

HIPAA Compliance Checklist for Medical Practices

A complete walkthrough of the essential HIPAA compliance steps — from risk assessment to breach response — for practices and business associates alike.

The Core Compliance Steps

- 1 **Conduct a risk assessment.** Identify where PHI is stored, received, maintained, or transmitted, and look for vulnerabilities across your systems and processes.
- 2 **Develop and implement policies and procedures.** Write clear policies covering data access controls and breach notification protocols, and keep them practical and accessible to staff.
- 3 **Train your workforce.** Everyone in the organization needs to understand HIPAA rules and their role in compliance, reinforced with regular training.
- 4 **Secure your systems.** Use technical safeguards — encryption, firewalls, secure authentication — alongside physical safeguards like locked file cabinets and controlled workstation access.
- 5 **Monitor and audit regularly.** Compliance isn't a one-time event; regular audits catch issues early.
- 6 **Prepare for breaches.** Have a clear incident response plan ready so you can act quickly if one occurs.

The Five HIPAA Rules to Know

Privacy Rule	Protects individually identifiable health information and limits use or disclosure without patient authorization.
Security Rule	Requires administrative, physical, and technical safeguards for electronic PHI — strong passwords, encrypted transmissions, and more.
Breach Notification Rule	Requires notifying affected individuals, HHS, and sometimes the media promptly after a breach of unsecured PHI.
Enforcement Rule	Outlines penalties for violations and the investigation and hearing process.
Omnibus Rule	Strengthens privacy and security protections, extending certain requirements to business associates.

Practical Measures Worth Adopting

- Role-based access controls — billing staff don't need access to clinical notes
- Encrypt data at rest and in transit, whether stored or sent
- Maintain audit logs of who accessed PHI and when
- Keep software and systems current to close known vulnerabilities
- Secure physical locations with locks, cameras, and visitor logs
- Assign a breach response team with clear roles, and practice the plan
- Document everything — risk assessments, training, and audits alike

HIPAA compliance is an ongoing process, not a one-time certification. VirtualScrivener builds every service — AI Scribe, Virtual Medical Scribe, Medical Transcription, and Records & Legal Document Support — on this same compliance program from day one: signed BAAs, encryption in transit and at rest, role-based access control, and audit logging.

VirtualScrivener · contactus@virtuallscrivener.com · +1 (307) 215-3356 · virtuallscrivener.com · 30 N Gould St STE 21483, Sheridan, WY 82801