Business IT Support, LLC · Phoenix, AZ · 2026 Edition

The Healthcare & Legal Practice Security Guide 2026

Seven chapters of actionable security guidance for Phoenix healthcare practices and law firms — written from real incident data, not vendor marketing materials.

- Zero Trust Implementation Checklist
- HIPAA & ABA Gap Analysis
- Ransomware Response Playbook
- Microsoft 365 Hardening Guide
- AI Governance Policy Template
- Vendor & Third-Party Risk Assessment
- Self-Assessment Scorecard

$1.1M	94%	32%	45 days
avg healthcare breach cost	of OCR audits find deficiencies	ransomware increase (2024)	AZ notification deadline

Business IT Support, LLC is a security-first managed IT services provider serving healthcare practices and law firms across the Phoenix Metropolitan Area. This guide is based on security incidents our team responded to and assessments our team conducted in 2024–2025.

businessitsupport.net · (602) 935-5505 · info@businessitsupport.net

Table of Contents

This guide covers the security controls our team most frequently finds missing during assessments of Phoenix-area healthcare practices and law firms. Each chapter includes specific, actionable guidance — checklists, templates, and playbooks you can use immediately.

How to use this guide

Start with the Self-Assessment Scorecard on the final pages to identify your highest-priority gaps. Then work through the chapters that address those gaps. Print the scorecard and checklists for use during your assessment. Share relevant chapters with clinical leads, managing partners, or office administrators who own those controls.

Questions about this guide? Contact Business IT Support at (602) 935-5505 or info@businessitsupport.net. We offer a free 30-minute security assessment that benchmarks your environment against every control in this guide and delivers a written gap report within 48 hours.

CHAPTER 01

Zero Trust Implementation Checklist

Never trust, always verify — the minimum security posture for healthcare and legal environments in 2026.

Zero Trust is not a product — it is an architecture built on one principle: every user, device, and application must prove who it is, every time, regardless of where the connection originates. For healthcare practices and law firms, a single compromised credential can expose thousands of patient records or attorney-client privileged communications. Zero Trust is the only defensible baseline.

Why this matters: the Change Healthcare breach

The 2024 Change Healthcare breach — which disrupted billing for hundreds of Phoenix-area practices — succeeded because an attacker used stolen credentials to access a Citrix portal that had no MFA. One account. No MFA. $872 million in direct costs. Months of revenue disruption for practices that had nothing to do with the breach.

Pillar 1 — Identity: Make Every Login Prove Itself

- Enable Microsoft Entra ID (formerly Azure AD) as your identity provider for all practice applications — EHR, billing, practice management, email.
- Require MFA for every user account without exception, including admin accounts, service accounts, and accounts that have not been used recently.
- Deploy phishing-resistant MFA for high-privilege accounts: Microsoft Authenticator with number-matching (not just push notifications, which are vulnerable to MFA fatigue attacks) or FIDO2 hardware security keys. Avoid SMS-based MFA — SIM-swap attacks are documented and inexpensive.
- Block legacy authentication protocols via Conditional Access. Entra ID ’ Security ’ Conditional Access ’ New Policy. Block access where Client Apps = Exchange ActiveSync + Other clients. Legacy auth bypasses MFA entirely.
- Create a Conditional Access Policy blocking sign-ins from high-risk countries. Unless your staff regularly travel to Russia, North Korea, or China, there is no reason to accept login attempts from those IP ranges.
- Enable Entra ID Identity Protection with risk-based Conditional Access: medium-risk sign-ins require MFA step-up; high-risk sign-ins require password reset.
- Activate Privileged Identity Management (PIM). Convert all permanent Global Admin and Exchange Admin assignments to eligible — require just-in-time elevation with a business justification and approval workflow.
- Audit service accounts and shared credentials. "Front desk login" shared across staff is a HIPAA violation (§164.312(a)(2)(i)) and makes incident forensics impossible. Convert to individual accounts or managed identities.

