Apptega

GUIDE

HIPAA

Privacy & Breach Notification Rule Compliance Guide

Understanding and Implementing Security Requirements for Electronic Protected Health Information (ePHI)

Update note: On June 18, 2025 a federal court vacated most of the 2024 reproductive-health privacy amendments. HHS has indicated some Notice of Privacy Practices (NPP) modifications still have a compliance date of February 16, 2026. Coordinate with counsel for applicability.

Heads-up on tracking tech: A federal court vacated portions of HHS's "online tracking technologies" bulletin on June 20, 2024; HHS later declined to appeal. Treat that bulletin accordingly and rely on core HIPAA definitions and your risk analysis.

Current as of August 19, 2025 • Applies to Covered Entities & Business Associates handling PHI

Apptega

Apptega

1. Introduction

The HIPAA Privacy Rule governs how covered entities and business associates use and disclose protected health information (PHI) and defines individual rights. This guide is implementation-focused to help an organization become compliant. It assigns owners, parameters, measurable acceptance criteria, evidence locations, and section-by-section mappings to 45 CFR Part 164 Subpart E, and incorporates the HIPAA Breach Notification Rule (45 CFR §§164.400–414).

1A. Beginner Quick-Start (First 30—90 Days)

Days 1-15 — Program stand-up

- Appoint: Privacy Official; Privacy Counsel contact; Security Official liaison; HIM/Records Lead; Digital/Web Lead; TPRM Lead.
- Define the PHI authorization boundary and systems of record; draft PHI data flows (EHR, portals, websites/apps, analytics, vendors).
- Publish current NPP and distribution plan; inventory BAs and contract status.
- Stand up request intake for access, amendments, accounting, restrictions, confidential communications, and complaints.

Days 16-45 — Tailor and implement

- Operationalize minimum-necessary workflows and verification procedures; deploy authorization forms; configure disclosure logging.
- Approve program parameters (SLAs, disclosure logging scope, identity verification levels).
- Draft Privacy Documentation Set narratives and acceptance criteria per section.

Days 46-90 — Evidence & readiness

- Populate the Evidence Register; conduct a privacy incident tabletop and a Right of Access drill.
- Perform a self-assessment against this guide; record gaps in the Remediation Log with owners and due dates.

2. Scope & Alignment

Scope. All people, processes, systems, and third parties that create, receive, maintain, or transmit PHI, including clinical, plan, and business operations; portals, websites, and mobile apps; analytics/data lakes; archival/backups; communications; and BA ecosystems.

Key Definitions

- **HI:** Individually identifiable health information held by a covered entity/BA, excluding de-identified data.
- **Designated Record Set (DRS):** Records used to make decisions about individuals (e.g., medical/billing records for providers; enrollment/claims for plans).
- **Personal Representative:** Individual authorized under applicable law to act for the patient.
- **Minimum Necessary:** Limit uses, disclosures, and requests to the least amount needed.
- **Business Associate (BA):** Performs functions involving PHI for a covered entity and must be under a compliant BAA.

Governance & Roles

- Privacy Official (program, policies, monitoring, complaint resolution)
- HIM/Records Lead (DRS catalog; access, amendments, accounting)
- Digital/Web Lead (web/app data collection, tagging/SDKs, contracts, risk analysis)
- TPRM Lead (BA due diligence and contract lifecycle)
- Security Official (safeguards, incident response, breach risk assessments)

Apptega

3. Standards & Practices

Each topic includes: Intent • Minimums • Implement (Procedural/Technical/ Contractual) • Evidence • Acceptance Criteria • Common Failures • Internal QA Plan • Documentation tie-in.

PR1 — Uses & Disclosures — General Rules (§164.502)

Intent: Establish lawful bases and boundaries for uses/disclosures by workforce and BAs.

Minimums: Use/disclose only as permitted or required; ensure BA compliance; apply minimum necessary.

Implement — Procedural: Catalog routine uses/disclosures; decision trees for non-routine and special cases; approval checkpoints.

Implement — Technical: Release queues with reasons; disclosure logging for non-rroutine events; redaction tools.

