PETRONELLA TECHNOLOGY GROUP

FREE PLAYBOOK · 2026 EDITION

HIPAA COMPLIANCE PLAYBOOK

A practical playbook for medical practices, dental offices, behavioral-health providers, and the IT teams that support them. Security Rule safeguards, Privacy Rule implementation, risk analysis, Business Associate Agreements, breach response, HITECH, and the 2024 NPRM updates — all in one 24-page reference.

Author: Craig Petronella — CMMC-RP, CCNA, CWNE, DFE #604180
Publisher: Petronella Technology Group · Raleigh, NC · Founded 2002
Credentials: Entire team CMMC Registered Practitioner · PPSB Accredited · BBB A+ since 2003

Contents

Every chapter cites the primary regulation and HHS / NIST guidance it is based on. Use the page numbers to jump straight to what your practice needs.

> **Disclaimer.** This playbook is educational reference material, not legal advice. HIPAA enforcement is conducted by the U.S. Department of Health & Human Services Office for Civil Rights (OCR). For binding legal interpretation, consult qualified healthcare counsel. No such thing as a "HIPAA-certified" vendor exists in U.S. law — Petronella Technology Group is a HIPAA-focused IT and compliance services firm, not a HIPAA auditor.

How to Use This Playbook

HIPAA is a living compliance program, not a one-time project. The practices that do well in an OCR investigation are not the ones with the thickest binder — they are the ones whose daily operations match their documentation.

This playbook is structured to be read front-to-back the first time, then used as a reference whenever a specific situation arises: a new vendor, a lost laptop, a ransomware alert, a patient records request, an audit letter.

The four regulations you need to know

- **The Privacy Rule** — 45 CFR Part 160 and Subparts A and E of Part 164. Governs the use and disclosure of Protected Health Information (PHI).
- **The Security Rule** — 45 CFR Part 160 and Subparts A and C of Part 164. Governs the administrative, physical, and technical safeguards for electronic PHI (ePHI).
- **The Breach Notification Rule** — 45 CFR 164.400-414. Governs what to do and who to notify when unsecured PHI is breached.
- **The Enforcement Rule** — 45 CFR Part 160, Subparts C-E. Governs how HHS investigates and imposes civil money penalties.

Who is covered?

HIPAA applies to two groups:

1. **Covered Entities:** health plans, healthcare clearinghouses, and healthcare providers that transmit any health information in electronic form in connection with a HIPAA transaction (which includes virtually every practice that bills electronically).
2. **Business Associates:** any person or entity that creates, receives, maintains, or transmits PHI on behalf of a Covered Entity — cloud storage vendors, IT managed service providers, billing services, transcription services, law firms that review PHI, and so on. Since HITECH, Business Associates are directly liable for Security Rule compliance and most Privacy Rule provisions.

What is PHI and ePHI?

PHI is individually identifiable health information held or transmitted by a Covered Entity or Business Associate in any form (paper, oral, electronic). ePHI is the subset that is electronic — the focus of the Security Rule.

PHI includes the 18 identifiers listed at 45 CFR 164.514(b)(2)(i), including name, address, dates (except year), phone, email, SSN, medical record number, health plan beneficiary number, account number,

certificate or license number, device identifier, URL, IP address, biometric identifier, photograph, and any other unique identifying characteristic.

> **Pro tip.** If you handle data that is technically de-identified but can be re-identified with reasonable effort, treat it as PHI. The expert determination and safe-harbor methods at 45 CFR 164.514 are strict for a reason.

Chapter 1 · Security Rule Technical Safeguards

The Security Rule organizes safeguards into three categories: **administrative** (45 CFR 164.308), **physical** (45 CFR 164.310), and **technical** (45 CFR 164.312). This chapter focuses on the technical safeguards — the ones your IT vendor is supposed to implement.

Each standard is either **Required (R)** or **Addressable (A)**. Addressable does not mean optional. It means you must either implement it, implement a reasonable equivalent, or document why it is not reasonable and appropriate for your practice — and then document what you are doing instead.

1.1 Access Control · 45 CFR 164.312(a)(1)

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

- **Unique User Identification (R)** — Each workforce member gets a unique username. No shared logins. This is the single most-cited technical failing in OCR investigations.
- **Emergency Access Procedure (R)** — A documented way to access ePHI in an emergency (for example, break-glass accounts with audited logs).
- **Automatic Logoff (A)** — Session timeouts on workstations with ePHI. Industry practice: 10-15 minutes of inactivity.
- **Encryption and Decryption (A)** — Encrypt ePHI at rest. Encryption is "addressable" but if you do not encrypt and you lose a laptop, you must notify under the Breach Notification Rule. If the device was encrypted to FIPS 140-2 (now 140-3) standards, the breach notification obligation may not apply — that is what the HHS Guidance to Render Unsecured PHI Unusable calls "safe harbor."

1.2 Audit Controls · 45 CFR 164.312(b) · Required

Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

- Log all access to ePHI — who, what, when, from where.
- Protect logs from tampering (write-once storage or a SIEM).
- **Review logs regularly.** OCR routinely asks for evidence of review, not just existence of logs. A monthly documented review is the minimum defensible cadence.

1.3 Integrity · 45 CFR 164.312(c)(1)

Protect ePHI from improper alteration or destruction.

