HIPAA Compliance Checklist (2026): Privacy, Security and Breach Requirements

By Craig Besnoy

Craig Besnoy is a Partner at Dunlap Bennett & Ludwig, where he advises on cybersecurity, data privacy, and regulatory compliance with a core focus on mergers, acquisitions, and strategic transactions involving data-driven and highly regulated businesses. He works extensively with healthcare organizations, financial services firms, technology companies, and investors on cybersecurity risk management, HIPAA compliance, incident response, and third-party risk oversight.

Craig has more than a decade of experience advising on complex transactions and compliance matters in which data security and privacy risk are material considerations, including acquisitions, restructurings, and growth-stage investments. His experience includes helping physician-owned practices achieve HIPAA compliance and training physicians and staff on privacy and security best practices as part of pre-acquisition readiness efforts. He is admitted to practice in New York and is recognized for translating evolving cybersecurity and privacy regulations into operationally practical and legally defensible frameworks.

DUNLAP BENNETT & LUDWIG

This guide is educational and does not constitute legal advice.

HIPAA compliance divides into three rules—privacy, security, and breach notification. Each sets obligations that covered entities and business associates must meet. This checklist organizes those obligations into actions. It reflects 2025 regulatory proposals including mandatory multi-factor authentication, continuous asset inventory, and accelerated breach timelines.

Covered entities are providers, health plans, and clearinghouses. Business associates are vendors that create, receive, maintain, or transmit PHI for covered entities. The Omnibus Rule made both groups directly liable. Compliance work includes risk analysis, written safeguards, workforce training, Business Associate Agreements with vendors, audit logging, breach response, and six years of documentation.

Key Terms: PHI and Business Associate Agreements

Protected Health Information (PHI) is individually identifiable health information held or transmitted by covered entities or business associates. PHI includes medical records, billing records, insurance claims, lab results, prescription records, and any other health data linked to an individual. Electronic PHI (ePHI) is PHI stored, accessed, or transmitted electronically.

Business Associate Agreements (BAAs) are contracts between covered entities and vendors that handle PHI. BAAs define permitted uses of PHI, require safeguards, set breach notification duties, and establish audit rights. Every vendor that touches PHI—cloud hosts, billing services, EHR platforms, telehealth tools—must sign a BAA before accessing data.

What HIPAA Is and Who It Binds

The Health Insurance Portability and Accountability Act sets national standards for PHI privacy and security. It grants patients access and amendment rights. It requires covered entities and business associates to implement safeguards, execute BAAs with vendors, and report breaches within defined windows.

Determining Applicability

HIPAA applies if you handle PHI for treatment, payment, or health care operations, or if you process PHI on behalf of a covered entity. Cloud storage, telehealth, billing vendors, and EHR add-ons fall under business associate rules and carry direct compliance obligations.

Three Core Rules: Privacy, Security, and Breach Notification

Three federal rules set HIPAA requirements. The Privacy Rule governs who sees PHI and under what conditions. The Security Rule requires safeguards for ePHI—administrative controls, physical controls, technical controls. The Breach Notification Rule sets notification obligations when protected data is exposed. Each rule drives different controls but all three feed the same compliance program.

Rule	Focus	Core obligations	Timeline
Privacy Rule	Use and disclosure of PHI	Minimum necessary, Notice of Privacy Practices, patient access, authorizations	On request and ongoing
Security Rule	Safeguards for ePHI	Risk analysis, administrative/physical/technical controls	Ongoing with periodic reviews
Breach Notification Rule	Reporting breaches	Notify individuals, HHS, and media (if ≥500 affected)	Within 60 days for ≥500; annually for <500. *Proposed 2025 changes may reduce window to 24 hours for certain incidents.*

Privacy Rule Scope

The Privacy Rule applies to PHI in any form. It requires minimum necessary disclosures, a Notice of Privacy Practices, and patient access and amendment mechanisms. Treatment, payment, and health care operations disclosures proceed without authorization. Other uses require written authorization or must fit permitted categories—public health reporting, law enforcement, as required by law.

Security Rule Scope

The Security Rule applies to ePHI. It requires an enterprise risk analysis followed by safeguards in three categories. **Administrative safeguards** cover risk management, workforce access policies, training, contingency planning, and vendor oversight. **Physical safeguards** address facility access, workstation placement, and device disposal. **Technical safeguards** include access control, audit logging, integrity monitoring, authentication, and transmission encryption.

Proposed 2025 updates add 10 new and 15 revised definitions for "risk," "threat," and "vulnerability." They expand scope to "relevant electronic information systems" that affect ePHI security even if they do not store PHI directly.