- **Contractual:** BAAs define permitted uses, limits, safeguards, and reporting.
- **Evidence:** Use/disclosure catalog; BAAs; sample disclosure logs.
- **Acceptance Criteria:** 100% non-routine disclosures documented with legal basis and minimum-necessary review.
- **Common Failures:** Assuming “TPO” covers everything; undocumented BA onward uses.
- **Internal QA Plan:** Quarterly sample of 25 non-routine disclosures.
- **Documentation tie-in:** Uses/Disclosures policy; BA management procedure.

PR2 — Minimum Necessary (§164.502(b), §164.514(d))

Intent: Limit PHI to the least amount required.

Minimums: Policies for uses, disclosures, and requests; role-based access; standard protocols.

Implement: Role matrices; segmentation/masking; default-to-minimum queries; analytics/export controls.

- **Evidence:** Role matrix; system configs; sample requests.
- **Acceptance Criteria:** Spot checks show data elements limited to purpose; annual re-validation of role matrices.
- **Common Failures:** Broad exports; “all fields” habits.
- **Internal QA Plan:** Monthly checks of 20 releases.
- **Documentation tie-in:** Minimum Necessary standard; access governance.

PR3 — Authorizations (§164.508)

Intent: Obtain valid authorization when required (e.g., most marketing, psychotherapy notes, sale of PHI).

Minimums: Required elements, expiration, revocation process; tracking of disclosures under authorization.

Implement: Standard forms; ID verification; revocation workflow; repository with status.

- **Evidence:** Executed authorizations/revocations; disclosure logs.
- **Acceptance Criteria:** 100% required elements present; revocations actioned ≤5 business days.
- **Common Failures:** Using access requests as authorizations; expired/ overbroad forms.
- **Internal QA Plan:** Sample 20 authorizations quarterly.
- **Documentation tie-in:** Authorization policy and procedures.

PR4 — Uses/Disclosures Permitted Without Authorization (§164.512)

Intent: Enable permitted disclosures (public health, oversight, judicial/administrative, law enforcement, serious threats, specialized government, workers' comp) with safeguards.

Implement: Decision trees; legal intake; subpoena/order review; redaction protocols; minimum-necessary overlays.

- **Evidence:** Disclosure logs with legal basis; legal reviews; copies of orders/subpoenas.
- **Acceptance Criteria:** 100% disclosures show basis, scope, and timeliness.
- **Common Failures:** Over-disclosure; bypassing legal review.
- **Internal QA Plan:** Sample 10 disclosures per category.
- **Documentation tie-in:** Legal Requests SOP; Disclosure Logging standard.

PR5 — Opportunity to Agree or Object (§164.510)

Intent: Respect patient preferences for facility directories and disclosures to family/friends/caregivers.

Minimums: Provide opportunity to agree/object when practical; use professional judgment in emergencies.

Implement: Capture preferences; bedside/registration workflows; emergency exception documentation.

- **Evidence:** Preference records; training materials.
- **Acceptance Criteria:** Preferences captured and honored; exceptions documented.
- **Common Failures:** Missing directory opt-outs.
- **Internal QA Plan:** Spot-check 20 admissions.
- **Documentation tie-in:** Directory & Family/Friends policy.

PR6 — De-identification & Limited Data Sets (§164.514(a)—(c), (e))

Intent: Manage data for secondary purposes.

Minimums: De-identification via Expert Determination or Safe Harbor; limited data sets under DUA.

Implement: Expert documentation or removal of 18 identifiers; DUAs; re-identification controls.

- **Evidence:** De-identification reports; DUAs; dataset catalogs.
- **Acceptance Criteria:** Required artifacts exist; releases mapped to method.
- **Common Failures:** "Anonymized" claims without method.
- **Internal QA Plan:** Review 5 datasets/quarter.
- **Documentation tie-in:** Data Use & De-identification standard.

PR7 — Verification of Identity/Authority (§164.514(h))

Intent: Verify identity and authority before disclosure.

Implement: ID checks; callback procedures; challenge-response for telephonic; validation of legal documents.

- **Evidence:** Verification logs; SOPs.
- **Acceptance Criteria:** 100% sampled disclosures show verification step.
- **Common Failures:** Casual phone releases.
- **Internal QA Plan:** Audit 25 phone/fax disclosures/quarter.
- **Documentation tie-in:** Verification SOP.