- **Mechanism to Authenticate ePHI (A)** — Checksums, hashing, digital signatures, version control in the EHR.

- Backups are part of integrity too. Test them at least quarterly.

Source: 45 CFR 164.312; HHS OCR HIPAA Security Rule Guidance; NIST SP 800-66 Revision 2 (Feb 2024).

1.4 Person or Entity Authentication · 45 CFR 164.312(d) · Required

Verify that the person or entity seeking access to ePHI is the one claimed. In 2026, this almost always means **multi-factor authentication (MFA)**.

- Passwords alone are no longer defensible. The 2024 HIPAA Security Rule NPRM explicitly proposes making MFA required for all ePHI access.
- Prefer phishing-resistant MFA (FIDO2 security keys, platform authenticators) over SMS one-time codes.
- Apply MFA not just to the EHR but also to email, remote access (VPN, RDP, cloud consoles), backup systems, and administrative accounts in any system that touches ePHI.

1.5 Transmission Security · 45 CFR 164.312(e)(1)

Protect ePHI that is being transmitted over an electronic communications network.

- **Integrity Controls (A)** — TLS 1.2 or 1.3 for all ePHI in transit. Disable TLS 1.0 and 1.1 on every server and mail gateway.
- **Encryption (A)** — Email containing PHI must be encrypted. Options: TLS-only enforcement with trusted recipients; portal-based secure messaging; or dedicated encrypted email platforms. Standard Gmail/Outlook.com does not reliably encrypt in transit to every recipient.

1.6 Mapping the technical safeguards to NIST SP 800-53

NIST SP 800-66r2 is the HHS-referenced crosswalk between the HIPAA Security Rule and NIST SP 800-53 security controls. Use this table to translate HIPAA obligations into your existing NIST control catalog (common in healthcare organizations that also do federal work).

HIPAA Standard	NIST SP 800-53 Control Family	Example Controls
Access Control 164.312(a)	AC (Access Control), IA (Identification & Authentication)	AC-2, AC-3, IA-2, IA-5
Audit Controls 164.312(b)	AU (Audit & Accountability)	AU-2, AU-3, AU-6, AU-12
Integrity 164.312(c)	SI (System & Info Integrity), CP (Contingency Planning)	SI-7, CP-9, CP-10
Authentication 164.312(d)	IA (Identification & Authentication)	IA-2(1), IA-2(2), IA-5
Transmission 164.312(e)	SC (System & Comms Protection)	SC-8, SC-8(1), SC-13

> **Use the crosswalk.** If your EHR or cloud vendor publishes a SOC 2 or HITRUST report aligned with NIST 800-53, this table lets you tie their controls directly to your HIPAA obligations. That is how you document "addressable" decisions with something more substantial than a policy paragraph.

Source: NIST SP 800-66 Revision 2, "Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide" (February 2024).

1.7 Administrative safeguards that support the technical ones

You cannot implement the technical safeguards in isolation. Three administrative standards drive them:

- **Security Management Process · 164.308(a)(1)** — risk analysis, risk management, sanction policy, information system activity review.
- **Assigned Security Responsibility · 164.308(a)(2)** — a named Security Official (does not have to be full-time; does have to be documented).
- **Workforce Security · 164.308(a)(3)** — authorization, clearance, termination procedures. Every OCR case we have seen involving an insider-access breach comes back to broken termination procedures.

1.8 Physical safeguards · 164.310

- Facility Access Controls — lock server rooms, log visitors.
- Workstation Use and Workstation Security — screens that face away from waiting rooms, privacy filters, cable locks.
- Device and Media Controls — disposal (NIST 800-88 wipe or physical destruction), re-use, accountability (asset inventory), backup storage location.

1.9 Common enforcement themes (2018-2025 OCR resolution agreements)

Looking at resolution agreements published on hhs.gov/ocr, the same failings recur:

- No enterprise-wide risk analysis (the single most-cited issue).
- No risk management plan following from the analysis.
- Stolen or lost unencrypted devices containing ePHI.
- Missing or out-of-date Business Associate Agreements.
- Impermissible disclosures of PHI on social media or to media.
- Inadequate response to patient right-of-access requests (the HIPAA Right of Access Initiative has generated dozens of settlements since 2019).

> **The pattern.** Most six- and seven-figure settlements do not stem from a single headline breach — they stem from the investigation that followed, which revealed that the covered entity had no current risk analysis, no risk management plan, and gaps in training and BAAs. Those are the same four items that start and end this playbook.

Chapter 1 checklist — take to your next IT meeting

- [ ] Every workforce member has a unique login. No shared credentials.
- [ ] MFA enforced on the EHR, email, VPN/RDP, cloud admin consoles, and backup system.
- [ ] Session auto-logoff of 10-15 minutes on all ePHI-handling workstations.
- [ ] Full-disk encryption on every laptop, mobile device, and backup drive that stores ePHI.
- [ ] TLS 1.2 or 1.3 enforced; TLS 1.0 and 1.1 disabled on mail and web servers.
- [ ] A documented method for sending encrypted email with PHI.
- [ ] Audit logs enabled in the EHR and the identity provider, retained at least 6 years.
- [ ] Monthly documented review of those logs.
- [ ] Asset inventory with owner, location, encryption status for every device that touches ePHI.
- [ ] A named Security Official on file, with backup.
- [ ] Documented onboarding and termination procedures, followed and evidenced with timestamps.