Breach Notification Rule Obligations and Timelines

Organizations assess whether an impermissible use or disclosure triggers notification. For breaches affecting 500 or more individuals, notify affected persons, HHS (via the breach portal), and prominent media within 60 days of discovery. Breaches under 500 are logged and reported to HHS annually. **2025 trend:** Rectangle Health and other analyses point to regulatory movement toward 24-hour notification for certain high-risk breaches, aligning HIPAA with state laws and cybersecurity frameworks. Organizations are building accelerated playbooks now.

Operational Checklist: Administrative, Physical, and Technical Safeguards

The following control categories organize Security Rule requirements into actionable checkpoints.

Administrative Safeguards

- [ ] Conduct and document a risk analysis covering all ePHI locations, threats, and vulnerabilities. Update annually or when systems change.
- [ ] Designate a Privacy Officer and a Security Officer with clear accountability for policies, audits, and incident response.
- [ ] Develop written policies and procedures for PHI privacy and ePHI security. Maintain version history and change logs.
- [ ] Implement workforce access management with least-privilege principles, provisioning workflows, and termination procedures.
- [ ] Deliver security awareness and HIPAA training to all workforce members. Log attendance and attestations.
- [ ] Execute Business Associate Agreements with every vendor that touches PHI. Verify safeguard implementation through due diligence.
- [ ] Establish incident response, sanctions, and breach notification playbooks. Address modern threats including ransomware, phishing, and AI-driven malware.
- [ ] Plan for contingency operations: backups, disaster recovery, and emergency-mode access.
- [ ] Retain all compliance documentation for six years from creation or last effective date.

Physical Safeguards

- [ ] Control facility access with badge systems, visitor logs, and locked server rooms.
- [ ] Set workstation use and placement rules: screen privacy filters, clean-desk routines, and restricted placement in public areas.
- [ ] Manage device and media lifecycle: inventory, secure storage, transport protocols, and sanitized disposal (wiping, shredding).

Technical Safeguards

- [ ] Assign unique user IDs and enforce strong authentication. Multi-factor authentication is commonly required for administrative and remote access.
- [ ] Apply role-based access controls that expose only the minimum necessary ePHI.
- [ ] Enable audit logging for access and activity across applications, databases, and endpoints. Centralize logs with tamper protection and retention.
- [ ] Deploy integrity controls that detect unauthorized changes and trigger alerts.
- [ ] Secure data in transit with TLS and at rest with encryption.
- [ ] Maintain secure configuration baselines and patch management schedules for all systems processing ePHI. Include connected medical devices and IoT endpoints under technical safeguard oversight.

Implementation Pathway

Conduct a Risk Analysis and Gap Assessment

1. **Inventory PHI and ePHI.** Map data flows, storage locations, and systems. Outcome: a current data landscape.
2. **Identify threats and vulnerabilities.** Apply NIST criteria to create a documented risk register.
3. **Measure likelihood and impact.** Prioritize risks and assign treatment plans with owners and deadlines. Outcome: an actionable risk treatment roadmap.
4. **Validate gaps against HIPAA standards.** Outcome: a compliance gap report aligned to Privacy, Security, and Breach Notification Rules.

Implement Policies, Procedures, and BAAs

1. **Write policies matching risk and workflow.** Outcome: rules the workforce can follow in daily operations.

   Publish and distribute the Notice of Privacy Practices. Outcome: patients understand their rights and how PHI is used
2. **Execute BAAs with all PHI vendors.** Outcome: contractual safeguards and breach-notification obligations in place.
3. **Publish and distribute the Notice of Privacy Practices. Outcome: patients understand their rights and how PHI is used**

Monitor, Audit, and Respond to Incidents

1. **Enable audit logging.** Outcome: traceable activity records for investigations and OCR audits.
2. **Run periodic access reviews and compliance audits.** Outcome: current and correct permissions.
3. **Use breach playbooks for timely response.** Outcome: notification to individuals and HHS within required (or anticipated accelerated) timelines.

HIPAA Compliance Officer Requirements and Governance

The Privacy Officer leads privacy policies, patient-rights workflows, authorization processes, and the Notice of Privacy Practices. The Security Officer oversees ePHI risk analysis, safeguard selection, monitoring, and incident response. Both roles commonly require experience in healthcare operations, information security, and regulatory frameworks. Effective compliance programs typically align with the Office of Inspector General's Seven Fundamental Elements: written policies and procedures, designated compliance officer and committee, effective training and education, effective lines of communication, well-publicized disciplinary standards, system for routine monitoring and auditing, and procedures for prompt response to detected offenses and corrective action.

Roles and Accountabilities

- Set policy, approve exceptions, and manage change control.
- Coordinate with Legal, IT, Clinical Operations, and HR.
- Own risk analysis execution and gap remediation.
- Lead investigations and breach notification processes.
- Report compliance status to executives and the board with quarterly metrics (training completion, audit findings, access exceptions closed, incident handling time).

