PalladianCyber

HIPAA Security Rule: A Practical Guide for Small Medical Practices

Clear, actionable steps to protect patient information (PHI).

Executive Summary

This guide provides a practical, plain-language overview of the HIPAA Security Rule tailored for small and mid-sized medical practices. It focuses on the administrative, technical, and physical safeguards required to protect electronic Protected Health Information (ePHI), including access controls, encryption expectations, workforce training, and incident response fundamentals. The document highlights security controls that regulators and auditors routinely expect to see implemented in real clinical environments. The recommendations are designed to be achievable for resource-constrained practices while still establishing a defensible baseline security posture. The goal of this guide is to help healthcare organizations reduce risk, improve compliance readiness, and protect patient data through clear, actionable safeguards that can be implemented immediately.

1. What Counts as PHI?

PHI includes any information that identifies a patient and relates to health, billing, or treatment:

- Names, contact information, dates of birth, Social Security numbers
- Medical record numbers and insurance identifiers
- Lab results, diagnoses, and treatment notes
- Patient-linked images such as X-rays or scans

2. Minimum Necessary Principle

Staff should access only the information required to perform their job functions:

- Reception: scheduling and insurance only
- Billing: payments and insurance, not clinical notes
- Nurses: relevant current chart data
- Providers: full chart access

3. Access Controls

- Unique logins for all users — no shared accounts
- Automatic screen locking after short inactivity periods
- Role-based permissions within EHR systems
- Immediate account disablement upon employee departure
- Multi-factor authentication for email and remote access

4. Encryption Expectations

- Full-disk encryption on laptops, tablets, and mobile devices
- Use of HTTPS-based EHR and patient portals
- Avoid emailing PHI; use secure messaging instead
- Encrypted backups prior to storage or transmission

5. Employee Training

- HIPAA and security training at hire and annually
- Basic phishing and social engineering awareness
- Clear documentation of prohibited actions

6. Audit Logs & Incident Response

- Logging of logins, chart access, and data exports
- Tracking of account creation, deletion, and permission changes
- Identify, contain, document, notify, and review incidents

7. Quick Compliance Checklist

- Unique logins for all staff
- Screen locking enabled on all systems
- Encrypted laptops and backups
- Regular review of EHR permissions
- Annual HIPAA training documented
- Printed PHI minimized and securely destroyed
- Backups tested periodically

Prepared by Patrick Muller — Cybersecurity & Compliance Analyst, PalladianCyber