BROTHERLY TECHNOLOGY

HIPAA CHECKLIST

HIPAA IT Compliance Checklist

The technical safeguards auditors ask about, translated out of regulation-speak. Built for practices without a compliance officer on staff.

01	**Required vs addressable safeguards, plainly explained**
02	**The documentation gaps that trigger most findings**
03	**A vendor/BAA tracker you can start using immediately**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

BROTHERLY TECHNOLOGY

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] A current security risk analysis covers systems, people, vendors, and electronic protected health information.	[ ] Yes [ ] Partial [ ] No
[ ] A risk management plan assigns owners and dates to identified risks.	[ ] Yes [ ] Partial [ ] No
[ ] Every workforce member has a unique user ID and role-appropriate access.	[ ] Yes [ ] Partial [ ] No
[ ] MFA is used for remote, cloud, email, and privileged access wherever supported.	[ ] Yes [ ] Partial [ ] No
[ ] Emergency access procedures are documented and tested.	[ ] Yes [ ] Partial [ ] No
[ ] Automatic logoff or an equivalent risk-based control is documented.	[ ] Yes [ ] Partial [ ] No
[ ] Audit logs are enabled, protected, reviewed, and retained according to policy.	[ ] Yes [ ] Partial [ ] No
[ ] Integrity controls help detect unauthorized alteration or destruction of ePHI.	[ ] Yes [ ] Partial [ ] No
[ ] Transmission security protects ePHI across external and untrusted networks.	[ ] Yes [ ] Partial [ ] No
[ ] Backups and recovery are tested against defined RTO and RPO targets.	[ ] Yes [ ] Partial [ ] No
[ ] Business associate agreements are tracked before vendors handle ePHI.	[ ] Yes [ ] Partial [ ] No
[ ] Policies, training, incidents, sanctions, evaluations, and decisions are retained as required.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

SAFEGUARD MAP

Required and addressable do not mean mandatory and optional

Required specifications must be implemented. For an addressable specification, assess whether it is reasonable and appropriate, then implement it or document why an equivalent measure or non-implementation is appropriate.

Specification	Status	Evidence to keep
Unique user identification	Required	User list, identity standard, provisioning records
Emergency access procedure	Required	Runbook, emergency accounts, test record
Automatic logoff	Addressable	Risk decision, timeout settings, compensating controls
Encryption / decryption	Addressable	Risk decision, device and storage encryption evidence
Audit controls	Required standard	Log sources, review record, alert and retention settings
Integrity mechanism	Addressable	Risk decision, application or file integrity controls
Transmission security	Addressable	Risk decision, TLS, VPN, secure messaging controls

Addressable is a documented risk decision. A blank policy, inherited vendor setting, or 'not applicable' with no analysis is not a defensible decision.

EVIDENCE AND VENDORS

Close the documentation gaps that create findings

Audits and investigations look for proof that the program operates. Keep versioned records, approvals, dates, owners, and corrective actions.

1	Create an evidence index for risk analysis, risk plan, policies, training, access reviews, incidents, backups, and evaluations.
2	Record each addressable decision, the factors considered, the chosen control, the approver, and the review date.
3	Build a vendor tracker with service, data touched, owner, BAA status, security review, renewal, and termination date.
4	Review access and vendors after role changes, departures, system changes, and at a documented recurring interval.
5	Retain HIPAA-required documentation for six years from creation or last effective date, as applicable.

What to watch for

WATCH: A copied risk analysis does not identify the practice's actual systems or ePHI.

WATCH: A vendor handles ePHI before a BAA and security review are complete.

WATCH: Policies have no approval date, owner, version, or operating evidence.

WATCH: Backups exist, but no recovery test shows that patient care can resume.

WATCH: Shared accounts prevent attribution to an individual.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

_____

_____

_____

_____

_____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: HHS HIPAA Security Rule: hhs.gov/hipaa/for-professionals/security/ | 45 CFR 164.308, 164.312, and 164.316: ecfr.gov

This checklist is educational and is not legal advice or a certification of HIPAA compliance. HIPAA obligations depend on your role, systems, risks, contracts, and applicable law. Coordinate with qualified legal, privacy, compliance, and security professionals.