Pillar 2 — Devices: Trust Only What You Can See

- Enroll all endpoints in Microsoft Intune — Windows, macOS, iOS, and Android. Non-enrolled devices should not have access to practice data.
- Create Intune Compliance Policies requiring: disk encryption (BitLocker/FileVault), OS minimum version, screen lock after 5 minutes, and active antivirus.
- Create a Conditional Access Policy blocking access from non-compliant or unmanaged devices. This is the payoff for Intune enrollment.
- Deploy SentinelOne Singularity or Microsoft Defender for Endpoint Plan 2 on all endpoints with real-time behavioral protection active. Verify coverage — an agent that has not checked in for 30 days provides zero protection.
- Enable Intune Application Protection Policies for mobile: require PIN to access corporate data, block copy/paste to unmanaged apps, enable remote wipe of corporate data without wiping the personal device.
- Disable USB mass storage on clinical and legal workstations via Intune Device Configuration. A USB drive can copy every patient record in your EHR in minutes — this is a documented insider threat vector.

Pillar 3 — Network: Remove Implicit Trust

- Replace legacy VPN with Microsoft Entra Private Access (ZTNA). Traditional VPNs grant network-level access — ZTNA grants access only to specific applications for verified users on compliant devices.
- Deploy Cisco Umbrella or Entra Internet Access for DNS-layer threat filtering on all endpoints. Blocks connections to known command-and-control servers and phishing domains before a connection is established.
- Segment your network: clinical/legal workstations on a dedicated VLAN, isolated from guest Wi-Fi, IoT devices, printers, and medical equipment.
- Disable RDP (port 3389) exposure to the internet. Run a Shodan search for your public IP range. If RDP is visible, you are actively being scanned by automated attack tools.
- Review all firewall rules annually. Remove any allow-any-to-any rules and document the business justification for every rule permitting inbound internet traffic.

Pillar 4 — Applications & Data

- Enable Microsoft Defender for Cloud Apps (MCAS) for shadow IT discovery. You will find unapproved applications being used with patient and client data.
- Create DLP policies in Microsoft Purview using the HIPAA template. Block PHI/PII transmission to personal email, USB drives, and unapproved cloud storage.
- Apply Microsoft Purview Sensitivity Labels to PHI-containing documents. Labels enforce encryption and access controls that travel with the file.

Review all OAuth application consents in Entra ID. Revoke any application with permissions like "Read all mail" or "Full access to all files" from an unknown publisher. OAuth consent phishing is a primary attack vector against law firms.

CHAPTER 02

HIPAA & ABA Compliance Gap Analysis

The controls most practices fail — from real OCR audit findings and Bar disciplinary proceedings.

The Office for Civil Rights audited 166 healthcare organizations between 2022 and 2024. 94% had at least one HIPAA Security Rule deficiency. The most cited failures are not exotic technical problems — they are foundational controls that were never implemented or documented. This chapter covers the specific safeguards where practices consistently fail.

How OCR investigations typically start

Most practices discover compliance gaps through a breach — not through proactive assessment. OCR investigations are typically triggered by a breach report, a patient complaint, or a media report. Once opened, OCR requests documentation you must produce within 10 business days. If you cannot produce it, OCR assumes it does not exist.

The 12 HIPAA Security Rule Controls Most Practices Fail

- Access Controls (§164.312(a)(1)): Unique usernames and automatic logoff required. Shared login credentials — even 'just for the front desk' — are a direct violation. Every login must be attributable to a specific individual.
- Audit Controls (§164.312(b)): Your EHR must log who accessed which patient record and when. Most practices have logging enabled but have never reviewed the logs. OCR will request 6 months of access logs.
- Transmission Security (§164.312(e)): ePHI transmitted over open networks must be encrypted. Sending patient records via standard Gmail or unencrypted Outlook — even to a colleague — is non-compliant.
- Workforce Training (§164.308(a)(5)): Annual security awareness training is required and must be documented. Digital completion records must be retained. 'We covered it in the staff meeting' is not documentation.
- Risk Analysis (§164.308(a)(1)): A written, comprehensive risk analysis of all ePHI is required — not a vendor checklist, not a generic template. This is the #1 deficiency cited in OCR audits.
- Sanction Policy (§164.308(a)(1)(ii)(C)): You must have a documented policy for disciplining employees who violate HIPAA, and you must enforce it. Without it, you cannot demonstrate accountability to OCR.
- Contingency Plan (§164.308(a)(7)): Data backup plan, disaster recovery plan, and emergency mode operation plan are all required. Most practices have backups but no documented recovery procedure.
- Device & Media Controls (§164.310(d)(1)): Old workstations and hard drives must be professionally wiped (NIST 800-88) or physically destroyed before disposal. 'We deleted the files' is insufficient.
- Workstation Use (§164.310(b)): Documented policies for workstation functions and physical security. In clinical areas: screen privacy filters, automatic lock after 5 minutes, screens not visible to patients in waiting areas.
- Business Associate Agreements (§164.308(b)(1)): Signed BAAs with every vendor who handles ePHI — IT provider, EHR vendor, billing company, cloud backup, transcription service, answering service. Verbal agreement is not a BAA.

