cycore

FREE DOWNLOAD

2026 EDITION

HIPAA

# HIPAA Compliance Checklist

Cycore's 70-item HIPAA self-assessment. Settle whether HIPAA applies to you first, then score your safeguards out of 140 and take the gaps to counsel.

PREPARED BY

Cycore

ONLINE

cycoresecure.com

Cycore built this 70-item checklist for teams that need to know where they stand on HIPAA. It starts with the question that decides everything else: whether you're a covered entity or a business associate. If you're neither, the HIPAA Rules don't apply to you, however much health data you handle. If you're one of the two, score the nine sections from 0 to 140 and put a name next to every gap. Then take the list and its open questions to counsel or whoever advises you on privacy and security.

## Start here: are you a covered entity or a business associate?

The HIPAA Rules apply to two kinds of organization, and the definitions sit in 45 CFR 160.103.

- A **covered entity** is a health plan, a health care clearinghouse, or a health care provider that sends health information electronically in a transaction HHS has set a standard for, such as a claim.
- A **business associate** is a person or company that creates, receives, maintains, or transmits protected health information (PHI) on a covered entity's behalf, or provides a service to a covered entity that involves PHI. A subcontractor that does the same for a business associate is a business associate too.

Handling health-related data, by itself, doesn't make you either one. The test is your role: what you are, and whose behalf you act on. HHS's own page says an organization that meets neither definition doesn't have to comply with the HIPAA Rules. Read the HHS pages on covered entities and business associates before you decide, and write the decision down with the reasoning.

Your answer sets how to read the rest:

- **Covered entity.** Work the whole list. The Privacy, Security, and Breach Notification Rules all apply to you.
- **Business associate.** The Security Rule and the Breach Notification Rule apply to you directly. Beyond the ten things HHS lists below, Privacy Rule duties

reach you only through your business associate agreement (BAA), so read the Privacy Rule section against that contract. HHS's fact sheet on the direct liability of business associates lists what you're directly liable for:

- Give HHS your records and compliance reports, cooperate with its complaint investigations and compliance reviews, and let it see information, PHI included, that bears on your compliance.
- Don't retaliate against anyone for filing a HIPAA complaint, taking part in an investigation or enforcement process, or opposing a practice the HIPAA Rules make unlawful.
- Comply with the Security Rule.
- Notify the covered entity, or the business associate you work for, of a breach.
- Use and disclose PHI only as your BAA permits or the law requires.
- Hand over an electronic copy of PHI for an individual's access request, to the covered entity, the individual, or the person the individual names, whichever your BAA specifies.
- Limit PHI to the minimum necessary for the use, disclosure, or request.
- Give an accounting of disclosures in certain circumstances.
- Sign BAAs, with the required terms, with subcontractors that create or receive PHI for you.
- Take reasonable steps when a subcontractor materially breaches its BAA.

- **Neither.** The HIPAA Rules don't apply to you. Other laws might, including state breach and privacy laws and the FTC's breach rule for vendors of personal health records, so the list still works as a security baseline.
- **Not sure.** Settle it before you treat anything below as a legal obligation. Ask counsel or a qualified privacy and security adviser to make the call. Until then, treat every item below as a security practice to weigh.

#### What enforcement looks like

HHS civil money penalties depend on the violation date, the organization's knowledge and culpability, and whether willful neglect was corrected. Amounts

are adjusted for inflation. Confirm current figures in 45 CFR 102.3 and current HHS enforcement materials. Some violations may be referred to the Department of Justice for criminal enforcement.

## How to use this checklist

Score every item 0, 1, or 2: 0 for not in place, 1 for partial (started, or running with no documentation), and 2 for in place and documented. Add up each section, then total the nine subtotals. 70 items at 2 points each gives a maximum of 140. The total is a Cycore planning number. It isn't an HHS score, a legal conclusion, or evidence that you comply, and there are no bands. Use it to see which sections need the work.