PR8 — Notice of Privacy Practices (NPP) (§164.520)

Intent: Inform individuals about uses/disclosures, rights, and duties.

Minimums: Required content; distribution at first service delivery; posting on website; good-faith acknowledgment in provider settings.

Implement: Versioned NPP; language access; posting in facilities and online; distribution via portals/mail as applicable; change management.

- **Evidence:** Current NPP; posting screenshots; acknowledgments.
- **Acceptance Criteria:** Current NPP published and distributed; acknowledgments captured where applicable.
- **Common Failures:** Outdated NPP; missing web posting.
- **Internal QA Plan:** Quarterly NPP content and presence check.
- **Documentation tie-in:** NPP policy and change log.

PR9 — Individual Right of Access (§164.524)

Intent: Provide timely access to PHI in the DRS.

Minimums: Respond within 30 days (one 30-day extension with written notice); provide form/format if readily producible; allow third-party designee where applicable; fees limited to cost-based.

Implement: Intake portal; ID verification; routing to DRS owners; form/format library; fee schedule; secure delivery channels.

- **Evidence:** Request logs; turnaround metrics; fee records.
- **Acceptance Criteria:** ≥95% on-time responses; requested form/format when feasible; fees documented and compliant.
- **Common Failures:** Delays; unjustified denials; excessive fees.
- **Internal QA Plan:** Monthly timing report; sample 20 requests.
- **Documentation tie-in:** Access policy; fee schedule; ID verification procedure.

PR10 — Right to Amend (§164.526)

Intent: Allow individuals to request amendment of PHI in the DRS.

Minimums: Written request; decision within 60 days (one 30-day extension with notice); denial in writing with basis and rights; append notices to identified downstream recipients as required.

Implement: Standard request channel; routing; documentation and notification to recipients as applicable.

- **Evidence:** Amendment logs; decisions; downstream notices.
- **Acceptance Criteria:** ≥95% decisions on time; proper denial content where used.
- **Common Failures:** Ignoring non-DRS requests without guidance; failing to notify recipients.
- **Internal QA Plan:** Sample 10 amendments/quarter.
- **Documentation tie-in:** Amendment policy and SOP.

PR11 — Accounting of Disclosures (§164.528)

Intent: Provide a record of certain disclosures for the prior 6 years (with exceptions).

Minimums: Track non-TPO disclosures and those required to be logged; provide accounting within 60 days (one 30-day extension).

Implement: Logging standard; system capture for non-routine releases; request handling process.

- **Evidence:** Disclosure logs; response packets.
- **Acceptance Criteria:** Accounting provided on time; scope accurate.
- **Common Failures:** Missing non-routine logs.
- **Internal QA Plan:** Semiannual log review.
- **Documentation tie-in:** Disclosure logging SOP.

PR12 — Restrictions & Confidential Communications (§164.522)

Intent: Honor reasonable requests for restrictions and confidential communications.

Minimums: Required restriction when individual pays in full and requests restriction to health plan for that item/service; accommodate reasonable confidential communications.

Implement: Flags in EHR/billing; alternative address/phone handling; staff workflows.

- **Evidence:** Restriction logs; communication preferences.
- **Acceptance Criteria:** 100% self-pay restrictions honored; confidential channels used.
- **Common Failures:** Leaks to plans despite self-pay restriction.
- **Internal QA Plan:** Sample 10 restricted encounters/month.
- **Documentation tie-in:** Restrictions & Confidential Communications policy.

PR13 — Special Situations (Personal Representatives, Minors, Deceased, Psychotherapy Notes, Research)

Intent: Apply specialized rules correctly.

Implement: State-law matrix for minors/reps; segregate psychotherapy notes; research authorizations or waivers; decedent disclosures per rule.

- **Evidence:** State-law references; segregation controls; IRB documentation.
- **Acceptance Criteria:** Sampling shows correct basis used.
- **Common Failures:** Treating all parents as reps; mixing psychotherapy notes with general record.
- **Internal QA Plan:** Quarterly review of 10 special-case disclosures.
- **Documentation tie-in:** Special Situations SOPs.

BN1 — Breach: Definitions & Risk Assessment (§§164.402—404)

Intent: Determine if an impermissible acquisition, access, use, or disclosure of unsecured PHI is a reportable breach.