- Assigned Security Responsibility (§164.308(a)(2)): A named Security Officer required in writing. Does not need to be full-time, but must understand their responsibilities and be documented in your policies.
- Physical Safeguards (§164.310(a)(1)): Unlocked server closets, unattended clinical workstations logged into the EHR, and patient records visible on screens facing waiting rooms are all common OCR findings.

OCR Civil Penalty Tiers

Violation Category	Per Violation	Annual Cap
Did not know (reasonable cause)	**$100–$50,000**	**$25,000**
Reasonable cause — no willful neglect	**$1,000–$50,000**	**$100,000**
Willful neglect — corrected	**$10,000–$50,000**	**$250,000**
Willful neglect — not corrected	**$50,000**	**$1,500,000**

Penalties are per violation category, not per incident. A single breach involving a missing BAA, inadequate training, and no risk analysis can trigger three penalty tiers simultaneously.

ABA Formal Opinion 477R — The 5 Cybersecurity Obligations for Law Firms

- Competency (Model Rule 1.1): Attorneys must understand the benefits and risks of technology they use in client representation — including AI tools, cloud storage, and remote access systems. Ignorance of a tool's security properties is not a defense in a disciplinary proceeding.
- Confidentiality (Model Rule 1.6): Reasonable measures must be taken to prevent unauthorized disclosure of client information. 'Reasonableness' considers the sensitivity of the information, the cost of the safeguard, and the probability of a breach.
- Factor Analysis for Communication Methods: The Opinion requires contextual analysis of each communication method. Email without encryption may be reasonable for scheduling — it is not reasonable for transmitting litigation strategy or settlement terms.
- Supervision (Model Rules 5.1 and 5.3): Partners are responsible for supervising associates' and staff's use of technology — including AI drafting tools, legal research platforms, and cloud storage. Unsupervised AI work product used in client matters is a supervision failure.
- Due Diligence on Technology Vendors: Before using any cloud platform, collaboration tool, or legal technology product with client data, the firm must conduct reasonable due diligence on the vendor's security practices.

Arizona-Specific: State Bar and Breach Notification

The State Bar of Arizona has adopted ABA Model Rules including Rule 1.6 comment [18], which explicitly requires attorneys to make reasonable efforts to prevent unauthorized disclosure of client information. The Arizona Data Breach Notification Act (A.R.S. § 18-552) requires notification to affected individuals within 45 days of discovering a breach — shorter than HIPAA's 60-day window.

CHAPTER 03

Ransomware Response Playbook

72-hour response guide based on real healthcare and legal ransomware incidents in the Phoenix metro area (2024–2025).

Ransomware targeting healthcare and legal practices increased 32% in 2024. The average ransom demand for a medical practice is $450,000. The average total recovery cost — including downtime, legal fees, OCR penalties, notification costs, and remediation — is $1.1 million for practices under 50 employees. The first four hours determine whether you pay, whether you recover, and whether you face an OCR investigation. Most practices waste those hours because no one has thought through the response before.

Real incident: Phoenix orthopedic practice, December 2024

A 12-physician orthopedic practice contacted our team 14 hours after discovering ransomware. Staff had spent 8 hours trying to 'fix' individual machines by running antivirus scans — during which the malware continued encrypting network shares. Their backup server was on the same network segment and was also encrypted. Recovery: 3 weeks. Patient records unavailable for 18 days. OCR investigation opened. Total cost: approximately $340,000.

Before an Incident: Emergency Contact Sheet (Print This Now)

Print and store physically — your email and files may be inaccessible during an incident.

