Guess Compliance Consulting LLC

Compliance made simple — for small healthcare teams

HIPAA Audit Checklist

Administrative Safeguards

■ Do you have a designated Privacy and Security Officer?

■ Are HIPAA policies and procedures documented and reviewed annually?

■ Is workforce HIPAA training documented and updated annually?

■ Do you have a sanction policy for staff who violate HIPAA?

■ Are Business Associate Agreements (BAAs) in place with all vendors handling PHI?

Physical Safeguards

■ Are paper records stored securely with access limited to authorized staff?

■ Are workstations positioned to prevent unauthorized PHI viewing?

■ Is there a facility access control system (keys, badges, logs)?

■ Are devices with PHI properly disposed of or destroyed when retired?

Technical Safeguards

■ Is PHI encrypted on all devices and during transmission (email, portals)?

■ Are unique user IDs and strong passwords required for PHI access?

■ Do you have audit logs enabled to track access to PHI?

■ Are audit trails maintained and reviewed regularly for unusual activity?

■ Is remote access secured with multi-factor authentication (MFA)?

Organizational Requirements

■ Are vendors and subcontractors bound by HIPAA-compliant agreements (BAAs)?

■ Do you review vendor compliance annually?

Patient Rights

■ Do you provide patients with a Notice of Privacy Practices (NPP)?

■ Are patient requests for access to records handled within HIPAA timeframes?

■ Do you have a process for amending patient records when requested?

■ Is there a clear process for patients to request restrictions or confidential communications?

Documentation

■ Are HIPAA policies and procedures documented and accessible to staff?

■ Do you retain HIPAA-related documentation for at least 6 years as required?

■ Are training logs, risk analyses, and breach notifications maintained?

Breach Notification

■ Do you have a breach response plan documented and tested?

■ Are patients notified of breaches within 60 days as required?

■ Do you maintain a breach log for all incidents, even minor ones?

■ Use this expanded checklist to identify gaps and prepare your practice for HIPAA compliance audits. For support, contact Guess Compliance Consulting LLC.