The "addressable" myth

The most misunderstood word in the Security Rule is "addressable." If you decide a standard is not reasonable and appropriate, you must:

1. Document the decision and the rationale.
2. Implement an equivalent alternative measure.
3. Document that alternative and review it whenever your environment changes.

"We did not do it because it was addressable" is not a defense. "We decided this standard did not fit our environment because X, and instead we implemented Y, as documented in our Security Management Process dated MM/DD/YYYY" is a defense.

Source: 45 CFR 164.306(d); HHS OCR HIPAA Security Rule Guidance.

Chapter 2 · Privacy Rule Implementation

The Privacy Rule governs the *use and disclosure* of PHI in any form — paper, oral, or electronic. Where the Security Rule is "how," the Privacy Rule is "what" and "why."

2.1 The baseline rule

A Covered Entity may not use or disclose PHI except as permitted or required by the Privacy Rule — 45 CFR 164.502(a). Everything else in the Privacy Rule is elaboration on that sentence.

2.2 Permitted uses and disclosures without authorization

- **To the individual** — 164.502(a)(1)(i). Always permitted.
- **For Treatment, Payment, and Health Care Operations (TPO)** — 164.506. The day-to-day operational permission.
- **With written authorization** — 164.508. Required for marketing, sale of PHI, most psychotherapy notes, and any disclosure not otherwise permitted.
- **Opportunity to agree or object** — 164.510. Facility directories, notification of family.
- **Public interest categories** — 164.512. Required by law, public health, abuse, health oversight, judicial proceedings, law enforcement, organ donation, research (with safeguards), serious threat, workers comp.
- **Limited Data Sets** — 164.514(e). With a Data Use Agreement, for research, public health, or operations.

2.3 The minimum necessary standard · 164.502(b)

When using, disclosing, or requesting PHI, limit the information to the minimum necessary to accomplish the intended purpose. Exceptions: disclosures to the individual, uses for treatment, disclosures under authorization from the individual, and disclosures required by law.

In practice, minimum necessary means role-based access in the EHR. A front-desk user should not see clinical notes; a billing user should not see psychotherapy notes; a referring-provider portal should not expose the whole chart.

> **Practice tip.** Minimum necessary is also the argument for data minimization in your web forms, fax cover sheets, and referral letters. If you do not need it, do not collect it.

2.4 Notice of Privacy Practices (NPP) · 164.520

Every direct-treatment provider must give each new patient a Notice of Privacy Practices and make a good-faith effort to obtain the patient's written acknowledgment of receipt (or document why one was not obtained). The NPP must be:

- Available in the office and prominently posted on the practice website.
- Revised whenever material privacy practices change.
- Written in plain language. Include the patient's rights, the practice's duties, and contact information for complaints (internal complaint contact *and* the HHS OCR address).

Source: 45 CFR 164.502, 164.506, 164.508, 164.512, 164.514, 164.520.

2.5 Patient rights under the Privacy Rule

Right of Access · 164.524

Patients have the right to inspect and obtain a copy of their PHI in a designated record set, in the form and format requested if readily producible. Response deadlines:

- **30 days** from the request (one 30-day extension allowed with written notice explaining the delay).
- Fees limited to labor for copying, supplies, postage, and preparation of an explanation or summary if requested. Retrieval fees are not allowed.

> **Enforcement alert.** The HHS OCR Right of Access Initiative has generated dozens of settlements since 2019, with penalties typically in the range of $5,000 to $240,000 per case. Missed response deadlines and inflated fees are the two most common triggers.

Right to Amend · 164.526

Patients can request amendment of PHI in the designated record set. The practice must respond within 60 days (one 30-day extension allowed). If denied, the patient can submit a statement of disagreement that must be included with future disclosures of the disputed PHI.

Right to Accounting of Disclosures · 164.528

Patients can request a list of disclosures of their PHI made by the practice in the prior six years (excluding TPO, disclosures to the individual, and a few other categories).

Right to Request Restrictions · 164.522

Patients may request restrictions on how their PHI is used or disclosed. The practice is not required to agree — except for one case: if a patient pays in full, out of pocket, for a service, they can require the practice not to disclose that service to their health plan.

Right to Confidential Communications · 164.522(b)

Patients can request communication by alternative means or at alternative locations — for example, "call my mobile, not my home" or "mail to a P.O. Box, not my house." Practices must accommodate reasonable requests.

2.6 Uses and disclosures requiring authorization

Written authorization is required for:

- Marketing (with narrow exceptions for face-to-face communications and promotional gifts of nominal value).
- Sale of PHI.

- Most uses and disclosures of psychotherapy notes.
- Any other use or disclosure not otherwise permitted by the Privacy Rule.

A valid authorization must include: a description of the PHI to be used or disclosed, the persons authorized to use or disclose, the persons who can receive, the purpose, an expiration date or event, the individual's signature and date, and the required statements about the right to revoke and the possibility of redisclosure — 164.508(c).

2.7 The 2024 Reproductive Health Privacy Final Rule

On April 26, 2024, HHS published a final rule (89 FR 32976) modifying the Privacy Rule to strengthen protections for reproductive health care information. The key changes took effect December 23, 2024 for most provisions, with compliance required by February 16, 2026 for updated Notices of Privacy Practices.