- IT provider emergency line: Business IT Support — (602) 935-5505 — available 24/7 for active incidents
- Cyber insurance carrier claims line: [Find your carrier's claims number NOW and document it] — most policies require notification within 24 hours
- FBI Phoenix Field Office Cyber Division: (623) 466-1999 — report ransomware; they can identify the attacker group and advise on OFAC sanction implications before any payment
- Your healthcare attorney / outside general counsel: [Document now] — you need privilege protection over your breach investigation immediately
- HHS OCR Breach Hotline: 1-800-368-1019 — 60-day notification clock starts at discovery, not at containment
- Your EHR/EMR vendor emergency line: [Find in your contract before an incident] — they may have a clean database backup
- Arizona State Bar (law firms): (602) 252-4804 — consult on client notification obligations before contacting clients

Hour 0–1: Immediate Isolation

- Disconnect affected computers from the network immediately — unplug ethernet and disable Wi-Fi on any machine showing symptoms. Do NOT power off the machine — memory forensics may be needed to identify the attack vector.

Do NOT pay the ransom before consulting your cyber insurance carrier and legal counsel. Certain ransomware groups are on the U.S. Treasury OFAC sanctions list — paying them can result in additional federal penalties.

Call your IT provider immediately to begin environment isolation and forensic preservation. Waiting until morning allows active malware to continue spreading.

Document the time of discovery, who discovered it, what systems appear affected, and photograph the ransom note. This documentation becomes your evidence of 'reasonable response' for OCR.

Identify clean systems not yet affected — isolate them from the network before the malware reaches them.

Notify your cyber insurance carrier within 24 hours. Late notification can void your claim. Most carriers dispatch an IR team covered by your policy — use that resource.

Hour 1–4: Assessment and Investigation

- Determine the attack vector with your IT provider: phishing email, RDP brute force, compromised credentials, or supply chain compromise. Check firewall and mail logs.
- Map the blast radius: which systems are encrypted, which are intact. Check for large outbound data transfers in the 48–72 hours before encryption — most modern ransomware exfiltrates data before encrypting ('double extortion').
- Determine whether ePHI or attorney-client privileged data was on affected systems. This drives your breach notification obligations. If PHI was on an encrypted system, assume exfiltration until forensics prove otherwise — that triggers the OCR 60-day clock.
- Verify backup integrity: confirm your most recent clean backup predates the infection, is accessible, and is not encrypted.
- Engage your cyber insurance carrier's incident response team. Forensics, legal counsel, PR support, and negotiation services are typically covered by your policy.

Hour 4–24: Communication Decisions

Do not notify patients or clients yet

HIPAA requires notification within 60 days of discovery — not immediately. Premature patient notification before a forensic determination of what was accessed can complicate the investigation, inflate liability, and cause unnecessary distress. For law firms, consult with the State Bar and general counsel before any client notification.

- Prepare internal staff communication: what happened, what staff should and should not say, and what operational changes are in effect.
- If patient appointments are affected, communicate operational disruptions without disclosing the nature of the incident until forensics are complete.
-

Document every decision with a timestamp and rationale in writing — this becomes your evidence of reasonable response for OCR.

Hour 24–72: Recovery Sequencing

Restore from the most recent verified clean backup — never from a backup taken after the infection date. Ransomware can be dormant for weeks before encrypting.

Reset all passwords organization-wide before reconnecting any system to the network. Assume all credentials are compromised.

Rebuild compromised systems from scratch rather than attempting to clean them. Malware persistence mechanisms (registry changes, scheduled tasks, rootkits) are routinely missed by cleanup tools.

Re-enable systems in priority order: patient scheduling and case management first, billing second, administrative functions last.

Conduct a post-incident review within 30 days — document the full timeline, forensic findings, attack vector, and control improvements. Required for an OCR submission if one is opened.

CHAPTER 04

Microsoft 365 Security Hardening Guide

The 23 settings Microsoft ships disabled — with exact Admin Center navigation paths.

Microsoft 365 ships with security features disabled because Microsoft optimizes for frictionless onboarding, not security. The settings below are all off by default. Each represents a real attack vector our team has seen exploited in Phoenix-area practice environments. Admin Center paths are current as of March 2026.