Minimums: Conduct risk assessment considering: (1) nature/extent of PHI involved; (2) unauthorized person; (3) whether PHI was actually acquired or viewed; (4) extent of mitigation. Presumptive breach unless low probability of compromise.

Implement: Intake → classify incident → risk assessment → determination → documentation. Recognize exceptions (unintentional good-faith within scope; inadvertent disclosure between authorized persons within the same entity; recipient cannot retain information). Apply encryption/destruction safe harbors for "unsecured PHI".

- **Evidence:** Risk assessment record; determination; mitigation steps.
- **Acceptance Criteria:** 100% incidents evaluated with the four-factor analysis; exception rationale documented when used.
- **Common Failures:** Skipping formal risk assessment; over-use of exceptions.
- **Internal QA Plan:** Review three determinations/quarter.
- **Documentation tie-in:** Breach assessment SOP.

BN2 — Individual Notice (§164.404)

Intent: Notify affected individuals without unreasonable delay and no later than 60 calendar days after discovery.

Minimums: Written notice by first-class mail (or email if individual agrees). Substitute notice when contact info insufficient. Urgent cases may require telephone or other means in addition to written notice.

Content: Brief description; types of PHI involved; actions individuals should take; what the entity is doing; contact information.

- **Evidence:** Notices; mailing/email proofs; returned mail handling.
- **Acceptance Criteria:** Notices sent on time with required content.
- **Common Failures:** "Day-60" planning; missing content elements.
- **Internal QA Plan:** Validate last two mailings.
- **Documentation tie-in:** Notification templates and SOP.

BN3 — Media Notice (§164.406)

Intent: For breaches affecting more than 500 residents of a state/jurisdiction, provide notice to prominent media outlets without unreasonable delay and no later than 60 days.

- **Evidence:** Media release; distribution confirmation.
- **Acceptance Criteria:** Issued on time; content aligns with individual notice.
- **Internal QA Plan:** Annual press-release drill.
- **Documentation tie-in:** Media notification procedure.

BN4 — Notice to HHS (§164.408)

Intent: Report to HHS via its breach portal.

Minimums: For 500+ individuals, report contemporaneously (without unreasonable delay, no later than 60 days from discovery). For fewer than 500 individuals, log and submit to HHS no later than 60 days after end of the calendar year.

- **Evidence:** Portal confirmations; breach log.
- **Acceptance Criteria:** Timely submission; accurate counts and summaries.
- **Common Failures:** Missing annual submission for small breaches.
- **Internal QA Plan:** Year-end breach log reconciliation.
- **Documentation tie-in:** HHS reporting SOP.

BN5 — Business Associates (§164.410)

Intent: BA must notify the covered entity without unreasonable delay and no later than 60 days after discovery, including identities of affected individuals when possible and information needed for notices.

Implement: Contractual timelines; incident reporting channels; secure data exchange.

- **Evidence:** BA notice; data transfer receipts.
- **Acceptance Criteria:** BA notices within contracted window; sufficient detail for CE notifications.
- **Common Failures:** BA delays; incomplete event details.
- **Internal QA Plan:** Sample 3 BA incidents.
- **Documentation tie-in:** BAA breach clauses and BA intake procedure.

BN6 — Content, Timelines & Method (Consolidated)

Intent: Ensure all required elements, methods, and timing are met across individual, media, and HHS notices.

Implement: Checklist per event; calendar controls; translation/accessibility; call-center scripting; credit monitoring where risk warrants.

- **Evidence:** Completed checklist; scripts; translations.
- **Acceptance Criteria:** Zero late notices; content elements complete; accessibility addressed.
- **Common Failures:** Missing TTY/translation; weak call scripts.
- **Internal QA Plan:** Post-mortem checklist audit.
- **Documentation tie-in:** Breach notification checklist.

BN7 — Documentation & Recordkeeping (§164.414)

Intent: Maintain records for 6 years: risk assessments, determinations, notices, media/HHS submissions, BA communications, and mitigation.

Implement: Central breach register; evidence repository; retention/holds.

- **Acceptance Criteria:** Complete record set for each event; retention met.
- **Common Failures:** Scattered artifacts; no central register.
- **Internal QA Plan:** Semiannual register audit.
- **Documentation tie-in:** Breach register and retention policy.