What changed

- **New prohibition.** A Covered Entity or Business Associate may not use or disclose PHI for investigating or imposing liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that was lawful under the circumstances in which it was provided.
- **Attestation requirement.** When PHI potentially related to reproductive health care is requested for certain purposes (health oversight, judicial proceedings, law enforcement, coroner/medical examiner), the requester must sign an attestation that the use or disclosure is not for a prohibited purpose.
- **Updated NPP language.** Practices must update their Notice of Privacy Practices to describe these new protections by February 16, 2026.

What your practice should do

- [ ] Update your Notice of Privacy Practices before February 16, 2026.
- [ ] Build an attestation intake process for relevant requests (often built into the EHR release-of-information workflow).
- [ ] Train intake, release-of-information, and front-desk staff on how to recognize and route in-scope requests.
- [ ] Document the attestation with each disclosure so you have evidence of compliance.

2.8 Marketing, sale, and fundraising

Three nuances that trip up practices:

- **Marketing** is defined narrowly at 164.501 but broadly interpreted. "Refill reminders" are treatment, not marketing, if the communication is about a drug the individual is already prescribed.
- **Sale of PHI** requires authorization and must disclose that remuneration is being received — 164.508(a)(4).
- **Fundraising** to existing patients is permitted for limited demographic and treatment information, but each fundraising communication must include a clear opt-out and the practice must honor opt-outs permanently — 164.514(f).

Chapter 2 checklist

- [ ] Current Notice of Privacy Practices posted in office and on website, matching pre-2024 and post-2024 requirements.
- [ ] Staff trained on minimum necessary, NPP, patient rights, and the 2024 reproductive health protections.
- [ ] Role-based access configured in the EHR; least privilege reviewed quarterly.
- [ ] Documented 30-day response process for right of access requests, with extension tracking.
- [ ] Documented 60-day response process for amendment requests.
- [ ] Accounting-of-disclosures log maintained for six years.
- [ ] Authorization form meeting all 164.508 elements, kept in the patient record with each disclosure it authorized.
- [ ] Process for out-of-pocket restriction requests.
- [ ] Attestation intake workflow for reproductive health-related disclosures.
- [ ] Documented complaint process with both internal contact and HHS OCR contact information.

> **Right of Access is low-hanging fruit.** If you review only one Privacy Rule process before OCR knocks, make it your right-of-access workflow. This is where most recent enforcement settlements live, the standard is clear, and the fix is almost entirely operational rather than technical.

Source: 45 CFR 164.522, 164.524, 164.526, 164.528; HHS 2024 Reproductive Health Privacy Final Rule (89 FR 32976).

Chapter 3 · Risk Analysis (Risk Assessment)

The Risk Analysis requirement at 45 CFR 164.308(a)(1)(ii)(A) is the single most important control in the HIPAA Security Rule. It is also the most commonly missing document in OCR investigations. This chapter walks through a risk analysis aligned with **NIST SP 800-66 Revision 2** — the February 2024 crosswalk that HHS publishes as its explicit reference guide.

3.1 What the regulation requires

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."

The regulation is deliberately technology-neutral. Any methodology that is accurate and thorough qualifies — NIST SP 800-30 and SP 800-66 are the most commonly cited.

3.2 The nine-step risk analysis

Step 1 — Scope of the analysis

Inventory every system, device, application, third-party service, and medium (paper, oral) that creates, receives, maintains, or transmits ePHI. This is your ePHI Asset Inventory.

Step 2 — Data collection

Document where ePHI lives, how it flows, and who has access. Data flow diagrams are strongly recommended.

Step 3 — Identify and document potential threats and vulnerabilities

Threats (ransomware, insider misuse, lost laptop, vendor breach, natural disaster) combined with vulnerabilities (missing MFA, unpatched EHR, orphaned accounts, unencrypted backup) produce risk scenarios.

Step 4 — Assess current security measures

For each threat/vulnerability pair, document the controls currently in place and how effective they are.

Step 5 — Determine the likelihood of threat occurrence

Scale: Low / Medium / High. Use historical incident data (yours or industry reports) where possible.

Step 6 — Determine the potential impact

Consider the number of records, sensitivity, regulatory exposure, financial cost of breach response, reputational impact.

Step 7 — Determine the level of risk

Likelihood x Impact, rated Low / Medium / High. Document the rationale for each rating — not just the number.

Step 8 — Finalize documentation

The risk analysis document is a living artifact. Date it, version it, attribute it to the person who performed it, and sign it.

Step 9 — Periodic review and updates

Review at least annually and after any significant environmental or operational change (new EHR, new office, new Business Associate, new service line).

Source: 45 CFR 164.308(a)(1)(ii)(A); NIST SP 800-66 Revision 2; NIST SP 800-30 Revision 1.

3.3 Risk Analysis Worksheet — template skeleton

Use this template as the baseline for every entry in your risk analysis. Every row produces one risk decision (accept, mitigate, transfer, or avoid) that then feeds the Risk Management Plan at 45 CFR 164.308(a)(1)(ii)(B).