Authentication & Identity (Start Here — Highest Impact)

- Block Legacy Authentication: Entra ID ’ Security ’ Conditional Access ’ New Policy. Condition: Client Apps = Exchange ActiveSync + Other clients. Grant: Block access. Legacy auth bypasses MFA entirely — this is the highest-value change in M365.
- Enable Security Defaults or Conditional Access MFA: Entra ID ’ Properties ’ Manage Security Defaults. If on M365 Business Basic/Standard without Entra P1, enable Security Defaults. With Entra P1/P2 (included in Business Premium), disable Security Defaults and use Conditional Access instead.
- Require MFA for All Admin Roles: Create a CA policy targeting all directory admin roles. Grant: Require MFA. Global Admin accounts should use FIDO2 hardware keys — a stolen Global Admin password without a physical key is useless to an attacker.
- Disable Auto-Forwarding to External Addresses: Exchange Admin Center ’ Mail Flow ’ Remote Domains ’ Default ’ Edit ’ Set Allow Automatic Forwarding to Off. BEC attackers configure inbox rules to silently forward all email to an external account — this blocks that exfiltration method.
- Enable the Unified Audit Log: Compliance portal ’ Audit ’ Start recording. Required for HIPAA audit controls (§164.312(b)). Default retention is 90 days — upgrade to 1 year with M365 E3 or the Audit (Standard) add-on.

Email Security

- Enable Anti-Phishing Policy with Impersonation Protection: Security portal ’ Policies & Rules ’ Threat Policies ’ Anti-phishing. Enable impersonation protection for your domain, managing physician/partner, and billing staff. Set action to Quarantine.
- Enable Safe Links: Security portal ’ Safe Links. Create a policy for all users. Enable 'Do not allow users to click through to the original URL' for clinical and billing staff. Enable URL scanning within Office documents.
- Enable Safe Attachments with Dynamic Delivery: Security portal ’ Safe Attachments. Create a policy for all users with action = Dynamic Delivery. Email body is delivered immediately; attachments are held for detonation analysis.
- Configure DMARC/DKIM/SPF: Verify SPF record includes all legitimate sending sources (M365, your EHR, billing platform). Enable DKIM signing in the Security portal. Add DMARC TXT record with p=quarantine minimum (p=reject preferred).

Enable Quarantine Notifications: Security portal ’ Quarantine Policies. Configure daily digest emails so users know when legitimate email has been quarantined.

Collaboration & Data Governance

Restrict External Sharing in SharePoint: SharePoint Admin Center ’ Policies ’ Sharing. Set to 'Existing guests only' or 'Only people in your organization' for any library containing PHI or client files.

Disable Guest Access in Teams by Default: Teams Admin Center ’ Org-wide settings ’ Guest access. Disable globally; re-enable on a per-team basis only where explicitly required.

Create a DLP Policy for PHI/PII: Compliance portal ’ Data Loss Prevention ’ Policies. Use the HIPAA template. Block external sharing and alert on email transmission of SSNs, health information, and financial data.

Enable Microsoft Purview Sensitivity Labels: Compliance portal ’ Information Protection ’ Labels. Create 4 tiers: Public, Internal, Confidential (PHI/Client), Highly Confidential. Apply encryption to Confidential and above.

Disable Personal Microsoft Account Connections: Entra ID ’ External Identities ’ External collaboration settings. Block invitations from personal Microsoft accounts.

Admin Account Hardening

Create Dedicated Admin Accounts: Admin tasks should use a separate account from the user's daily email account. Admin accounts should not have Exchange mailboxes — compromising them via phishing yields no email access.

Create a Break-Glass Emergency Account: One Global Admin account with a strong random password, not subject to Conditional Access MFA, stored physically in a sealed envelope. Used only if a CA policy misconfiguration locks out all admins. Review quarterly.

Enable PIM for All Admin Roles: Entra ID ’ Identity Governance ’ Privileged Identity Management. Convert all permanent admin assignments to eligible — require justification and approval for elevation.

Review and Revoke Unauthorized Admin Consent: Entra ID ’ Enterprise Applications ’ All Applications ’ filter by Admin consent. Revoke any application with permissions like 'Read all users' mail' or 'Full access to all mailboxes' that you did not explicitly authorize.

Configure Risky User Alerts: Entra ID ’ Security ’ Identity Protection. Configure email alerts to the Security Officer when a user is flagged as high risk. Set a CA policy to require password reset for high-risk users.

Enable SSPR with Writeback: Entra ID ’ Password reset ’ Properties. Enable self-service password reset to reduce helpdesk burden. Require authentication via Authenticator app or FIDO2, not SMS.

