Healthcare and HIPAA

ComplyClinic Playbook

HIPAA Security Readiness Playbook for Small Healthcare Practices

A practical readiness guide for protecting ePHI and documenting security controls.

Audience: Small healthcare, dental, therapy, and wellness practices handling electronic protected health information.

General educational resource only. This is not legal advice, certification advice, or a substitute for a formal security risk analysis, CMMC assessment, or incident response engagement.

HIPAA security in plain English

HIPAA security is about protecting electronic protected health information, or ePHI, using administrative, physical, and technical safeguards. Practices need reasonable and appropriate controls based on risk, size, systems, and workflows.

This playbook is not legal advice. It is an operational security guide to help you prepare, document, and improve.

Administrative safeguards

Maintain a current risk analysis, assign security responsibility, define workforce access rules, document sanction procedures, and train staff.

Keep evidence: policies, training records, access reviews, risk register, vendor list, and incident response notes.

Physical safeguards

Protect workstations, laptops, mobile devices, paper records, server closets, network gear, and front desk areas.

Common gaps include shared workstations left unlocked, lost laptops without encryption, exposed Wi-Fi equipment, and printed PHI left in public areas.

Technical safeguards

Use unique user accounts, MFA, role-based access, audit logs, encryption, automatic timeout, endpoint protection, and secure backups.

Review who can access the EMR, billing systems, shared drives, email, and cloud storage. Remove access quickly when staff leave.

BAAs and vendor oversight

Track vendors that create, receive, maintain, or transmit PHI on your behalf. Keep Business Associate Agreements organized and review critical vendors periodically.

Vendor risk is not only a compliance issue. A vendor outage, breach, or misconfiguration can directly affect patient care and operations.

Incident response basics

Have a simple process for suspected phishing, lost devices, ransomware, accidental disclosures, and suspicious EMR activity.

Document what happened, who was involved, when it was discovered, what systems were affected, and what containment steps were taken.

90-day improvement roadmap

Days 1-30: complete a basic asset and access inventory. Days 31-60: address MFA, encryption, backups, and email security. Days 61-90: update policies, train staff, and run a tabletop exercise.

Next step: Schedule a HIPAA security readiness call to identify practical next steps for your practice. Schedule now

Need help turning this into a practical roadmap? Book a free consultation at complyclinic.com.

ComplyClinic • Practical cybersecurity, compliance readiness, automation, app development, and AI governance support.