Comprehensive HIPAA Security Training (level 2)

The focus of this 2 days classroom HIPAA training program is to better understand the implications of HIPAA security rule and identify critical compliance requirements for your business/client. It helps you better understand how to create a framework for initiating and working towards a blueprint for HIPAA Security compliance and regular audit to avoid violation of regulations.

Our Training includes changes to the HIPAA regulations due to Health Information Technology for Economic and Clinical Health (HITECH) Act which is part of American Recovery and Reinvestment Act of 2009 (ARRA) and Omnibus rule published in 2013. Our HIPAA Instructors are HIPAA consultants who help organizations meet the HIPAA audit checklist requirements issued by the DHHS. Learn from Instructor what your next steps are to meet these newly issued audit requirements by dept. of Health and Human Services' (DHHS) Office of e-Health Standards and Services.

In this training we also explain the relevance of HIPAA to information systems infrastructure and initiatives towards HIPAA security compliance.

This training will prepare you for HIPAA certification of Certified HIPAA Security Expert (CHSE) and Certified HIPAA Privacy Associate (CHPA).

Learning Objectives:

This training helps you better understand HIPAA's Security rule and how to create a framework for initiating and working towards a blueprint for Security compliance and regular audit to avoid violation of regulations. We examine all defined HIPAA security specifications and identify options and solutions available to secure health care entities.

- Understand the changes to HIPAA rules due to ARRA 2009 HITECH Act and 2013 Omnibus Rule final changes.

- Review specific requirements and implementation features within each security category.
- Step through how to plan and prepare for HIPAA compliance. HIPAA is about awareness first, assessment second and finally action focused on gaps identified.
- Understand all required and addressable HIPAA Security implementation specifications.
- Analyze international security standards, NIST, ISO's 27002 and the BS 7799.
- Review core elements of a security policy document for a health care entity.
- Identify core elements of a compliance plan that every health care entity is required to develop for business continuity and disaster recovery.
- Cross walk between NIST, SOX, ISO and HIPAA requirements.

Target Audience

- All key members of a health care provider security compliance team
- All Business Associates required to comply under HITECH
- IT Professionals servicing Healthcare Industry
- Lawyers involved in healthcare
- Computer security technical staff of any organization that retains personal healthcare information
- Senior network engineers
- Database administrators
- Security staff of computer service providers to medical organizations
- Consultants who provide security advice to healthcare organizations
- IT Vendors to healthcare industry

Cost:

Cost for each student is $1500. The cost includes

- HIPAA Compliance Training Manual (worth $450)

[View Classroom Training Schedule]

Course Outline

Day 1 -

HIPAA Fundamentals

- HIPAA Basics: An overview of the Health Insurance Portability and Accountability Act of 1996 (all provisions)
- HIPAA's Administrative Simplification Title: Review of the provisions of the Administrative Simplification Title. This includes transaction and code set standards (administrative transactions), national identifiers, privacy requirements and security requirements.
- HIPAA Penalties: Review of the HIPAA enforcement rule including informal and formal remedies, requirements of covered entities, the role of business associates as agents and enforcement bodies.
- HIPAA-Related Organizations: Discussion of entities/organizations specifically designated as standard maintenance organizations and statutorily defined advisory bodies.
- HIPAA Terminology and Definitions Covered Entity: Review of definitions included in the Administrative Simplification Title related rules (list not inclusive).
    - Covered Entity
    - Health Plan
    - Clearinghouse
    - Health Care Provider
    - Business Associates
    - Trading Partner Agreement
    - Workforce
    - Organized Health Care Arrangement

HIPAA Security Rule Part 1

1. General:

- Threats: General review of threats (real and perceived) prompting Congress to include security requirements in the HIPAA Administrative Simplification Title.