Asset / System	Threat	Vulnerability	Current Controls	Likelihood	Impact	Risk	Decision
EHR (SaaS)	Credential theft via phishing	No MFA on email or EHR	Password policy only	High	High	High	Mitigate: enforce MFA
Laptops (12)	Device loss/theft	No full-disk encryption	Cable locks	Med	High	High	Mitigate: deploy BitLocker/FileVault
On-prem backup NAS	Ransomware	Backups not air-gapped	Daily backup	High	High	High	Mitigate: immutable offsite
Fax machine	Misdirected fax	Manual dialing	Cover sheet policy	Med	Low	Med	Mitigate: digital fax w/ confirmation
Cloud storage (BA)	Vendor breach	No BAA signed	None	Low	High	High	Mitigate: sign BAA or replace vendor

3.4 The Risk Management Plan

The risk analysis identifies risks. The risk management plan documents the decisions. Each "Mitigate" row produces an action item with an owner, a deadline, and a verification step. Each "Accept" row produces a risk acceptance memo signed by the Security Official.

> **OCR tip.** When OCR opens an investigation, one of the first document requests is: "Please produce the most recent risk analysis and the risk management plan that follows from it." Practices that can produce both are typically two years ahead of practices that cannot.

Chapter 3 checklist

- [ ] Written ePHI asset inventory maintained and reviewed annually.
- [ ] Data flow diagram showing how ePHI moves between systems, vendors, and locations.
- [ ] Risk analysis aligned with NIST SP 800-66r2, dated and signed.
- [ ] Risk management plan with owners and due dates for each mitigation.
- [ ] Risk acceptance memos for any risks being accepted, signed by the Security Official.
- [ ] Annual review scheduled with a documented trigger for off-cycle reviews.
- [ ] Risk analysis artifacts retained for at least six years (HIPAA minimum retention).

Common gaps

- **Scope too narrow.** A risk analysis of "the EHR only" is not compliant. It must cover every system, vendor, and medium that touches ePHI.
- **Vulnerability scan confused with risk analysis.** A Nessus scan is a vulnerability assessment, not a risk analysis. It feeds the risk analysis; it is not a substitute for it.
- **No management plan.** The analysis documents risks; the management plan says what you are going to do about each one. Missing the second document is almost as bad as missing the first.
- **Forgotten paper, fax, voicemail, and mobile devices.** These are the easiest risks to miss and some of the most commonly breached.

Chapter 4 · Business Associate Agreements

4.1 Who is a Business Associate?

A Business Associate (BA) is any person or entity (other than a member of the Covered Entity's workforce) that creates, receives, maintains, or transmits PHI on behalf of a Covered Entity to perform functions or activities regulated by HIPAA — 45 CFR 160.103.

Common Business Associates in medical practices:

- Cloud-based EHR, PM, and billing platforms.
- Managed IT service providers and cloud-backup providers.
- Transcription services.
- Collection agencies.
- Answering services.
- Shredding and document storage services.
- Accountants and law firms that review PHI in the course of their work.
- Marketing vendors that handle patient lists.

Not a Business Associate: conduit-only services (US Postal Service, standard internet carriers without access to content), members of your own workforce, financial institutions processing standard payment transactions, and another Covered Entity when disclosures are for treatment.

4.2 Required provisions under 45 CFR 164.504(e)

Every Business Associate Agreement must include, at minimum:

1. Establish the permitted and required uses and disclosures of PHI by the BA.
2. Provide that the BA will not use or further disclose the PHI other than as permitted by the contract or required by law.
3. Require the BA to implement appropriate safeguards (administrative, physical, technical) for the ePHI.
4. Require the BA to report to the Covered Entity any use or disclosure not provided for by the contract, and any security incidents and breaches of unsecured PHI.
5. Require the BA to ensure that any subcontractors that create, receive, maintain, or transmit PHI agree to the same restrictions via their own BAAs.
6. Require the BA to make PHI available for access, amendment, and accounting of disclosures as required by the Privacy Rule.
7. Require the BA to make its internal practices, books, and records relating to PHI available to HHS for compliance purposes.

8. Require the BA to return or destroy all PHI at termination if feasible; if not, to extend the protections to retained PHI and limit further use and disclosure.
9. Authorize the Covered Entity to terminate the contract if the BA materially violates it.

> **Direct liability.** Since HITECH (45 CFR 164.502(e)(1)(ii)), Business Associates are directly liable to HHS for Security Rule compliance and for many Privacy Rule provisions. The BAA is not just a Covered Entity protection device; it is also the BA's roadmap to its own compliance obligations.

4.3 Vendor due diligence before signing

A signed BAA is necessary but not sufficient. Before onboarding any vendor that will handle PHI, ask for evidence of:

- Recent independent audit report (SOC 2 Type II, HITRUST r2, ISO 27001) covering the services you are buying.
- Encryption at rest and in transit, with the algorithm and key management disclosed.
- Incident response plan with breach-notification SLAs (24-72 hours is the common industry standard).
- Subcontractor list and confirmation that subcontractors have executed BAAs.
- Data-return or data-destruction commitment at contract end (with NIST SP 800-88 media sanitization for destruction).
- Cyber insurance coverage with limits commensurate with your PHI exposure.
- Data residency (specifically: does PHI leave the United States? Some state laws and federal contracts care about this even when HIPAA does not directly require it).

