BROTHERLY TECHNOLOGY

HEALTHCARE IT CHECKLIST

The Healthcare IT Compliance Checklist

The technical controls that keep patient data defensible under audit, written for practices without a dedicated compliance team.

01	**Access control and audit logging requirements**
02	**Encryption standards for data at rest and in transit**
03	**Vendor and BAA documentation you must keep**

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 risk analysis maps ePHI across clinical, business, cloud, device, and vendor systems.	[ ] Yes [ ] Partial [ ] No
[ ] Unique identities, role-based access, MFA, emergency access, and timely offboarding are operating.	[ ] Yes [ ] Partial [ ] No
[ ] Privileged access is separated, limited, logged, and reviewed.	[ ] Yes [ ] Partial [ ] No
[ ] Audit logs cover relevant identity, EHR, email, endpoint, network, and cloud activity.	[ ] Yes [ ] Partial [ ] No
[ ] Log review and alert handling have owners, thresholds, retention, and evidence.	[ ] Yes [ ] Partial [ ] No
[ ] Encryption protects supported endpoints, portable media, backups, storage, and untrusted transmission.	[ ] Yes [ ] Partial [ ] No
[ ] Exceptions to encryption or access controls have a documented risk decision.	[ ] Yes [ ] Partial [ ] No
[ ] Backups include critical clinical and cloud data and have proven recovery.	[ ] Yes [ ] Partial [ ] No
[ ] Medical and IoT devices are inventoried, segmented, supported, and vendor access is controlled.	[ ] Yes [ ] Partial [ ] No
[ ] Vendors are classified, reviewed, contracted, and tracked with BAAs where required.	[ ] Yes [ ] Partial [ ] No
[ ] Incident and downtime plans protect patient care, communications, and evidence.	[ ] Yes [ ] Partial [ ] No
[ ] Policies, training, reviews, exercises, incidents, and corrective actions are retained.	[ ] 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.

ACCESS AND LOGGING

Make patient-data access attributable and reviewable

The goal is to know who accessed what, whether that access was appropriate, and what the organization did when a signal appeared.

Control	Operating standard	Evidence
Identity	Unique ID for each workforce member and approved service identity	User roster, provisioning, shared-account exceptions
Role access	Minimum access based on job function and care workflow	Role matrix, approval, recurring review
MFA	Remote, cloud, email, privileged, and other risk-based access	Coverage report and exception decisions
Emergency access	Break-glass path with monitoring and after-action review	Runbook, test, access log, review
Audit logging	Relevant events enabled, protected, retained, and time-synchronized	Source inventory, settings, sample records
Review	Alerts and recurring reviews with owned follow-up	Tickets, investigations, corrective actions

Audit logs that are enabled but never reviewed do not provide the same assurance as a documented detection and response process.

ENCRYPTION AND VENDORS

Document both the control and the decision

Use current, vendor-supported encryption for data at rest and in transit. Track keys, recovery, exceptions, and business associates as part of one evidence system.

1	Inventory endpoints, servers, databases, backups, portable media, email, messaging, file transfer, portals, and interfaces that handle ePHI.
2	Record encryption method, owner, key/recovery process, verification evidence, exception, and review date for each.
3	Build a vendor/BAA tracker with service, ePHI touched, owner, contract, BAA, security review, renewal, incident contact, and termination steps.
4	Reassess after migrations, new interfaces, device changes, mergers, incidents, or material vendor changes.
5	Test one vendor outage and one suspected data exposure; confirm alternate workflows and notification decision-making.

What to watch for

WATCH: A cloud service is assumed secure without confirming tenant settings and responsibility.

WATCH: Portable devices are encrypted, but recovery keys are unmanaged.

WATCH: A vendor has remote access with a shared or permanently enabled account.

WATCH: A BAA exists, but the vendor's service or subcontractors changed.

WATCH: Retention and audit evidence disappear when a subscription ends.

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/ | HHS guidance on risk analysis: hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/

This checklist is educational and is not legal advice or a certification of compliance. Healthcare obligations vary by entity, data, services, contracts, state, and federal law. Coordinate with qualified legal, privacy, compliance, clinical, and security professionals.