Every item carries one of four labels, so you can tell the law from our advice:

- **HIPAA required.** A standard or a required implementation specification in the HIPAA Rules, with the paragraph cited.
- **HIPAA addressable.** An addressable implementation specification in the Security Rule. Addressable doesn't mean optional. You have to assess whether the measure is reasonable and appropriate in your environment, then put it in place, put an equivalent measure in place, or document why neither is warranted, and keep that decision in writing.
- **Cycore recommended practice.** Something we advise that the rules don't spell out.
- **Scope-dependent.** Whether it binds you depends on a fact: usually whether you're a covered entity or a business associate, what your BAA says, or what your risk analysis found.

The required and addressable split comes from the Security Rule itself (45 CFR 164.306(d)). HHS explains it in its Security Rule summary and its FAQ on addressable and required specifications. The Security Rule is also technology neutral: it says what to protect against, and you choose the measures through your risk analysis (164.306(b)). So where this list names a technology, that's our recommendation as of September 2026, and the label says so.

HHS published a proposed rule to amend the Security Rule on January 6, 2025 (90 FR 898); as of September 23, 2026, no final rule has been published, the current rule applies, and HHS's regulatory agenda lists final action as a long-term action with a July 2027 date (RIN 0945-AA22).

## Section 1: Foundational Decisions

Decide these before you buy tools or write policies. Everything below depends on knowing what PHI you hold, where it goes, and who owns the program. If you already run a GRC platform, use this before you map to its HIPAA framework: it settles whether HIPAA applies to you and marks which items are the law and which are our advice.

0 1 2 **PHI scope definition.** List every type of PHI you create, receive, maintain, or transmit, and check it against the 18 identifiers in the Privacy Rule's Safe Harbor list (164.514(b)(2)). This inventory is the first input to the risk analysis the Security Rule requires. Cycore recommended practice

0 1 2 **Data flow mapping.** Draw where PHI enters, where it's stored, where it moves, and where it leaves, including integrations, logs, backups, and analytics pipelines. In our experience, the surprises in a risk analysis come from copies of PHI nobody knew about. Cycore recommended practice

0 1 2 **Covered entity vs. business associate determination.** Write down which one you are, or that you're neither, with the reasoning and who signed off. The definitions are in 45 CFR 160.103, and the section above walks through them. If you're a business associate, list your covered entity customers. Cycore recommended practice

0 1 2 **Compliance officer designation.** One person owns the program, with written authority and a reporting line. The rules name two roles you can fold into that job: a security official (164.308(a)(2)) and, for covered entities, a privacy official (164.530(a)(1)). Cycore recommended practice

0 1 2 **Risk analysis timeline established.** The risk analysis is a required implementation specification: an accurate and thorough assessment of the risks to the confidentiality, integrity, and availability of the electronic PHI you hold (164.308(a)(1)(ii)(A)). Put the first one on the calendar with a method, a scope, and a finish date, and plan the repeats. The rule expects you to keep your security measures current as things change (164.306(e)). HIPAA required

0 1 2 **Compliance budget allocated.** Money set aside for tools, training, outside assessments, and fixing what the risk analysis finds. Without a remediation budget, a risk analysis gives you a list of known problems. Cycore recommended practice

**Your subtotal**: ___ of 12

## Section 2: Administrative Safeguards

The administrative safeguards are the people-and-process part of the Security Rule, and they bind covered entities and business associates alike. Paragraph references are to 45 CFR 164.308 unless another section is named.

0 1 2 **Security officer designation.** Name the security official responsible for developing and implementing your security policies and procedures. One person, by name, in writing (164.308(a)(2)). HIPAA required

0 1 2 **Workforce security procedures.** Policies and procedures so that everyone on your workforce has the access to electronic PHI their job needs and nobody else can get it (164.308(a)(3)(i)). The three specifications underneath (authorization and supervision, clearance, and termination) are addressable, so document how you assessed each one. HIPAA required

0 1 2 **Workforce training program.** A security awareness and training program for the whole workforce, management included (164.308(a)(5)(i)). Covered entities also train on their privacy policies (164.530(b)). Neither rule sets a calendar. We train at onboarding and repeat every year.