4. Authorization Boundary & PHI Data-Flow Mapping

Describe components, interfaces, trust zones, cloud services, external partners, and where PHI flows, rests, and leaves. Maintain processing records (sources, stores, transmissions, recipients). Update on material change.

Documentation tie-in: Diagram and narrative maintained with change management.

5. Privacy Documentation Set — Canonical Narratives

Write cohesive narratives proving how the program meets Privacy and Breach requirements for the defined boundary: overview/mission; boundary & inventory; PHI categories and lifecycle; roles/governance; BA management; key processes (uses/disclosures, minimum necessary, authorizations, verification); individual rights (access, amendments, accounting, restrictions/confidential communications); special situations; breach assessment and notification; training; monitoring; change management.

6. Applicability & Acceptance Criteria Mapping (to CFR)

Maintain a definitive record for each requirement: applicability, implementation summary, parameter values, measurable acceptance criteria, inheritance (if any), and evidence link.

Excerpt:

Ref	Title	Applicable	Implementation Summary	Parameters	Acceptance Criteria	Inheritance	Evidence
PR2	Minimum Necessary	Y	Role matrices; masked exports	Revalidation 12m	Spot checks show least-needed fields only	System	AccessGov/RoleMatrix.pdf
PR9	Right of Access	Y	Intake, IDV, DRS routing	SLA 30d	≥95% on time; fees compliant	Shared	HIM/AccessLog.csv
BN2	Individual Notice	Y	Mail/email; content checklist	SLA 60d	100% complete and timely	System	Breach/Notices/

7. Program Parameters (Organization-Specific Settings)

- **Access & Identity Verification:** Acceptable ID types; telephonic challenge-response; portal authentication.
- **Access/Amendment SLAs:** Access ≤30 days; amendment decision ≤60 days; extensions documented.
- **Disclosure Logging:** Scope for non-routine categories; minimum fields to capture; retention ≥6 years.
- **Restrictions & Confidential Comms:** Flag behavior in EHR/billing; alternate channels; verification steps.
- **De-identification:** Approved methods; DUA required elements; dataset cataloging.
- **Breach:** Risk assessment template; notification timing gates; content checklist; clock-start definition (discovery).
- **Training Cadence:** Onboarding; annual refresher; targeted modules for HIM, call center, web/app teams.

Apptega

8. Evidence Register

Artifact	Safeguards	Location/Path	Owner	Format	Retention
NPP (current + prior)	PR8	Privacy/NPP/	Privacy Official	PDF/HTML	6 years
Use/Disclosure Catalog	PR1	Privacy/ UseDisclosure/	Privacy Official	XLSX	6 years
Role Matrix & Recerts	PR2	AccessGov/Roles/	IAM Lead	CSV/PDF	6 years
Authorization Repository	PR3	Privacy/Auth/	HIM Lead	PDF	6 years
Disclosure Logs	PR1/PR4/PR11	Logs/Disclosures/	HIM Lead	CSV	6 years
Access Requests Log	PR9	HIM/Access/	HIM Lead	CSV	6 years
Amendments Log & Decisions	PR10	HIM/Amend/	HIM Lead	PDF/CSV	6 years
Restrictions & Conf. Comms	PR12	HIM/Restrictions/	HIM Lead	CSV	6 years
De-identification Records/DUAs	PR6	Data/DeID/	Data Gov	PDF	6 years
Breach Register & Assessments	BN1–BN7	IR/Breach/	Security/Privacy	PDF/CSV	6 years
BAAs & Due Diligence	PR1/OR	Legal/BAA/	Legal	PDF	Active + 6 years
Training Rosters & Content	AR/Program	L&D/Privacy/	L&D	CSV/PDF	6 years

9. Continuous Monitoring (Privacy Operations)

- **Daily:** Incident intake triage with Security; access request queue health; web/app tag change alerts.
- **Weekly:** Disclosure log spot checks; BA ticket review; exceptions for restrictions/ confidential comms.
- **Monthly:** NPP presence verification; role-matrix changes; dataset release review; metrics to leadership.
- **Quarterly:** Tabletop (privacy or breach scenario); authorization completeness audit; verification spot checks.
- **Automation:** Alerts for SLA breach risk, missing disclosure reasons, BA notice deadlines, and breach portal submission windows.