Reporting Structure and Oversight

Compliance officers commonly report with independence to executive leadership. A cross-functional HIPAA committee (IT security, clinical operations, revenue cycle, legal) typically provides oversight. Minutes and decisions are documented for audit readiness.

Training Frequency, Topics, and Audience

Training supports ongoing compliance by keeping privacy and security knowledge current and reducing accidental disclosures. Organizations commonly deliver training at hire (before PHI access), annually for all workforce members, and through role-based refreshers for high-risk functions.

Training Topics

- PHI definition and examples
- Minimum necessary standard
- Safe handling: email, messaging, social media risks
- Breach reporting and sanctions
- Security fundamentals: passwords, phishing recognition, physical security

Audience

Clinical staff, billing, support, IT, contractors, and volunteers who interact with PHI typically complete training and sign attestations.

HIPAA Compliance Certification Landscape

No official government HIPAA certification exists. HHS and the Office for Civil Rights do not issue or endorse certification programs. Organizations may pursue third-party audits or attestations to demonstrate program maturity to customers and partners, but these do not replace OCR oversight or provide safe-harbor protections. Certification claims should reference the specific framework (e.g., HITRUST, SOC 2) rather than "HIPAA certified."

Software, Apps, and Cloud Vendors as Business Associates

Vendors that handle ePHI on behalf of covered entities are business associates and carry direct compliance obligations under the HIPAA Omnibus Rule. Cloud platforms, EHR add-ons, billing tools, and telehealth applications must implement Security Rule safeguards, sign BAAs, and support breach response and documentation.

Security by Design, Encryption, and Access Controls

- Design systems with privacy and security built in: threat modeling, secure coding, and regular penetration testing.
- Encrypt ePHI in transit and at rest using modern ciphers and strong key management.
- Enforce role-based access, unique IDs, and multi-factor authentication. Limit administrative access and audit elevated sessions.

Business Associate Agreements and Vendor Due Diligence

- Sign BAAs defining permitted uses, safeguards, breach notification duties, and subcontractor requirements.
- Conduct due diligence: review policies, architecture diagrams, penetration test summaries, and compliance attestations.
- Monitor vendors through periodic reviews of controls and breach-handling readiness.

Audit Logging, Monitoring, and Data Retention

- Log access and actions on PHI. Centralize logs and set alerts for anomalies.
- Retain required documentation and logs for six years.
- Define data lifecycle: retention, archival, and disposal. Shred paper, wipe media, and delete data according to policy.

Downloadable Resources and Required Forms

CMS HIPAA Basics for Providers (PDF)

Official summaries of Privacy, Security, and Breach Notification Rules.

HHS HIPAA Privacy Rule Overview

Patient rights and permitted uses.

Required Documentation

- Notice of Privacy Practices, patient acknowledgments, and access request logs
- Business Associate Agreements, vendor inventories, and due diligence records
- Risk analysis templates, audit checklists, and remediation logs
- Incident and breach logs: notifications, investigation notes, corrective actions
- Workforce training records: attendance, tests, sanctions, policy attestations

Frequently Asked Questions

What are the three important rules for HIPAA compliance?

The Privacy Rule governs PHI use, disclosure, and patient rights. The Security Rule mandates administrative, physical, and technical safeguards for ePHI. The Breach Notification Rule sets notification obligations and timelines. Organizations commonly align policies and training to all three.

What are the five HIPAA technical safeguards?

The Security Rule specifies five technical standards: access control (unique IDs, role-based permissions), audit controls (logging and monitoring), integrity (change detection), person or entity authentication (passwords, MFA), and transmission security (encryption in transit).

How do I know if I need to be HIPAA compliant?

Providers, health plans, and clearinghouses are covered entities. Vendors that create, receive, maintain, or transmit PHI for covered entities are business associates. Both groups carry direct compliance obligations under the Omnibus Rule.

What are five exceptions to HIPAA disclosure requirements?

HIPAA permits disclosures without authorization for treatment, payment, health care operations, public health activities, and as required by law. Minimum necessary rules and documentation still apply.

Conclusion and Next Steps

HIPAA compliance is a program, not a project. Know what PHI you hold. Apply layered safeguards. Train the workforce. Contract through BAAs. Maintain breach response capacity. The rules shift as technology and threats evolve.

2025 Security Rule NPRM. On January 6, 2025, HHS Office for Civil Rights published a Notice of Proposed Rulemaking that would mandate multi-factor authentication, continuous asset inventory, risk-based monitoring, encryption at rest and in transit, and automated audit logging. Comment period closed March 7, 2025. Final rule expected in 2026 with 12-month implementation window. HHS tied the proposal to NIST Cybersecurity Framework 2.0 and the 2024 HHS Cybersecurity Performance Goals.