HIPAA required

---

0 1 2 **Security awareness program.** The four addressable pieces under the training standard: periodic security reminders, protection from malicious software, log-in monitoring, and password management (164.308(a)(5)(ii)). Phishing simulations are our addition. They're the cheapest way we know to find out whether the training took. HIPAA addressable

---

0 1 2 **Access management procedures.** Written procedures for authorizing access to electronic PHI, and for granting, changing, and reviewing it (164.308(a)(4)). The standard is required; the access authorization and access establishment specifications under it are addressable. Role-based definitions make all of it easier to run and easier to prove.

HIPAA required

---

0 1 2 **Access termination procedures.** Procedures to end access to electronic PHI when someone leaves or changes role (164.308(a)(3)(ii)(C)), covering applications, VPN, email, and building access. The rule sets no clock. We revoke access the same day. HIPAA addressable

---

0 1 2 **Incident response procedures.** Policies and procedures for security incidents, with a required specification to identify and respond to them, limit the damage, and document what happened and how it ended (164.308(a)(6)). The rule doesn't say to test the plan. We test ours at least once a year so the people named in it know their parts. HIPAA required

---

0 1 2 **Contingency plan.** A data backup plan, a disaster recovery plan, and an emergency mode operation plan, all three required (164.308(a)(7)(ii)(A) to (C)). Testing and revision, and the analysis of which applications and data matter most, are addressable. Run a restore before you need one. HIPAA required

---

0 1 2 **Evaluation procedures.** A written procedure for the periodic technical and non-technical evaluation the Security Rule requires (164.308(a)(8)): who runs it, how often, and what triggers one off-cycle. A migration, an acquisition, or a new product line each count as a trigger. This item scores the procedure. The self-assessment item in Section 9 scores the last run. HIPAA required

---

0 1 2 **Business Associate Agreement (BAA) management process.** A covered entity may let a business associate handle electronic PHI only with satisfactory written assurances, in a BAA, that it will safeguard the information (164.308(b)(1); 164.502(e)). A process to identify business associates, sign before any PHI moves, and track the status of every BAA is how you show that happened. HIPAA required

**Your subtotal**: ___ of 20

## Section 3: Physical Safeguards

The physical safeguards apply if your team has laptops, your office has a door, or anyone works from home. Cloud hosting shifts the data center part to your provider under its BAA. Your laptops, offices, and home setups stay yours. References are to 45 CFR 164.310.

0 1 2 **Facility access controls.** Policies and procedures that limit physical access to your electronic information systems and the places that house them, while letting authorized people in (164.310(a)(1)). The four specifications underneath (contingency operations, a facility security plan, access control and validation including visitor control, and maintenance records) are addressable. HIPAA required

0 1 2 **Workstation use policies.** Policies that say what a workstation that can reach electronic PHI is for, how it's used, and what its surroundings should look like (164.310(b)). A laptop in a coffee shop is a workstation. HIPAA required

0 1 2 **Workstation security.** Physical safeguards on every workstation that can reach electronic PHI, so only authorized users get at it (164.310(c)). Screen locks, privacy screens where people work in public, and screens turned away from walk-up traffic are our examples. The rule leaves the measures to you. HIPAA required

0 1 2 **Device and media controls: disposal.** Policies and procedures for the final disposition of electronic PHI and the hardware or media it lives on (164.310(d)(2)(i)). Certificates of destruction from your disposal vendor are our practice for proving it. HIPAA required

0 1 2 **Device and media controls: re-use.** Procedures to remove electronic PHI from media before the media is reused (164.310(d)(2)(ii)). That includes the laptop you hand to the next hire. HIPAA required

0 1 2 **Device and media controls: accountability.** A record of where hardware and electronic media move and who was responsible (164.310(d)(2)(iii)). Addressable, so if your asset inventory already tracks movement, document that it satisfies this. HIPAA addressable

0 1 2 **Remote work safeguards.** If anyone touches PHI from home or on the road, the workstation standards above follow them there. Write down what you expect of a home setup: network, screen, printouts, and who else can see the screen. Whether this item applies at all depends on how your people work. Scope-dependent

**Your subtotal**: ___ of 14

## Section 4: Technical Safeguards

The technical safeguards are the controls engineering teams usually own. Having a control is different from having it scoped, configured, and documented, which is what the scoring asks. References are to 45 CFR 164.312 unless another section is named.

