HIPAA IT Compliance Checklist for Medical Practices

From Galleon IT Solutions, healthcare-first managed IT for Dallas-Fort Worth and Houston. 2026 edition.

HIPAA does not tell you which products to buy. It tells you which safeguards you must have and be able to prove. This checklist translates the Security Rule into the concrete IT controls a practice, lab, or billing organization needs, organized the way an OCR investigator or a cyber insurer would review them.

How to use it: work through the eight sections in order. For each item, mark Done, Partial, or Missing, and note where the evidence lives. When you finish, the Missing and Partial items are your remediation plan, and the Done items with evidence are your audit file.

This checklist covers the Security Rule's technical and administrative safeguards as they apply to IT. It is not legal advice and does not replace a formal risk analysis, which HIPAA requires.

1. Risk analysis and governance

Control	Done	Partial	Missing	Evidence / notes
A written security risk analysis completed within the last 12 months, covering every system that creates, receives, stores, or transmits ePHI (EMR, PM, imaging, lab, email, file shares, backups, phones, tablets, cloud services).				
A remediation plan from that analysis with owners and dates, and evidence that items were closed.				
A named security officer and a named privacy officer.				
Written policies and procedures covering access, workstation use, device and media controls, incident response, contingency planning, and sanctions.				
A current inventory of hardware, software, and data locations, including personal devices used for work.				

Why it matters: OCR's most frequent finding is a missing or stale risk analysis. Insurers ask for it by name.

2. Access control and identity

Control	Done	Partial	Missing	Evidence / notes
Unique user IDs for every person; no shared logins on the EMR, workstations, or email.				
Multi-factor authentication on email, the EMR and PM, remote access, cloud file services, and administrative accounts.				
Role-based access: staff see only what their job requires, reviewed at least annually and on role change.				
Documented onboarding and same-day offboarding procedures with evidence (tickets or logs).				
Automatic screen lock and session timeouts on workstations and tablets; emergency access procedure documented.				
Privileged and administrator accounts separated from daily-use accounts.				

Why it matters: Business email compromise and stolen credentials are the leading breach vector; MFA is now table stakes for cyber insurance.

3. Endpoint, network, and email security

Control	Done	Partial	Missing	Evidence / notes
Managed endpoint detection and response (not just antivirus) on every workstation, laptop, and server; alerts monitored 24/7.				
Full-disk encryption on every laptop, tablet, and portable device; mobile device management with remote wipe.				
Supported operating systems and applications, patched on a schedule, including imaging and lab workstations certified by device vendors.				
Business-grade firewall with logging; network segmentation separating clinical systems, medical devices, guest Wi-Fi, and payment systems.				
Email security with impersonation and phishing protection, and encryption for messages containing PHI.				
Secure configuration standards for workstations and servers, and removal of local admin rights.				

Why it matters: Ransomware and phishing succeed through unpatched, unmanaged, unsegmented environments.

4. Audit logging and monitoring

Control	Done	Partial	Missing	Evidence / notes
Audit logging enabled on the EMR, PM, email, file servers, and firewalls; logs retained per policy.				
Periodic review of EMR access logs for inappropriate access, with the review documented.				
Alerting for failed logins, privilege changes, mass downloads, and after-hours access anomalies.				

Why it matters: HIPAA requires audit controls; the ability to show what happened is what separates a contained incident from a reportable breach.

5. Backup, contingency, and disaster recovery

Control	Done	Partial	Missing	Evidence / notes
Backups of the EMR or PM database, imaging, file shares, email, and cloud services (Microsoft 365 or Google Workspace), including vendor-hosted systems where you are responsible for exports.				
At least one backup copy isolated from the production network and from administrator credentials (immutable or offline).				
Documented recovery time and recovery point objectives, and restore tests performed and recorded on a schedule.				
A written disaster recovery plan and an emergency mode operation (downtime) plan staff can follow, tested at least annually.				
For Gulf Coast practices: a plan for extended power, internet, and access loss during hurricane season.				

Why it matters: The Security Rule's contingency plan standard is explicit, and untested backups are the difference between an afternoon and a month.

6. Vendors and business associate agreements

Control	Done	Partial	Missing	Evidence / notes
An inventory of every vendor that creates, receives, stores, or transmits ePHI: EMR, hosting, billing and RCM, clearinghouse, transcription, IT provider, cloud email and file services, phone and fax, shredding, and marketing or patient-communication tools.				
A signed business associate agreement with each, on file and current.				
Evidence of vendor security review for critical vendors (SOC 2, HITRUST, or a completed questionnaire).				
Contract terms addressing breach notification timelines and data return or destruction.				

Why it matters: Missing BAAs are the second most common OCR finding, and vendor breaches are now the largest source of exposed records.

7. Workforce training and physical safeguards

Control	Done	Partial	Missing	Evidence / notes
Security awareness training for all staff at hire and at least annually, with completion records; periodic phishing simulations.				
Documented sanctions policy and evidence it is applied.				
Physical controls: locked server closets or racks, badge or key logs, screens positioned away from public view, clean-desk practices for PHI.				
Media disposal procedures with certificates of destruction for drives, devices, and paper.				

Why it matters: People and physical access are still where many incidents start, and training records are requested in nearly every audit.

8. Incident response and breach readiness

Control	Done	Partial	Missing	Evidence / notes
A written incident response plan with roles, contact lists (counsel, cyber insurer, IT provider, forensics), and decision steps.				
A breach risk assessment procedure aligned to the HIPAA Breach Notification Rule and Texas notification law, with timelines.				
Cyber insurance policy on file, with the carrier's reporting requirements known and the required controls verified.				
Tabletop exercise conducted at least annually, documented.				

Why it matters: The first 72 hours determine cost and notification outcomes; a plan that exists only in someone's head does not count.

What to do with your results

If you have gaps in sections 1, 2, 5, or 6, address those first: they are the items OCR cites most and the items insurers decline over. Sections 3 and 4 are where ransomware and business email compromise are stopped. Sections 7 and 8 are what turn an incident into a documented, contained event.

Galleon builds every one of these controls into its healthcare managed IT service and maintains the evidence year-round. If you would like the assessment done for you, take the free three-minute IT risk assessment at galleonvirtual.com/it-risk-assessment or call (972) 776-6366 for a no-cost review.

Galleon Virtual Services, LLC (Galleon IT Solutions). Headquarters: 1901 N Central Expy, Richardson, TX 75080. Houston office: 15355 W. Vantage Parkway, Houston, TX 77032. galleonvirtual.com