4.4 Vendor monitoring after signing

- Annual BAA review and re-signing where term expires.
- Annual request for updated SOC 2 or HITRUST report.
- Tracking of vendor breach notifications (the vendor's breach becomes your Breach Notification Rule obligation).
- Offboarding checklist at contract termination: revoke access, retrieve or confirm destruction of PHI, document completion.

4.5 Common BAA gotchas

> **Gotcha #1:** Using the vendor's one-sided BAA without review. Vendor BAAs often cap liability, disclaim warranties, and waive indemnification — each of which is a risk transfer back to your practice.

> **Gotcha #2:** No BAA with your IT managed service provider. If your MSP has remote access, credentials, or backups containing ePHI, they are a Business Associate.

> **Gotcha #3:** Free tools with no BAA path. Free or "consumer" tiers of cloud services typically do not offer a BAA. Paid "business" or "enterprise" tiers do — but you must execute the BAA separately.

4.6 Subcontractor BAAs

If a Business Associate uses subcontractors (for example, your EHR vendor uses a cloud hosting provider), the BA must have BAAs with each of them. You are not required to have a direct BAA with subcontractors — but you are entitled to ask for and review the list.

4.7 Business Associate Agreement — template skeleton

This skeleton lists the mandatory sections required by 45 CFR 164.504(e) and the practical supplements we recommend. It is **not** a legal template — execute only after review by qualified healthcare counsel.

1. **Definitions** — incorporate definitions from 45 CFR 160.103 and 164.501.
2. **Permitted uses and disclosures** — describe the services and the scope of PHI access.
3. **Prohibited uses and disclosures** — catch-all prohibition beyond what the contract permits.
4. **Safeguards** — administrative, physical, and technical; explicit reference to 45 CFR 164.308, 164.310, 164.312.
5. **Reporting** — impermissible uses/disclosures, security incidents, breaches of unsecured PHI. Include a specific SLA (for example, notify within 24 hours of discovery).
6. **Subcontractors** — require written BAAs with all subcontractors; maintain current list; provide list on request.
7. **Individual rights support** — access, amendment, accounting of disclosures within specified timelines.
8. **HHS access** — make records available to HHS for compliance review.
9. **Mitigation** — BA agrees to mitigate any harmful effect of unauthorized use or disclosure.
10. **Term & termination** — effective date, term, termination for cause, cure periods.
11. **Return or destruction of PHI at termination** — define method (NIST SP 800-88), deadline, and certification.
12. **Permitted uses of PHI for BA's own management and administration** — narrow carve-out under 164.504(e)(4).
13. **Indemnification & liability** — practical supplement; not required by 164.504(e).
14. **Insurance** — cyber liability and errors-and-omissions coverage with minimum limits.
15. **Audit rights** — right to request SOC 2 / HITRUST / penetration test reports annually.
16. **Data location** — specify US data residency if applicable.
17. **Amendment** — written amendment process to accommodate regulatory change.
18. **Governing law & venue.**
19. **Entire agreement, severability, notices.**
20. **Signatures** — authorized representatives of both parties; effective date.

> **Using this skeleton.** Take this list to your healthcare attorney. Most HIPAA-experienced counsel will draft a custom BAA from this structure for a flat fee in the low four figures. Do not use free online generators for anything you intend to rely on in an OCR defense.

Chapter 5 · Breach Response — The 72-Hour Playbook

5.1 What counts as a breach?

45 CFR 164.402 defines a breach as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."

An impermissible use or disclosure is *presumed* to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised, based on a risk assessment considering at least:

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

5.2 The safe-harbor exception

If the PHI was encrypted to the HHS-specified standards (FIPS 140-2/140-3 at rest, TLS for in transit) at the time of the breach, it is not considered "unsecured" — and the Breach Notification Rule does not require notification. This is the single largest reason to encrypt by default.

5.3 The notification timelines

Individuals — 164.404

Notify affected individuals without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach. Written notice by first-class mail (or email if the individual has agreed). Must include description, types of info involved, steps the individual should take, mitigation steps, and contact information.

HHS Secretary (OCR) — 164.408

Report via the OCR breach portal:

- **If 500 or more individuals** are affected: concurrently with individual notification (i.e., within 60 days of discovery).
- **If fewer than 500**: annually, within 60 days after the end of the calendar year in which the breach was discovered.

Media — 164.406

If 500+ individuals in a single state or jurisdiction are affected, notify prominent media outlets serving that jurisdiction, without unreasonable delay and no later than 60 days after discovery.

Business Associate to Covered Entity — 164.410

A BA must notify the Covered Entity of a breach without unreasonable delay and in no case later than 60 days after discovery. Your BAA should tighten this to 24-72 hours.

> **State laws are on top, not instead.** Every state has its own breach notification law with its own deadlines, content requirements, and attorney general notification triggers. Several states require notification within 30 days. State AG notifications, credit monitoring offers, and state-specific content requirements are in addition to HIPAA.

Source: 45 CFR 164.400-414; HHS Breach Notification Rule; HHS Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable.

5.4 The 72-hour decision tree

The goal of the first 72 hours is not to notify — the goal is to preserve evidence, limit the blast radius, and set up a defensible record of how you responded. Notification comes later (within 60 days). Rushing to notify before you understand scope creates its own compliance problems.