0 1 2 **Unique user identification.** A unique name or number for every user, so activity traces to one person (164.312(a)(2)(i)). No shared accounts, no generic logins. HIPAA required

0 1 2 **Emergency access procedures.** Procedures for getting to electronic PHI during an emergency (164.312(a)(2)(ii)): who can authorize it, under what conditions, and how it's logged. HIPAA required

0 1 2 **Automatic logoff.** Sessions on systems that reach electronic PHI end after a set period of inactivity (164.312(a)(2)(iii)). Addressable: pick the period through your risk analysis and write the reasoning down. HIPAA addressable

0 1 2 **Encryption at rest.** A mechanism to encrypt and decrypt electronic PHI (164.312(a)(2)(iv)). Addressable, and the rule names no algorithm. As of September 2026 we recommend AES-256 or an equivalent validated standard for every store that holds PHI, backups included. You choose and document the standard through your risk analysis. HIPAA addressable

0 1 2 **Encryption in transit.** A mechanism to encrypt electronic PHI in transit whenever appropriate (164.312(e)(2)(ii)). Addressable, and again the rule names no protocol. As of September 2026 we recommend TLS 1.2 or higher on every connection that carries PHI, internal traffic included. HIPAA addressable

0 1 2 **Audit controls.** Hardware, software, or procedural mechanisms that record and examine activity in systems that contain or use electronic PHI (164.312(b)). HIPAA required

0 1 2 **Audit log review process.** Procedures to regularly review records of system activity, such as audit logs, access reports, and incident tracking reports (164.308(a)(1)(ii)(D)). Collecting logs nobody reads satisfies the item above and fails this one. Set a schedule and define what triggers an investigation. HIPAA required

0 1 2 **Integrity controls.** Policies and procedures that protect electronic PHI from improper alteration or destruction (164.312(c)(1)). The mechanism to confirm PHI hasn't been altered, such as checksums or versioning, is addressable (164.312(c)(2)). HIPAA required

0 1 2 **Authentication controls.** Procedures to verify that a person or system asking for electronic PHI is who it claims to be (164.312(d)). The current rule doesn't name multi-factor authentication. We recommend it on every remote and administrative path. HIPAA required

0 1 2 **Transmission security.** Technical measures that guard against unauthorized access to electronic PHI moving over a network (164.312(e)(1)). Integrity controls and encryption underneath it are both addressable. HIPAA required

**Your subtotal**: ___ of 20

## Section 5: Privacy Rule Requirements

The Privacy Rule governs how PHI is used and disclosed, and most of its duties sit with covered entities. If you're a business associate, HHS's direct liability fact sheet names the provisions that bind you directly, minimum necessary among them, and your BAA says which of the rest you carry out for your customers (164.504(e)(2)(ii)(H)). Score each item against your role.

0 1 2 **Notice of Privacy Practices (NPP).** Covered entities give individuals a notice of how PHI is used and disclosed, the individual's rights, and the entity's legal duties (45 CFR 164.520). A business associate doesn't issue one. Scope-dependent

0 1 2 **Minimum necessary standard.** When you use, disclose, or request PHI, limit it to the minimum needed for the purpose (45 CFR 164.502(b)). This one binds covered entities and business associates directly, with exceptions such as disclosures to a provider for treatment. Apply it to internal access, outside disclosures, and your own requests. HIPAA required

0 1 2 **Right of access.** Covered entities act on an individual's request for their PHI within 30 days, in the form and format asked for if it's readily producible, for no more than a reasonable, cost-based fee (45 CFR 164.524). A business associate makes PHI available for this under its BAA (164.504(e)(2)(ii)(E)). Scope-dependent

