align this policy with the adopted master template style, current HIPAA/HITECH/Omnibus expectations, the 2024 42 CFR Part 2 Final Rule compliance posture, AI governance expectations, and HIPAA Security Rule NPRM readiness. It is intended to be retained with the policy as audit-ready evidence.

Regulatory Status Snapshot
As of this review, the HIPAA Security Rule remains the current enforceable Security Rule, and the HHS OCR HIPAA Security Rule cybersecurity update remains an NPRM/proposed rule unless the organization verifies a published final rule, effective date, and compliance date before adoption. The 2024 42 CFR Part 2 Final Rule is effective, with compliance required beginning February 16, 2026 for entities and persons subject to Part 2. AI tools that create, receive, maintain, transmit, process, summarize, analyze, infer from, or store PHI/ePHI/Part 2 records must be handled as regulated technology assets and vendor/service arrangements, not informal productivity tools.

Regulatory Currency Findings

Topic	Status	Finding	Action in This Revision
HIPAA workforce security and termination procedures	Current rule	Original template strongly addressed access termination, HR/IT coordination, account disablement, asset return, log review, and evidence.	Expanded current-law status language and aligned with master template change history approach.
HITECH / Omnibus vendor and breach alignment	Current rule	Vendor, contractor, business associate, breach evidence, subcontractor and incident escalation concepts were present.	Added stronger downstream vendor, AI vendor, breach evidence, and retained ePHI investigation language.
42 CFR Part 2	Current rule / compliance required	Original policy referenced special data but did not fully operationalize Part 2 offboarding.	Added Part 2 account removal, segmentation/tagging, redisclosure controls, SUD record access review, AI/vendor handling, and incident response requirements.
AI offboarding	Emerging and current HIPAA application	Original policy had strong AI offboarding coverage.	Added persistent memory, prompt/output history, vector stores, connectors, model artifacts, service accounts, and owner-transfer detail.
HIPAA Security Rule NPRM	Proposed rule / readiness only	Original policy mentioned proposed-rule readiness.	Clarified readiness-only status and reinforced evidence-driven access termination targets.

Required Adoption Cautions

- Do not state that the HIPAA Security Rule NPRM is final unless the organization verifies publication of a final rule, effective date, and compliance date before approval.
- Do not apply 42 CFR Part 2 automatically to every SUD-related fact; determine whether the information is a Part 2 record and whether the organization, source, recipient, vendor, or workflow is subject to Part 2.
- Do not allow AI tools to ingest, retain, train on, summarize, infer from, or disclose PHI/ePHI/Part 2 records unless the use is approved, contracted where required, risk-assessed, configured for organization control, and supported by audit evidence.
- Do not rely on policy statements alone. Retain configuration evidence, system reports, test results, access logs, exception approvals, vendor confirmations, risk analysis references, and remediation records.
- Treat proposed-rule readiness controls as security program enhancements unless and until they become enforceable regulatory requirements.

Regulatory Currency Gap Analysis

Requirement / Topic	Original Template Coverage	Gap or Risk	Recommended Language / Control	Priority
Part 2 termination access review	General sensitive data references.	May miss SUD record segmentation, consent/redisclosure, and post-termination access evidence.	Add Part 2-specific access review, system query, audit log review, and vendor/AI revocation steps.	Critical
AI memory and artifacts	Strong AI offboarding but needs more artifact specificity.	Former user may retain influence or access through AI memory, agent config, prompt libraries, vector stores, or notebooks.	Transfer ownership, revoke connector grants, purge or lock unauthorized memory, rotate API keys, and certify retention controls.	Critical
Service accounts	Covered.	Secrets known by departing privileged users may remain active.	Rotate secrets, reassign owner, review vault access, inspect automation logs, and document owner attestation.	High

42 CFR Part 2 and Special Category Data Checklist

Status	Control	Owner	Evidence / Notes
[ ]	Determine whether the policy workflow creates, receives, maintains, transmits, accesses, tests, discloses, or supports Part 2 records.	Privacy Officer / Legal	Part 2 applicability memo, data inventory, workflow map.
[ ]	Identify systems, AI tools, logs, transcripts, notebooks, prompt/output stores, vector stores, vendor platforms, and backups that may contain Part 2 records.	Security / System Owners / AI Owner	Inventory, data-flow map, vendor list.
[ ]	Apply role-based access, minimum necessary, segmentation/tagging, masking, consent, redisclosure, audit logging, and breach-aligned incident response controls where applicable.	Security / Privacy / Legal	Access matrix, EHR flags, DLP rules, audit logs, incident playbook.
[ ]	Confirm vendors, business associates, qualified service organizations, subcontractors, or AI service providers have appropriate written terms for Part 2 records where required.	Vendor Management / Legal	Executed agreement, BAA/QSOA review, vendor attestation.
[ ]	Search for Part 2 records or SUD treatment access in systems used by the departing user where applicable.	Privacy / Security	Access logs, role reports, Part 2 applicability memo.
[ ]	Revoke AI platform sessions, prompt histories, connectors, personalizations, memory, API keys,	AI Owner / IAM	AI admin export, key rotation record, owner transfer evidence.

	and agent ownership tied to the user.		
[ ]	Confirm no PHI/ePHI/Part 2 records, AI outputs, transcripts, notes, exports, or screenshots remain in personal accounts or devices.	Supervisor / Security / Privacy	Exit certification, device inspection record, DLP results.

