HIPAA Security and Privacy Rule Compliance for Healthcare Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The landscape of U.S. healthcare compliance is complex and constantly evolving, placing significant responsibility on Covered Entities (CEs) and Business Associates (BAs) to safeguard patient data. The Health Insurance Portability and Accountability Act (HIPAA), particularly the Privacy and Security Rules, forms the bedrock of health data protection. HIPAA Security and Privacy Rule Compliance for Healthcare Training Course provides a comprehensive and practical guide to achieving and maintaining HIPAA compliance, focusing on the latest regulatory changes, including the HITECH Act and the Omnibus Rule. Participants will learn to navigate the intricate requirements for protecting both paper and electronic Protected Health Information (ePHI), implementing robust administrative, physical, and technical safeguards, and mitigating the rising threat of cybersecurity breaches to avoid substantial civil and criminal penalties.

This training is critically important for fostering a culture of compliance and reinforcing patient trust in an increasingly digitized healthcare ecosystem. It moves beyond theoretical knowledge, offering practical risk management strategies and focusing on real-world enforcement case studies to illustrate the direct consequences of non-compliance. The curriculum is designed to equip key personnel with the necessary expertise to develop, implement, and audit internal policies, manage Business Associate Agreements (BAAs), and execute effective breach notification procedures. Mastering these competencies is no longer optional it is a mandatory and continuous effort to ensure data integrity, confidentiality, and availability while adhering to the minimum necessary standard in all health information disclosures.

Programme Curriculum

HIPAA Security and Privacy Rule Compliance for Healthcare Training Course

Introduction

The landscape of U.S. healthcare compliance is complex and constantly evolving, placing significant responsibility on Covered Entities (CEs) and Business Associates (BAs) to safeguard patient data. The Health Insurance Portability and Accountability Act (HIPAA), particularly the Privacy and Security Rules, forms the bedrock of health data protection. HIPAA Security and Privacy Rule Compliance for Healthcare Training Course provides a comprehensive and practical guide to achieving and maintaining HIPAA compliance, focusing on the latest regulatory changes, including the HITECH Act and the Omnibus Rule. Participants will learn to navigate the intricate requirements for protecting both paper and electronic Protected Health Information (ePHI), implementing robust administrative, physical, and technical safeguards, and mitigating the rising threat of cybersecurity breaches to avoid substantial civil and criminal penalties.

This training is critically important for fostering a culture of compliance and reinforcing patient trust in an increasingly digitized healthcare ecosystem. It moves beyond theoretical knowledge, offering practical risk management strategies and focusing on real-world enforcement case studies to illustrate the direct consequences of non-compliance. The curriculum is designed to equip key personnel with the necessary expertise to develop, implement, and audit internal policies, manage Business Associate Agreements (BAAs), and execute effective breach notification procedures. Mastering these competencies is no longer optional it is a mandatory and continuous effort to ensure data integrity, confidentiality, and availability while adhering to the minimum necessary standard in all health information disclosures.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Analyze the scope and application of the HIPAA Privacy Rule and Security Rule for comprehensive regulatory compliance.
2. Differentiate between Covered Entities (CEs), Business Associates (BAs), and their respective HITECH Act obligations.
3. Identify and protect all forms of Protected Health Information (PHI) and electronic Protected Health Information (ePHI).
4. Implement required and addressable Administrative Safeguards for effective risk management and workforce training.
5. Establish necessary Physical Safeguards to secure facilities and technology assets against unauthorized access.
6. Deploy mandatory Technical Safeguards, including encryption and robust access controls, for ePHI security.
7. Conduct thorough and repeatable Security Risk Assessments (SRAs) to proactively identify vulnerabilities.
8. Formulate and manage legally sound Business Associate Agreements (BAAs) with third-party vendors.
9. Execute the Breach Notification Rule procedures accurately following a security incident or data breach.
10. Explain and uphold patient Individual Rights regarding access, amendment, and accounting of disclosures.
11. Apply the Minimum Necessary Standard in all uses and disclosures of patient health information.
12. Develop and enforce internal HIPAA policies and procedures and conduct regular internal compliance audits.
13. Mitigate the impact of current cybersecurity threats, such as ransomware and phishing, on ePHI.

Target Audience

1. HIPAA Privacy Officers and Security Officers
2. Compliance Officers and Risk Managers
3. IT Professionals and **Cybersecurity** Staff in Healthcare
4. Healthcare Providers and their staff
5. **Business Associates** and their subcontractors
6. Legal and Audit personnel handling health information
7. Health Plan Administrators and Insurance Professionals
8. Executive Leadership and governing body members

Course Modules

1. HIPAA Fundamentals and Scope

- HIPAA's Titles, the Administrative Simplification provisions, and the core rules.
- Covered Entities, Business Associates, and Organized Health Care Arrangements
- PHI, ePHI, and the Designated Record Set.
- The HITECH Act and the Omnibus Rule updates.
- Case Study: Analysis of a hospital?ÇÖs violation for failing to recognize a third-party vendor as a Business Associate.

2. The HIPAA Privacy Rule: Core Concepts

- Permitted uses and disclosures of PHI
- The Minimum Necessary Rule application and exceptions.
- Requirements for valid patient authorization for non-TPO disclosures.
- Policies and procedures for Privacy Rule compliance.
- Case Study: The $4.3 million fine against a health system for failure to implement minimum necessary policies, resulting in unauthorized disclosures.