0 1 2 **Right to amendment.** Covered entities act on a request to amend PHI within 60 days, with a documented process for granting or denying it (45 CFR 164.526). A business associate supports amendments under its BAA (164.504(e)(2)(ii)(F)). Scope-dependent

0 1 2 **Accounting of disclosures.** Covered entities can give an individual an accounting of certain disclosures of their PHI from the previous six years (45 CFR 164.528). A business associate keeps the records that feed that accounting (164.504(e)(2)(ii)(G)). Scope-dependent

0 1 2 **Authorization forms.** Any use or disclosure the Privacy Rule doesn't otherwise permit needs a valid authorization from the individual, with the core elements the rule lists (45 CFR 164.508). A covered entity duty. A business associate's permitted uses are whatever its BAA allows (164.502(a)(3)). Scope-dependent

0 1 2 **De-identification procedures.** Data counts as de-identified only under the expert determination method or the Safe Harbor method, which removes 18 listed identifiers (45 CFR 164.514(a) and (b)). Applies only if you de-identify PHI for analytics, research, or product work, and a business associate may only do it if its BAA permits (164.502(a)(3)). Scope-dependent

0 1 2 **Marketing and fundraising restrictions.** Covered entities need an authorization to use PHI for marketing, with narrow exceptions (45 CFR 164.508(a)(3)), and every fundraising communication has to offer a clear way to opt out (45 CFR 164.514(f)). Applies only if you do either. Scope-dependent

**Your subtotal**: ___ of 16

## Section 6: Business Associate Management

If a vendor holds your PHI, their breach is one you have to report. Sign the BAA first, then check how they actually run security.

0 1 2 **BAA inventory.** One current list of every business associate with access to PHI: what PHI, what service, when the BAA was signed, and who owns the relationship. Cycore recommended practice

0 1 2 **BAA template with required provisions.** Your BAA carries every provision 45 CFR 164.504(e)(2) requires. That means permitted and required uses and disclosures, safeguards, reporting of impermissible uses and breaches, subcontractor flow-down, support for individual rights, the Privacy Rule's requirements for any covered entity duty the business associate carries out, access for HHS to the business associate's books and records, return or destruction of PHI at the end, and the covered entity's right to terminate for a material breach. Add the Security Rule terms in 45 CFR 164.314(a). HIPAA required

0 1 2 **BAA execution before PHI sharing.** No PHI goes to a business associate, or from a business associate to a subcontractor, until the BAA is signed. A covered entity may only disclose PHI to a business associate with those written assurances in place (45 CFR 164.502(e); 164.308(b)), and a business associate owes the same to its subcontractors. HIPAA required

0 1 2 **Subcontractor chain tracking.** A business associate must bind each subcontractor that touches PHI to the same restrictions, in writing, before any PHI flows (164.502(e)(1)(ii); 164.504(e)(2)(ii)(D); 164.314(a)(2)(i)(B)). A covered entity isn't party to those downstream contracts, so ask your business associates who their subcontractors are and how they're bound. Which side of that you're on decides what this item asks of you. Scope-dependent

0 1 2 **Breach notification requirements in BAAs.** The BAA requires the business associate to report uses and disclosures the contract doesn't permit, including breaches of unsecured PHI (164.504(e)(2)(ii)(C)), and security incidents (164.314(a)(2)(i)(C)). The rule's outer limit for a business associate to notify the covered entity is 60 calendar days from discovery (45 CFR 164.410). Many contracts set a shorter clock; the 60 days is the ceiling, and you can agree to less. HIPAA required

0 1 2 **Periodic BAA review.** Reread each BAA when the service changes, when the rules change, and at renewal. The service the BAA describes and the service you actually get drift apart over the years. Cycore recommended practice

0 1 2 **Business associate security assessment.** Look at a business associate's security posture before you sign and periodically after: their SOC 2 report, HITRUST certification, or a questionnaire, with the evidence kept. The rules require the contract. We check the vendor's security on top of it. Cycore recommended practice

**Your subtotal**: ___ of 14

## Section 7: Breach Notification Preparedness

The Breach Notification Rule sets who gets told, by when, and what they're told. Individual, media, and HHS notices are the covered entity's duties. A business associate's duty is to notify the covered entity, unless the BAA hands it more.