Hour 0 to 4 — Detect and contain

1. Invoke the Incident Response Plan. Pull out the signed, dated version.
2. Activate the incident response team (Security Official, a clinical leader, IT/MSP, counsel, privacy officer, communications).
3. Contain the incident. Isolate, disconnect, disable credentials — do not power down machines if forensic preservation is needed.
4. Start a written incident timeline. Every decision, timestamp, and action. This becomes evidence.

Hour 4 to 24 — Investigate scope

1. Engage a digital forensics vendor if ePHI may have been exfiltrated. Chain of custody on logs, drives, memory.
2. Identify what data was affected, how many individuals, what identifiers, and whether the PHI was encrypted.
3. Notify cyber insurance carrier. Most policies require notification within hours; late notification is a common claim denial reason.
4. Engage breach counsel. Attorney-client privilege on the forensic work product where appropriate.
5. Preserve logs beyond normal retention. Many practices lose critical evidence because their EHR or firewall rotated logs in the first week.

Hour 24 to 72 — Analyze and decide

1. Conduct the four-factor risk assessment at 164.402. Document it.
2. Determine whether safe harbor applies (encrypted to HHS standards at time of breach).
3. Decide: reportable breach, not a reportable breach, or further investigation needed.
4. If reportable: start drafting individual notification letters, OCR portal submission, media statement, and state AG notification packages.
5. Continue containment and remediation work in parallel.

5.5 What to document (always)

- [ ] Discovery date and how the incident was discovered.
- [ ] Root cause (or hypothesis if forensics is ongoing).
- [ ] Containment and remediation actions with timestamps.

- [ ] PHI inventory: data elements, number of individuals, encryption status.
- [ ] Four-factor risk assessment with rationale for the conclusion.
- [ ] Notification decisions and rationale (including any not-a-breach decisions).
- [ ] Copies of all notifications sent.
- [ ] Remediation follow-up (what you changed so this cannot happen again).

5.6 72-Hour Breach Response Checklist — print and post

Detect / Contain (first 4 hours)

- [ ] Invoke Incident Response Plan; record exact discovery time.
- [ ] Assemble incident response team: Security Official, IT/MSP, counsel, privacy officer, clinical lead, communications.
- [ ] Contain (isolate affected systems, disable credentials, block exfiltration).
- [ ] Start written incident timeline.
- [ ] Do *not* wipe or reimage yet — preserve forensic evidence.

Investigate (4-24 hours)

- [ ] Engage digital forensics provider.
- [ ] Notify cyber insurance carrier.
- [ ] Engage breach counsel.
- [ ] Preserve logs beyond normal retention.
- [ ] Identify affected PHI: data elements, approximate individual count, encryption status.
- [ ] Confirm or rule out safe-harbor (FIPS-validated encryption at time of incident).

Decide (24-72 hours)

- [ ] Complete four-factor risk assessment under 164.402.
- [ ] Document breach-or-not determination with rationale.
- [ ] If breach: identify all notification obligations (individuals, OCR, media, state AGs, Business Associates affected).
- [ ] Draft notification letter templates (clinical, legal, communications review).
- [ ] Prepare OCR portal submission package.
- [ ] Engage credit monitoring vendor if warranted.

Notify (within 60 days of discovery)

- [ ] Individual notifications mailed (or emailed where permitted).
- [ ] OCR submission completed (500+ immediately; under 500 at year end).
- [ ] Media statement issued if 500+ in a single state/jurisdiction.
- [ ] State AG notifications completed per state-specific requirements.
- [ ] Affected Business Associates notified.

Close (post-incident)

- [ ] Root cause analysis written up and filed.
- [ ] Risk analysis updated to reflect the incident.
- [ ] Risk management plan updated with new or changed mitigations.
- [ ] Workforce retraining conducted on the root-cause pattern.
- [ ] Tabletop exercise scheduled within 6 months.

Chapter 6 · HITECH & the 2024 HIPAA Security Rule NPRM

6.1 HITECH in one page

The Health Information Technology for Economic and Clinical Health Act (HITECH), enacted in 2009 as part of the American Recovery and Reinvestment Act, significantly strengthened HIPAA:

- **Breach Notification Rule** — formalized notification obligations at 164.400-414.
- **Business Associate direct liability** — BAs now directly liable to HHS for Security Rule compliance and certain Privacy Rule provisions, not just contractually to Covered Entities.
- **Tiered civil money penalties** — 164.404(f), adjusted annually for inflation. 2024 caps (adjusted by HHS): approximately $137 to $2,067,813 per violation depending on culpability tier, with an annual cap of approximately $2,067,813 per identical provision.
- **Right of electronic access** — strengthened right of individuals to receive PHI in electronic form.
- **Expanded enforcement by state attorneys general** — state AGs may bring HIPAA civil actions in federal court on behalf of residents.
- **Accounting of EHR disclosures** — statutorily expanded (implementation has been incremental).

6.2 The 2024 HIPAA Security Rule NPRM

On January 6, 2025, HHS published a Notice of Proposed Rulemaking (NPRM) modifying the HIPAA Security Rule — the first substantive rewrite since 2013. Comments closed March 7, 2025. A final rule is pending.

Note: NPRM proposals may change in the final rule. Treat the list below as a preview of the regulatory direction, not current binding law.

