

Healthcare Compliance and HIPAA Training

Wealth Horizons Academy | \$397

PROTECT YOUR PRACTICE AND YOUR PATIENTS

HIPAA compliance is not optional. Healthcare providers and business associates who handle Protected Health Information (PHI) are legally required to comply with HIPAA regulations. Non-compliance can result in fines from \$100 to \$50,000 per violation.

MODULE 1: HIPAA FUNDAMENTALS

What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. Its Privacy Rule and Security Rule set national standards for: - Protecting patient health information - Controlling who can access PHI - Securing electronic PHI - Establishing patient rights over their information

Who Must Comply?

Covered Entities: - Healthcare providers (physicians, hospitals, clinics) - Health plans (insurance companies) - Healthcare clearinghouses

Business Associates: Any vendor or contractor who handles PHI on behalf of a covered entity: - Billing companies - IT vendors - Transcription services - Legal services with access to PHI

Protected Health Information (PHI)

PHI is any health information that can identify an individual combined with health data.

18 HIPAA Identifiers: 1. Names 2. Geographic data smaller than state 3. Dates related to individual 4. Phone numbers 5. Fax numbers 6. Email addresses 7. Social Security numbers 8. Medical record numbers 9. Health plan beneficiary numbers 10. Account numbers 11. Certificate/license numbers 12. Vehicle identifiers 13. Device identifiers 14. Web URLs 15. IP addresses 16. Biometric identifiers 17. Full-face photographs 18. Any other unique identifying number

MODULE 2: PRIVACY RULE COMPLIANCE

Patient Rights Under HIPAA

Patients have the right to: - Access their PHI - Request corrections to their records - Receive a notice of privacy practices - Request confidential communications - Restrict certain disclosures - Receive an accounting of disclosures

Minimum Necessary Standard

When using or disclosing PHI, provide only the minimum amount necessary to accomplish the purpose.

Example: A billing staff member needs the patient's diagnosis code — not their full medical record.

Permitted Disclosures Without Authorization

PHI can be used or disclosed without patient authorization for: - Treatment purposes - Payment activities - Healthcare operations - Public health activities - Law enforcement (limited) - Serious threat to health/safety

MODULE 3: SECURITY RULE COMPLIANCE

Administrative Safeguards

- Designate a Security Officer
- Conduct regular risk assessments
- Implement workforce training
- Create access management policies
- Establish contingency plans

Physical Safeguards

- Workstation access controls
- Device and media controls
- Facility access controls
- Visitor policies

Technical Safeguards

- Unique user identification
- Automatic logoff
- Encryption of data in transit and at rest
- Audit controls and logs
- Transmission security

MODULE 4: BREACH NOTIFICATION

What Is a Breach?

An impermissible use or disclosure of PHI that compromises its security or privacy.

Breach Notification Requirements

To Patients: Within 60 days of discovery **To HHS (OCR):** Within 60 days (500+ patients); annual report (under 500) **To Media:** Within 60 days if 500+ patients in a state/jurisdiction affected

Breach Prevention

- Regular staff training
- Strong password policies
- Encryption of all devices containing PHI
- Business associate agreements with all vendors
- Regular risk assessments

MODULE 5: COMPLIANCE PROGRAM ESSENTIALS

Building a HIPAA Compliance Program

1. Designate a Privacy Officer and Security Officer
2. Conduct and document annual risk assessments
3. Implement written policies and procedures
4. Train all workforce members annually (document training)
5. Execute Business Associate Agreements with all vendors
6. Establish a complaint process for patients
7. Apply appropriate sanctions for non-compliance
8. Review and update policies regularly

OCR Audit Readiness

The Office for Civil Rights (OCR) conducts HIPAA audits. Be ready to produce: - Risk assessment documentation - Workforce training records - Policies and procedures - Business Associate Agreements - Incident response logs - Notice of Privacy Practices

Educational purposes only. Not professional advice. Results vary.

© 2026 Wealth Horizons Academy | wealthhorizonsacademy.org