0 1 2 **Breach assessment process.** An impermissible use or disclosure of PHI is presumed to be a breach unless you can show a low probability that the PHI was compromised (45 CFR 164.402). The assessment uses at least four factors: the nature and extent of the PHI, who received it, whether it was actually acquired or viewed, and how far the risk has been mitigated. The burden of proof is yours, so document every assessment (45 CFR 164.414(b)). HIPAA required

0 1 2 **60-day notification timeline.** Notices go out without unreasonable delay and no later than 60 calendar days after discovery (45 CFR 164.404(b)), and a breach counts as discovered on the first day you knew, or would have known with reasonable diligence (164.404(a)(2)). The same 60-day outer limit applies to a business associate notifying the covered entity (45 CFR 164.410). HIPAA required

0 1 2 **Individual notification procedures.** Covered entities notify affected individuals in writing by first-class mail, or by email if the person agreed to electronic notice (45 CFR 164.404(c) and (d)). The notice covers what happened, what PHI was involved, what the person should do, what you're doing about it, and how to reach you. A business associate notifies the covered entity (45 CFR 164.410) unless the BAA delegates individual notice to it. Scope-dependent

0 1 2 **HHS reporting procedures.** Covered entities report breaches to HHS (45 CFR 164.408). For 500 or more individuals, report at the same time as individual notice. For fewer than 500, log it and report within 60 days after the end of the calendar year in which you discovered it. Find the HHS breach portal now and bookmark it. Scope-dependent

0 1 2 **State notification requirements.** State breach laws can add recipients, shorter deadlines, and content requirements on top of HIPAA. List every state where you have affected individuals and know each one's rule. This is state law, outside HIPAA, and it depends on where your people are. Scope-dependent

0 1 2 **Media notification triggers.** A breach involving more than 500 residents of one state or jurisdiction also requires notice to prominent media outlets serving that area, on the same 60-day clock (45 CFR 164.406). A covered entity duty. Keep a draft statement ready. Scope-dependent

0 1 2 **Breach response team identified.** Named people for each role, inside and outside the company, legal counsel included, with current contact details and the authority to act without waiting for a meeting. Cycore recommended practice

0 1 2 **Breach response drill completed.** At least one tabletop exercise that walks a realistic breach through assessment, notification, and the regulators, with the gaps written down. Cycore recommended practice

**Your subtotal**: ___ of 16

## Section 8: Documentation and Training

The Security Rule requires written policies and written records of what it makes you do (45 CFR 164.316), and the Privacy Rule requires the same of covered entities (45 CFR 164.530(j)). References are to those two sections unless another is named.

0 1 2 **Policy documentation.** Every policy and procedure the rules require exists in writing, electronic or paper, and is available to the people who have to follow it (164.316(a) and (b); 164.530(i) and (j) for covered entities). Management approval, with a date and a name, is our practice for showing the policy is real. HIPAA required

0 1 2 **Policies reflect actual practice.** The policy describes what your team actually does, in your stack, with your workflows. If you started from a template, rewrite it until it matches. Cycore recommended practice

0 1 2 **Training records.** Covered entities document that privacy training happened (164.530(b)(2)(ii)). The Security Rule requires a training program and a written record of it (164.308(a)(5); 164.316(b)(1)), so keep a record per person: date, content, and who attended. HIPAA required

0 1 2 **Training content updates.** Update the material when the rules change, when your environment changes, and when incidents show a gap. The one hard trigger in the rules is for covered entities: retrain the people affected by a material change in your privacy policies (164.530(b)(2)(i)(C)). Cycore recommended practice

0 1 2 **Risk assessment documentation.** Each risk analysis is written up: method, scope, threats and vulnerabilities found, risk ratings, and the remediation decided (164.308(a)(1)(ii)(A); 164.316(b)(1)(ii)). The rule requires the record, so an undocumented analysis doesn't satisfy it. HIPAA required