Key proposed changes

- **Eliminate the Required/Addressable distinction.** All implementation specifications would become required. The "addressable" escape valve goes away.
- **Multi-factor authentication mandate.** MFA explicitly required for all access to ePHI.
- **Encryption of ePHI at rest and in transit.** Required by default, with narrow exceptions.
- **Annual compliance audits.** Formal annual compliance audits against the Security Rule.
- **Annual technical testing.** Vulnerability scans every six months; penetration testing annually.
- **Asset inventory and network map.** Formal requirement for up-to-date ePHI asset inventory and network diagram.

- **Written technology policies.** Formal written procedures for technology deployment and configuration management.
- **Incident response plan documentation.** Written, tested incident response and contingency plans; incident response testing on a defined cadence.
- **Sanction policy with examples.** Documented sanction policy with specific example scenarios.
- **Patch management cadence.** Critical patches within specified windows.

> **How to prepare.** Even before the final rule lands, most of the NPRM proposals reflect existing industry best practice. Practices that implement MFA, encryption by default, annual penetration testing, and a documented incident response plan now will have minimal gap remediation when the rule is finalized.

6.3 Your 2026 preparation roadmap

This quarter

- [ ] Complete or refresh your risk analysis under NIST SP 800-66r2.
- [ ] Enforce MFA on every system that touches ePHI.
- [ ] Verify full-disk encryption on every laptop, mobile device, and backup drive.
- [ ] Update Notice of Privacy Practices for the 2024 reproductive health final rule (deadline Feb 16, 2026).
- [ ] Inventory all Business Associates and confirm current signed BAAs.

Next quarter

- [ ] Schedule annual penetration test and quarterly vulnerability scans.
- [ ] Document and test the incident response plan via tabletop exercise.
- [ ] Rewrite the Security Management Process policy to reflect MFA and encryption-by-default as policy, not exception.
- [ ] Implement documented monthly log review with named reviewer.

Next six months

- [ ] Formalize vendor due-diligence process with annual SOC 2 reviews.
- [ ] Move from "addressable" language in policies to "required" language everywhere.
- [ ] Write a network diagram and ePHI data-flow diagram if you do not have one.
- [ ] Conduct refresher training for all workforce, including 2024 Privacy Rule updates.

6.4 Common pitfalls to avoid

- **Treating HIPAA as a one-time project.** It is a program.
- **Documenting policies you do not follow.** Worse than no policy at all — it is evidence of willful neglect.
- **Outsourcing compliance entirely.** Your IT vendor can implement controls; they cannot be your Security Official. You are responsible.
- **Trusting vendor marketing over vendor contracts.** "HIPAA-compliant" on a vendor website means nothing without a signed BAA and evidence of safeguards.
- **Ignoring state law.** Several states (California, Texas, New York, Washington) have health-privacy laws that overlap and sometimes exceed HIPAA.

Source: HITECH Act (PL 111-5); 45 CFR Part 160, 164; HHS 2024 HIPAA Security Rule NPRM; HHS OCR Enforcement Highlights.

About Petronella Technology Group

Petronella Technology Group is a Raleigh, North Carolina based IT and cybersecurity firm founded in 2002. We specialize in HIPAA compliance, CMMC 2.0 readiness, managed IT services, and cybersecurity for regulated industries — healthcare, defense contractors, legal, and financial services.

Credentials

- **Founder & CEO Craig Petronella** — CMMC Registered Practitioner (CMMC-RP), CCNA, CWNE, DFE #604180. Author of an Amazon-published HIPAA compliance book and additional books on cybersecurity and CMMC.
- **Entire technical team CMMC-RP certified.**
- **Firm accredited by the Professional Process Service Board (PPSB).**
- **Better Business Bureau A+ rating since 2003.**
- **Registered with the Cyber AB as a Registered Practitioner Organization (RPO)** for CMMC work.

What we do for medical practices

- HIPAA Security Rule risk analysis aligned with NIST SP 800-66r2.
- Risk management plan development and ongoing program management.
- Privacy Rule policy development and staff training.
- Business Associate Agreement review and vendor due diligence.
- Breach response and forensic investigation (via partner forensic providers when chain-of-custody is required).
- Managed IT services tuned for HIPAA: MFA, endpoint encryption, email encryption, EHR security, 24x7 monitoring, backup and disaster recovery.
- Penetration testing and vulnerability management.
- Employee security awareness training including HIPAA-specific content.

What we do not do

We are not a HIPAA auditor and do not issue HIPAA certifications (no such certification exists under U.S. law). We do not practice law. For binding legal interpretation on HIPAA, state breach notification, or contract disputes, we refer clients to healthcare counsel — and collaborate with your counsel when needed.

> **Our philosophy.** Compliance is a byproduct of good security and good operational discipline. We build the security program first; the compliance documentation follows. That is why our clients tend to

> do well when an OCR letter arrives: the operations, the policies, and the evidence all tell the same story.

NEXT STEP

Ready for a HIPAA Readiness Review?

We will review your current risk analysis, your Business Associate Agreements, your Notice of Privacy Practices, and your technical safeguards — and give you a written gap list with concrete, prioritized actions.

No pressure, no obligation. If we are a fit, we will tell you. If we are not, we will tell you who is.

Schedule a HIPAA Consultation

CALL

(919) 348-4912

Monday-Friday, 8am-6pm ET

WEB

petronellatech.com/contact-us

Contact form, 24-hour response

VISIT

5540 Centerview Dr

Raleigh, NC 27606