Audit Guest User Accounts Quarterly: Entra ID ’ Users ’ filter by User Type = Guest. Remove any guest accounts that are no longer needed. Guest accounts with stale access are a persistent exposure.

Enable Continuous Access Evaluation (CAE): Entra ID ’ Security ’ Conditional Access ’ Named Locations. CAE allows near-real-time session revocation when a user's risk level changes or conditions are violated — without waiting for token expiry.

CHAPTER 05

AI Governance Policy Template

A ready-to-distribute policy for Microsoft Copilot and third-party AI tools — written for HIPAA and ABA compliance.

AI tools are in use at your practice whether you have authorized them or not. Staff are using ChatGPT, Copilot, Grammarly, Perplexity, and AI search tools with patient records and client files. Without a written policy, you cannot enforce responsible use, document compliance for OCR, or defend against a Bar disciplinary proceeding.

The HIPAA risk you may not know about with Microsoft Copilot

Microsoft 365 Copilot — by default — indexes all content in your M365 tenant, including SharePoint, OneDrive, and Teams. Without proper Purview DLP policies and Sensitivity Labels in place, Copilot can surface PHI to users who are not authorized to see it. Before deploying Copilot, ensure your tenant's data governance foundation is in place.

READY-TO-USE AI ACCEPTABLE USE POLICY — CUSTOMIZE BRACKETED FIELDS AND DISTRIBUTE TO ALL STAFF

1. Purpose and Scope

This policy governs the use of artificial intelligence (AI) tools, including large language models, AI-assisted writing platforms, and AI-powered search tools, by all employees, contractors, and agents of [Practice Name]. This policy applies to all AI tools regardless of whether they are practice-provided or personally owned, and whether used on practice premises or remotely.

2. Definitions

AI Tool: Any application that uses machine learning or large language models to generate text, images, code, or analysis — including Microsoft 365 Copilot, ChatGPT, Claude (Anthropic), Google Gemini, Grammarly, Harvey AI, and any AI features embedded in existing software.

Protected Health Information (PHI): Any individually identifiable health information as defined under 45 CFR §160.103, including patient names, dates, diagnoses, medications, and any information that could identify a patient.

Confidential Client Information: Any information relating to client representation, including facts, legal strategy, privileged communications, draft documents, and financial information.

3. Approved AI Tools

The following AI tools are approved for use with appropriate data handling restrictions: Microsoft 365 Copilot (only after IT confirmation of HIPAA-compliant configuration with Purview DLP active); [Additional approved tools — document here]. All other AI tools require written approval from the Security Officer before use with any practice data.

Prohibited Uses — Non-Negotiable

Do NOT enter patient names, dates of birth, medical record numbers, diagnoses, medications, or any PHI into any AI tool — including Microsoft Copilot — unless your IT provider has confirmed in writing that the tool is covered under a signed Business Associate Agreement.

Do NOT enter client names, matter numbers, case facts, legal strategy, privileged communications, draft pleadings, or confidential documents into any AI tool without written approval from the Security Officer.

Do NOT use AI-generated legal research, clinical documentation, case summaries, or analysis without independent attorney or physician review and verification. AI hallucination — confident but factually incorrect output — is a documented risk in all current AI systems.

Do NOT use personal AI accounts (personal ChatGPT subscription, personal Google Gemini) for any practice work. Only practice-provisioned accounts with organizational data governance controls may be used.

Do NOT share AI-generated output externally — to clients, courts, regulators, or payers — without identifying it as AI-assisted and confirming its accuracy through independent verification.

4. Attorney Supervision Obligations (ABA Model Rules 1.1, 5.1, 5.3)

Attorneys are personally responsible for supervising staff use of AI on their matters. AI-generated work product must be reviewed, verified, and edited by the supervising attorney before use. Attorneys must independently verify any AI-generated legal authority cited in a court filing or client communication. Submitting AI content to a court without verification violates the duty of candor (Model Rule 3.3) and competence (Model Rule 1.1).

5. Clinical Documentation AI (HIPAA & State Licensing)

AI-assisted clinical documentation tools — ambient AI scribes, AI-assisted coding, AI note summarization — must be approved by the Security Officer and covered by a signed BAA before deployment. The treating clinician is responsible for reviewing, editing, and attesting to the accuracy of all AI-generated clinical documentation. AI documentation not attested by the responsible clinician is not a valid medical record.