10. Remediation & Risk Acceptance Workflow

Identify gaps → Record in Remediation Log (severity, owner, due date, milestones) → Treat (process change/training/technology/contracting) → Verify with evidence → Report to governance.

High-impact privacy gaps resolved promptly; deadlines tracked; extensions documented with rationale.

Risk acceptance only by designated leadership with explicit expiry and compensating controls where feasible.

11. Cloud, Websites, Mobile Apps & BAAs

Define shared-responsibility for platforms and SDKs; verify admin MFA, logging/export, encryption defaults, public-object policies, and data-sharing settings. Maintain tag/SDK inventories for sites/apps; require BAAs or appropriate data-protection contracts; validate permitted uses and onward disclosures; document vendor incident notice timelines.

12. Training & Awareness (Role-Based)

Tracks for workforce baseline, HIM/records, call center, digital/web, leadership, and BAs with access to PHI. Onboarding before access; annual refresher; targeted refreshers after incidents; metrics include completion ≥98% and declining error rates in sampled disclosures.

13. Vendor & Supply Chain (Business Associates)

Tier BAs by PHI sensitivity; require BAAs with permitted uses, safeguards, breach notice, subcontractor flow-down, and audit rights where appropriate. Perform due diligence at onboarding and at least annually; verify claims (encryption, logging, retention); maintain offboarding steps for data return/destruction.

14. Change Management for Privacy Impact

Run privacy impact checks for product/process changes, web/app tag updates, analytics use cases, and new data-sharing arrangements. Require legal review for novel uses; update NPP if material; adjust role matrices and disclosure logging as needed.

15. Evidence Sampling Plans (Internal QA)

- **Uses/Disclosures:** Sample 25 non-routine releases/quarter for basis, minimum necessary, and timeliness.
- **Access:** Sample 20 access requests/month for timing, form/format, fees, and ID verification.
- **Authorizations:** Sample 20/quarter for required elements and scope.
- **Restrictions/Confidential Comms:** Sample 10/month for adherence.
- **Breach Events:** Review last 3 determinations for four-factor analysis and notice timing.
- **BA Oversight:** Sample 5 BA files for BAA terms, due diligence, and incident reporting.

16. Common Pitfalls

Treating “TPO” as blanket approval; outdated NPP or missing web posting; unclear DRS boundaries; weak identity verification; failing to honor self-pay restrictions; missing non-routine disclosure logs; rushed breach notices at day 60 with missing content; BA contracts with vague breach timelines or onward disclosures.

17. Quick Reference Summary

Area	Core Artifacts	Examples
PR1	Use/disclosure catalog; BAAs	Decision trees; logs
PR2	Role matrix; masked exports	Default-to-minimum queries
PR3	Authorization repository	Revocation workflow
PR8	NPP versions + proof	Web/facility postings
PR9	Access logs & metrics	Fee schedule; secure delivery
BN1–BN7	Breach register & notices	Four-factor assessments; portal receipts
Program	Training rosters; parameters	SLA dashboards

18. Self-Assessment & Leadership Attestation

Use status: **Compliant (C) / Partially Compliant (PC) / Not Compliant (NC) / Not Applicable (N/A).**

Tracker (illustrative):

Requirement	Status	Rationale (for N/A or gaps)	Evidence Link	Owner	Action ID
PR2 – Minimum Necessary	PC	Analytics exports too broad	DataGov/ExportsReview.pdf	Data Gov Lead	ACT-2025-011
PR9 – Right of Access	C	—	HIM/AccessMetrics.csv	HIM Lead	—
BN2 – Individual Notice	C	—	Breach/Notices/2025/	Privacy Official	—

Leadership attests that scope is complete, evidence exists for each “C”, and gaps have assigned owners and due dates in the Remediation Log.

Apptega

19. References & Resources

HIPAA Privacy Rule (45 CFR Part 164 Subpart E)
https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E

HIPAA Breach Notification Rule (45 CFR §§164.400–414)
https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D

HHS Privacy Rule Guidance
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

HHS Breach Notification Guidance & Portal
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Business Associates — HHS Guidance
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

De-identification Guidance
https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com