AI Regulatory Readiness and Vendor Control Checklist

Status	AI Control	Owner	Evidence / Notes
[ ]	AI tool or agent has an approved use case, owner, data classification, and PHI/ePHI/Part 2 determination.	AI Governance Owner	AI inventory and approval record.
[ ]	BAA, contract, QSOA, data processing terms, or legal exception analysis is complete before regulated data is processed.	Vendor Management / Legal	Executed agreement or legal analysis.
[ ]	Vendor training, model improvement, cross-customer learning, persistent memory, and prompt/output retention settings are disabled unless approved and documented.	AI Owner / Privacy	Configuration export and vendor statement.
[ ]	SSO, MFA, role-based access, session controls, unique identity, logging, and revocation are configured where feasible.	IAM / AI Owner	Policy export, screenshots, test evidence.
[ ]	Connectors, API keys, service accounts, and AI agents use least privilege, owner assignment, logging, runtime limits, rotation, and kill switch procedures.	Security / Automation Owner	Agent runbook, vault report, logs.
[ ]	AI prompt/output logs are available for audit and incident response without creating unnecessary PHI exposure.	Security / Privacy	Log location and retention schedule.

Additional References Reviewed for Version 1.1

- HHS OCR, HIPAA Security Rule NPRM and Fact Sheet, proposed rule issued December 27, 2024 and published January 6, 2025 at 90 FR 898.
- HHS OCR, Summary of the HIPAA Security Rule and current Security Rule guidance materials.
- eCFR, 45 CFR Part 160 and 45 CFR Part 164, Subparts A and C, current HIPAA Security Rule regulatory text.
- HHS/SAMHSA/OCR, Fact Sheet: 42 CFR Part 2 Final Rule; effective April 16, 2024; compliance required February 16, 2026.
- eCFR, 42 CFR Part 2, Confidentiality of Substance Use Disorder Patient Records.
- HHS, Understanding Confidentiality of Substance Use Disorder Patient Records or Part 2.
- HHS OCR, Part 2 civil enforcement program information and Part 2/HIPAA breach notification alignment materials.
- NIST SP 800-66 Rev. 2, Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide.
- NIST AI Risk Management Framework and NIST AI 600-1 Generative AI Profile.

Final Change History Record

This final page documents the substantive regulatory, operational, and formatting changes made to align this policy with the adopted master template style and current regulatory-readiness requirements.

Change ID	Section / Area	Change Type	Description of Change	Regulatory / Operational Rationale	Adoption Status
CH-001	Document control / version history	Revision	Updated Termination Policy and Procedure to Version 1.1 Review Draft with review date of May 18, 2026.	Maintains auditable version control and distinguishes this regulatory-current review draft from the original template.	Included
CH-002	Regulatory status language	Clarification	Added current-law versus proposed-rule distinction for HIPAA Security Rule NPRM readiness items.	Avoids representing proposed OCR Security Rule requirements as final regulatory text until final rule publication, effective date, and compliance date are verified.	Included
CH-003	42 CFR Part 2	Addition	Added Part 2 applicability, SUD record handling, consent/redisclosure, segmentation/tagging, incident response, and vendor/AI handling concepts where relevant.	2024 Part 2 Final Rule is effective, and compliance is required beginning February 16, 2026 for entities and persons subject to Part 2.	Included
CH-004	AI governance	Enhancement	Strengthened treatment of AI tools, AI agents, prompt/output history, vector stores, connectors, APIs, model artifacts, and vendor-managed AI services.	AI systems processing PHI/ePHI/Part 2 records must be governed as regulated technology assets, business associate/vendor arrangements, or approved internal systems.	Included
CH-005	Evidence and audit readiness	Enhancement	Added stronger documentation, testing, approval, vendor evidence, configuration evidence, and review requirements.	OCR audit readiness and Security Rule documentation require proof of implementation, not only written policy language.	Included
CH-006	Appendices and tools	Addition	Added policy-specific regulatory currency analysis, gap analysis, Part 2 checklist, AI/vendor readiness checklist, and final change history record.	Provides operational forms and artifacts that can be used in GRC, ticketing, vendor review, audit, and compliance evidence repositories.	Included

CH-007	Final regulatory addendum / change history record	Revision	Standardized the final regulatory addendum heading to the accepted Batch 1 title. No substantive policy controls were changed.	Implements Priority 2 audit-consistency update while preserving the current-law versus NPRM-readiness distinction.	Included

Final adoption note: This policy remains a template. Before implementation, replace placeholders, validate system inventory and data flows, confirm Part 2 applicability, verify final HIPAA Security Rule status, review state law and contracts, and obtain approval through the organization's governance process.