6. Training, Enforcement & Incident Reporting

All staff must complete AI security awareness training within 30 days of hire and annually thereafter. Training records must be retained for 6 years minimum (HIPAA requirement).

Any staff member who believes they entered PHI or confidential client data into an unauthorized AI tool must report to the Security Officer within 24 hours. Prompt reporting allows the practice to conduct a breach risk assessment and meet regulatory notification timelines.

Violations may result in disciplinary action up to and including termination and may be reported to applicable regulatory bodies (OCR, State Bar) as required by law.

Adopted: [Date] · Last Reviewed: [Date] · Next Review: [Annual] · Security Officer: [Name, Title]

CHAPTER 06

Vendor & Third-Party Risk Assessment

Every vendor who touches your data is a potential breach vector. Here's how to evaluate them.

The Change Healthcare breach in February 2024 — the largest healthcare data breach in U.S. history, affecting more than 190 million patients — was a third-party supply chain attack. Hundreds of Phoenix-area practices were disrupted for weeks or months. Your practice did nothing wrong. HIPAA requires Business Associate Agreements with every vendor who handles your ePHI. But a signed BAA alone is not sufficient — it must be with a vendor who actually has adequate security controls.

12-Question Vendor Security Questionnaire

Use for every new vendor — EHR, billing, cloud backup, IT provider, marketing agency, transcription, answering service — before signing a contract.

- Do you sign a HIPAA Business Associate Agreement? If a vendor says a BAA is 'not necessary for their type of service,' terminate the evaluation immediately — this signals HIPAA ignorance or deliberate evasion.
- Where is our data stored, and in which country? U.S.-hosted data is strongly preferred for healthcare and legal data. Offshore storage creates complex questions about OCR jurisdiction and law enforcement access.
- How do you encrypt data at rest and in transit? Acceptable: AES-256 at rest, TLS 1.2+ in transit. Unacceptable: 'Yes, we take security seriously' without specifics.
- What is your SOC 2 Type II audit status? Ask for the executive summary of the most recent report. A vendor who cannot produce one from the past 18 months has not been independently audited.
- How do you manage subprocessors? Are sub-vendors contractually bound by the same security obligations? The Change Healthcare incident involved an inadequately secured subprocessor.
- What is your breach notification commitment? Your BAA must specify a timeline — typically 24–72 hours to notify your practice, so you can meet your own OCR 60-day and Arizona 45-day notification deadlines.
- Do you conduct annual penetration testing? Ask for the executive summary and remediation status. A vendor who cannot produce this has not been tested; a vendor who cannot show remediation has known unpatched vulnerabilities.
- What access do your employees have to our data, and how is it controlled? Require role-based access controls, MFA for all employees accessing customer data, and least-privilege principles.
- How do you handle data deletion at contract termination? Require the specific process, timeline, and written confirmation in your contract — not a verbal assurance.
- Have you experienced a data breach in the past 3 years? A past breach does not disqualify a vendor. A poor response to a past breach does. Ask: 'What specifically changed after the breach?'
- What are your RTO and RPO commitments? Recovery Time Objective and Recovery Point Objective should be contractual service level commitments — not marketing language about 'high availability.'
- Do you maintain a software bill of materials (SBOM)? The Change Healthcare breach exploited a vulnerable third-party library. Vendors must be able to identify their software dependencies and patch status.

BAA Required Elements (45 CFR §164.504(e))

- Specifies permitted uses and disclosures of ePHI — must enumerate exactly what the vendor is allowed to do with your data
- Vendor agrees to use appropriate safeguards and comply with applicable HIPAA Security Rule requirements
- Vendor agrees not to use or disclose ePHI except as permitted or required by law
- Vendor agrees to report breaches, security incidents, and unauthorized disclosures within the timeframe specified
- Vendor agrees to make ePHI available to support individual patient access rights upon your request
- Vendor agrees to return or destroy all ePHI upon contract termination — method and timeline specified
- Vendor agrees to make internal practices, books, and records available to HHS upon request
- Vendor agrees all subprocessors are bound by equivalent BAA obligations
- BAA identifies your organization and the vendor by legal entity name — not 'customer' or 'client'
- BAA is signed by an authorized representative of the vendor with authority to bind the organization legally