3. Patient Rights and Access

- The patient's right of access to their PHI/ePHI.
- Procedures for amendment, restriction, and confidential communication requests.
- The right to an accounting of non-TPO disclosures.
- Creating and distributing the Notice of Privacy Practices.
- Case Study: An OCR settlement for an entity's failure to provide a patient with timely access to their medical records at a reasonable, cost-based fee.

4. Administrative Safeguards: Security Management

- Conducting a comprehensive, organization-wide Security Risk Assessment.
- Developing and applying a robust sanction policy for workforce violations.
- Designating the mandatory Security and Privacy Officials.
- Written security and compliance policies and procedures development.
- Case Study: A clinic?ÇÖs violation and subsequent fine for lacking a current, documented Security Risk Analysis.

5. Administrative Safeguards: Workforce and Access

- Security and Awareness Training requirements and documentation.

- Establishing and controlling authorized user access to ePHI systems.
- Implementing role-based access based on the principle of least privilege.
- Procedures for promptly revoking access upon workforce member separation.
- Case Study: A fine issued to an entity where a terminated employee's access to ePHI was not revoked in a timely manner.

6. Physical Safeguards: Facility and Device Security

- Limiting and monitoring physical access to facilities and data centers.
- Disposal procedures for paper and electronic media containing ePHI.
- Policies for securing workstations, including unattended log-off.
- Inventory and security of Mobile Devices and portable media
- Case Study: A large fine resulting from a data breach caused by unencrypted laptops containing ePHI stolen from a locked facility.

7. Technical Safeguards: Access Control

- Implementing and enforcing strong Multi-Factor Authentication standards.
- The standard for protecting ePHI both at rest and in transit.
- Procedures for securely decrypting ePHI when necessary.
- Establishing emergency access procedures for ePHI systems.
- Case Study: An entity fined after a cyber-attack where they failed to implement data encryption on all endpoints, leading to a breach.

8. Technical Safeguards: Audit and Integrity

- Implementing hardware, software, and procedural mechanisms to record and examine system activity.
- Measures to protect ePHI from improper alteration or destruction.
- Procedures for routine audit log review and Security Event Monitoring.
- Anti-malware and system patch management best practices.
- Case Study: An organization sanctioned for having audit logs enabled but failing to regularly review them, missing signs of a system compromise.

9. Business Associate Agreements

- Determining who qualifies as a Business Associate and Subcontractor BA.
- Mandatory terms and provisions required in a legally compliant BAA.
- Understanding the direct liability of BAs under HIPAA/HITECH.
- Vetting and monitoring vendors who handle PHI
- Case Study: A financial penalty against a CE for operating without a current, signed BAA with a key contractor who was exposed in a breach.

10. The Breach Notification Rule

- What constitutes a reportable Data Breach of unsecured PHI.
- Mandatory reporting timelines for Covered Entities and Business Associates.
- Notification requirements to affected individuals, HHS-OCR, and the media.
- The risk assessment required to determine if notification is necessary.
- Case Study: A settlement involving a CE that failed to notify HHS and affected individuals within the required 60-day window following a major breach.

11. Security Incidents and Disaster Recovery

- Developing and testing an effective Incident Response Plan for security events.
- Implementing a Disaster Recovery and Business Continuity Plan for ePHI availability.
- Requirements for data backup and storage, including regular testing.
- Post-incident analysis to identify root causes and improve defenses.
- Case Study: A CE's fine exacerbated by their poor response and inability to restore PHI following a system failure due to an inadequate contingency plan.

12. HIPAA and Emerging Technologies

- Compliance considerations for remote patient monitoring and virtual visits.
- Securing ePHI in Cloud Computing environments
- Risks and compliance for health-related mobile applications.
- Privacy implications of using Big Data and AI in healthcare.
- Case Study: The privacy risks highlighted in an enforcement action involving a mental health app that impermissibly shared user data with third-party advertisers.

13. Enforcement, Penalties, and Audits

- The role of the Office for Civil Rights in HIPAA enforcement.
- Understanding the four tiers of Civil Penalties and criminal liability.
- Review of notable Resolution Agreements and Corrective Action Plans.
- Preparing for and responding to an OCR compliance audit.
- Case Study: The significant fine levied on a small practice due to willful neglect and a complete disregard for HIPAA rules over an extended period.

14. Special Privacy Topics and State Laws

- HIPAA rules governing patient communication and health-related marketing.
- Techniques and requirements for rendering PHI anonymous
- Understanding when state privacy laws are stricter than HIPAA and must be followed.
- PHI access and privacy rights for adolescents and children.
- Case Study: A clinic?ÇÖs impermissible use of PHI in a patient testimonial for marketing purposes without proper authorization.

15. Developing a Culture of Compliance

- The crucial role of executive management in supporting compliance initiatives.
- Continuous Compliance Monitoring and internal self-audits.
- Creating a non-retaliatory process for reporting suspected violations.
- Integrating HIPAA into a broader GRC strategy.
- Case Study: A success story detailing how a large health plan avoided a major fine by demonstrating a proactive and mature compliance program to the OCR.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.

- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com