First-year implementation carries an estimated $9 billion industry cost. The draft includes phasing for small practices. Early adopters gain operational time before enforcement tightens.

Planning Considerations

- Run a current-year risk analysis and prioritize remediation within 90 days.
- Update policies, BAAs, and training materials to reflect operational changes and 2025 regulatory developments.
- Enable comprehensive logging, conduct an internal audit, and close access gaps.
- Test breach playbooks and confirm notification workflows account for potential 24-hour timelines.
- Publish or refresh the Notice of Privacy Practices and patient-facing materials.

Official Guidance and Resources

Start with HHS Office for Civil Rights materials and the CMS HIPAA Basics PDF. NIST SP 800-66 provides detailed security mapping. HIPAA Journal and similar industry resources offer context, but confirm regulatory details against official sources. For breach reporting, visit the HHS breach portal. Use the risk analysis templates, audit checklists, and training logs linked above to accelerate implementation.

Treat this checklist as a living control document. Keep it accessible for audits, board briefings, and onboarding. Assign owners and dates, then schedule the first compliance audit.

Legal and Compliance Advisory Support

Dunlap Bennett & Ludwig advises healthcare providers, technology vendors, and life-sciences organizations on HIPAA compliance, Security Rule readiness, vendor contracting, and breach response. Our approach focuses on building defensible compliance programs that withstand OCR audits, enforcement actions, and transactional scrutiny.

About the Author

Craig Besnoy is a Partner at Dunlap Bennett & Ludwig, where he advises on cybersecurity, data privacy, and regulatory compliance with a core focus on mergers, acquisitions, and strategic transactions involving data-driven and highly regulated businesses. He works extensively with healthcare organizations, financial services firms, technology companies, and investors on cybersecurity risk management, HIPAA compliance, incident response, and third-party risk oversight.

Craig has more than a decade of experience advising on complex transactions and compliance matters in which data security and privacy risk are material considerations, including acquisitions, restructurings, and growth-stage investments. His experience includes helping physician-owned practices achieve HIPAA compliance and training physicians and staff on privacy and security best practices as part of pre-acquisition readiness efforts. He is admitted to practice in New York and is recognized for translating evolving cybersecurity and privacy regulations into operationally practical and legally defensible frameworks.

Strategic Partnership for Legal Protection

This article highlights risk analysis workflows, BAA execution, breach notification timelines, the OIG Seven Elements framework, and emerging Security Rule proposals around MFA, asset inventory, and continuous risk assessment. Dunlap Bennett & Ludwig helps teams turn these regulatory requirements into defensible operational patterns so compliance timelines, audit readiness, and incident response hold up under OCR scrutiny.

If you are aligning vendor contracts, preparing for accelerated breach notification windows, or implementing 2026 Security Rule controls, our attorneys can help you design guardrails that protect both execution timelines and long-term defensibility.

Call 888-306-4030 or email **clientservices@dbllawyers.com**.

Dunlap Bennett & Ludwig is a veteran-owned law firm with offices across multiple states. Our privacy and business attorneys combine legal expertise with practical operational experience to help companies navigate GDPR compliance while maintaining focus on their core business objectives.

To learn more about Dunlap Bennett & Ludwig, call **888-306-4030** or email **clientservices@dbllawyers.com**.

References

1. U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. Accessed October 26, 2025. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
2. Centers for Medicare and Medicaid Services. HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules. Accessed October 26, 2025. https://www.cms.gov/files/document/mln909001-hipaa-basics-providers-privacy-security-breach-notification-rules.pdf
3. U.S. Department of Health and Human Services Office for Civil Rights. Breach Notification Rule Guidance and Portal. Accessed October 26, 2025. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
4. U.S. Department of Health and Human Services. HIPAA Security Rule Guidance. Accessed October 26, 2025. https://www.hhs.gov/hipaa/for-professionals/security/index.html
5. HIPAA Journal. HIPAA Compliance Guidelines. Accessed October 26, 2025. https://www.hipaajournal.com/hipaa-compliance-guidelines/
6. Varonis. HIPAA Compliance: Your Complete 2025 Checklist. Accessed October 26, 2025. https://www.varonis.com/blog/hipaa-compliance
7. Kiteworks. HIPAA Compliance: Requirements and Checklists. Accessed October 26, 2025. https://www.kiteworks.com/hipaa-compliance/hipaa-compliance-requirements/
8. National Institute of Standards and Technology. Introductory Resource Guide for Implementing the HIPAA Security Rule (NIST SP 800-66 Rev. 2). Accessed October 26, 2025. https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final