Red Flags — Walk Away Immediately

- 'A BAA is not necessary for our type of service' — factually incorrect for any vendor accessing, storing, or transmitting ePHI. Signals HIPAA ignorance or deliberate evasion.
- Template BAA that does not specify a breach notification timeframe — your vendor can discover a breach today and notify you 59 days later, eliminating your ability to meet notification deadlines.
- Data stored offshore without a clear legal framework governing law enforcement access and adequate contractual protections for patients' rights.
- Inability to produce a SOC 2 Type II report from the past 18 months — absence of audit evidence is evidence of absent security controls.
- Security questionnaire responses that are vague or consist of marketing language — 'We use industry-leading security' is not an answer to a specific security question.
- Requests for permanent admin-level access to your M365 tenant, EHR, or network with no ability to scope permissions — legitimate IT vendors do not need permanent Global Admin access.

SELF-ASSESSMENT

Security Scorecard

For each item below, check the box if the control is fully implemented. A gap in any box is a potential compliance deficiency or attack surface. Use this scorecard as the starting point for your risk analysis. A fully honest scorecard is the foundation of a useful security program.

Identity & MFA

- [ ] MFA enabled for every user account — no exceptions
- [ ] Legacy authentication protocols blocked via Conditional Access
- [ ] Privileged Identity Management (PIM) active — no permanent admin roles
- [ ] No shared credentials — every login attributable to an individual
- [ ] Conditional Access Policy blocking high-risk country sign-ins
- [ ] Risky user and risky sign-in alerts configured to Security Officer

Devices & Endpoints

- [ ] All endpoints enrolled in Microsoft Intune (Windows, macOS, iOS, Android)
- [ ] Intune Compliance Policy active — disk encryption, OS version, screen lock
- [ ] EDR (SentinelOne or Defender P2) deployed on all endpoints, coverage verified
- [ ] USB mass storage disabled on clinical/legal workstations
- [ ] Conditional Access blocking non-compliant device access

Email Security

- [ ] Anti-phishing policy with impersonation protection enabled
- [ ] Safe Links enabled for all users with block-through protection
- [ ] Safe Attachments enabled with Dynamic Delivery
- [ ] DMARC, DKIM, and SPF configured and validated
- [ ] Auto-forwarding to external addresses disabled
- [ ] Unified Audit Log enabled with minimum 1-year retention

HIPAA Documentation

- [ ] Current written risk analysis (updated within past 12 months)
- [ ] BAAs signed with all vendors who handle ePHI
- [ ] Annual workforce security awareness training — completion documented
- [ ] Security Officer named in writing with documented responsibilities
- [ ] Sanction policy for HIPAA violations documented and distributed
- [ ] Workstation use policy documented and enforced

Incident Response

- [ ] Emergency contact sheet printed and stored physically
- [ ] Backup tested and restored successfully in the last 90 days
- [ ] Backup is offline or immutable (not on the same network as workstations)
- [ ] Recovery time estimate documented in writing

AI & Data Governance

- [ ] AI acceptable use policy distributed and acknowledged by all staff
- [ ] DLP policies active in Microsoft Purview
- [ ] Sensitivity Labels deployed across SharePoint and OneDrive
- [ ]

- [ ] Cyber insurance policy obtained and claims process understood
- [ ] Post-incident documentation process defined

Inventory of all AI tools in use (sanctioned and unsanctioned) completed

- [ ] M365 Copilot — if deployed — configured with Purview DLP active
- [ ] Training on AI policy and data classification requirements completed

Scoring guidance: 0–6 unchecked — schedule an emergency risk assessment immediately. 7–16 unchecked — significant gaps requiring prioritized remediation. 17–24 unchecked — critical exposure; contact Business IT Support for an emergency assessment. 25–35 unchecked — your organization has not yet implemented foundational security controls.

Ready to close your gaps?

Business IT Support offers a free 30-minute security assessment that benchmarks your environment against every control in this guide and delivers a written gap report within 48 hours — no obligation, no high-pressure sales. We serve healthcare practices and law firms across the Phoenix Metropolitan Area.

Book Free Assessment
businessitsupport.net/contact

Call Direct
(602) 935-5505 · Mon–Fri 8AM–6PM MST

Business IT Support, LLC · Phoenix Metropolitan Area · info@businessitsupport.net · businessitsupport.net