0 1 2 **Remediation tracking.** The risk management specification requires security measures sufficient to reduce the risks you found to a reasonable and appropriate level (164.308(a)(1)(ii)(B)). Track each finding to closure with an owner, a date, and evidence of the fix. That's how you show the measures happened. HIPAA required

0 1 2 **Six-year retention compliance.** Keep required documentation for six years from when it was created or when it was last in effect, whichever is later (164.316(b)(2)(i); 164.530(j)(2) for the Privacy Rule). Old policy versions and old risk analyses count. HIPAA required

0 1 2 **Version control for policies.** Version numbers, effective dates, and approval records on every policy. The rule requires you to review documentation periodically and update it as things change (164.316(b)(2)(iii)). Versioning is how you prove which one was in force when. Cycore recommended practice

**Your subtotal**: ___ of 16

## Section 9: Audit Readiness

An OCR investigation can begin with a complaint or a breach report. Expect a request for documents early.

0 1 2 **OCR audit protocol familiarity.** Your compliance owner knows the areas OCR examines and the evidence it asks for, and keeps a copy of OCR's audit protocol within reach. Read it before an investigator quotes it to you. Cycore recommended practice

0 1 2 **Evidence organization.** Compliance records live in one place with an index, so you can produce a policy, a training record, or a risk analysis within hours. Scattered drives, chat threads, and one person's laptop don't count as a system. Cycore recommended practice

0 1 2 **Self-assessment completed.** You've run the evaluation from Section 2 within the last year and can hand over the write-up (164.308(a)(8), with the record kept under 164.316(b)(1)). The rule doesn't say how often. Yearly is our cadence, and we cover all three rules, Privacy and Breach Notification included, in the same pass. This checklist is one way to run it. HIPAA required

0 1 2 **Gap remediation plan.** Every gap from the self-assessment has an owner, a date, and a status, and the list gets reviewed on a schedule. Cycore recommended practice

0 1 2 **Third-party assessment.** An outside firm has checked your HIPAA posture at least once. No rule requires it. We recommend it because your own team wrote the policies it would be checking. Cycore recommended practice

0 1 2 **Audit trail integrity.** Audit logs and compliance records are protected from tampering, with restricted write access and a retention period set by policy. The six-year rule in 164.316(b)(2)(i) covers policies, procedures, and records of required actions and assessments. It doesn't name logs, so the log period is yours to set, and we'd match it to six years. Cycore recommended practice

**Your subtotal**: ___ of 12

## Your score

| SECTION | ITEMS | MAXIMUM | YOUR SUBTOTAL |
|---|---|---|---|
| 1. Foundational Decisions | 6 | 12 | |
| 2. Administrative Safeguards | 10 | 20 | |
| 3. Physical Safeguards | 7 | 14 | |
| 4. Technical Safeguards | 10 | 20 | |
| 5. Privacy Rule Requirements | 8 | 16 | |
| 6. Business Associate Management | 7 | 14 | |
| 7. Breach Notification Preparedness | 8 | 16 | |
| 8. Documentation and Training | 8 | 16 | |
| 9. Audit Readiness | 6 | 12 | |
| Total | 70 | 140 | |

Whatever the number, the next moves are the same. Give every 0 and 1 an owner and a date. Write down every item where you weren't sure the rule applies to you, and take that list to counsel or your privacy and security adviser. If you're not sure where to begin, the risk analysis is where we'd start, because it sets the order for everything else.

## More Cycore guides and checklists

- SOC 2 Readiness Checklist
- ISO 27001 Gap Assessment
- HITRUST Readiness Guide
- AI Governance Starter Kit

## Next step

**Talk to Cycore about your HIPAA program**

This Cycore self-assessment is educational and does not provide legal advice or establish HIPAA compliance. The score is a Cycore planning indicator. It is not an HHS score, a legal conclusion, or evidence of compliance. Which items bind you depends on whether you are a covered entity or a business associate, on your business associate agreements, and on your own risk analysis. Confirm your obligations with qualified counsel.