- Definition and Terminology: Review of general definitions of security and specifically how those definitions apply to the rule and what data must be protected by implementation of appropriate security measures
- Security Rules: Detailed review of the security rule, components of the security rule and specific requirements (including reference back to security requirements referenced in the HIPAA Privacy Rule).
    - Categories of Safeguards
    - Implementation Specifications
    - Approach and Philosophy
    - Security Principles
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures, and Documentation Standards

2. Administrative Safeguards: Definition of "administrative safeguards" as they relate to security and the rule. A review of required administrative safeguards and their application within a covered entity and business associate.
    - Administrative Safeguards
    - Security Management Process
    - Assigned Security Responsibility
    - Workforce Security
    - Information Access Management
    - Security Awareness and Training
    - Security Incident Procedures
    - Contingency Plan
    - Evaluation
    - Business Associate Contracts Standard

3. Physical Safeguards: Definition of "physical safeguards" as they relate to security and the rule. A review of required physical safeguards and their application within a covered entity and business associate.
    - Requirements
    - Facility Access Controls
    - Workstation Use
    - Workstation Security
    - Device and Media Controls

- Physical Safeguards Review

4. Technical Safeguards (general): Definition of "technical safeguards" as they relate to security and the rule. A review of required technical safeguards and their application within a covered entity and business associate.
   - Requirements
   - Access Control
   - Audit Controls
   - Integrity
   - Person or Entity Authentication
   - Security Compliance process: Risk Analysis, Vulnerability Assessment, Remediation, Contingency Planning, Audit & Evaluation
   - Transmission Security

5. Technical Safeguards (technical details): A review of required technical safeguards including a more technical review of required or addressable safeguards, implementation and on-going maintenance.
   - TCP/IP Network Infrastructure
   - Firewall Systems
   - Virtual Private Networks (VPNs)
   - Wireless Transmission Security
   - Encryption
   - Overview of Windows XP and Vista Security

Day 2:

HIPAA Security Rule Part 2

1. Digital Signatures & Certificates: A review of the use of higher forms of individual or entity authentication that is quickly becoming a requirement legally and to reduce legal risk.
   - Requirements
   - Digital Signatures
   - Digital Certificates
   - Public Key Infrastructure (PKI)
   - Solution Alternatives
   - Identity theft prevention and HIPAA

2. Security Policy: A review of the requirements to document security program practices and processes in policy and related workforce training requirements. Also a review of required policy maintenance and retention.
   - Risks, Risk Management and Policy Development/Implementation
   - General Security Standards Impact on Policy Development
   - Policy Training Requirements
   - Security Policy Considerations

Enforcement Rule

- Overview: An overview of the rule and rule requirements including entities and individuals the rule applies to.
- Definitions: A review of rule definitions including (not inclusive) what represents a violation, compliance, definition of agent, resolution processes and HHS enforcement powers.
- Informal resolution process: A discussion of what an informal resolution is and what it entails. Also, a review of the rule's emphasis on informal resolution and language allowing such resolution at any phase of violation investigation, penalty assessment and appeal.
- Formal resolution process (i.e., penalties, administrative hearings, appeal process, etc.): A discussion of what would likely trigger a formal resolution process, HHS requirements and authority to investigate, rights and responsibilities of covered entities and resulting actions if civil penalties are levied and paid by the covered entity.
- Compliance audits: A discussion of the authority to conduct compliance audits, current audit activity and prospective audit activity.

Identity Theft Protection Laws

A general review of existing identity theft protection laws and breach notification requirements. Includes specific discussion of California identity theft and medical identity theft protection laws.

American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII

A general overview of Title XIII health information technology (HIT) incentives and requirements provisions. This discussion will focus on an overview of the role of privacy and security in HIT investment provisions and standards development.

American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, Subtitle D - HITECH

1. Privacy Provision Overview: Overview of the privacy provisions included ARRA and the relationship to the HIPAA Administrative Simplification Title provisions.

American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, Subtitle D - HITECH

2. Business Associates – New Requirements: A discussion of business associates' new requirement to statutorily adhere to the provisions of the HIPAA Administrative Simplification Title Privacy and Security Rules. The discussion includes a review of the timeline for compliance and the implications for business associates.

3. National Identity Theft Protection Provisions: A discussion of the requirements of the new identity theft protection provisions, what is considered a breach or inappropriate disclosure, breach notification requirements and entities/individuals covered. Discussion also includes new reporting requirements by entity/individual, HHS and the Federal Trade Commission (FTC).

4. Marketing Prohibitions and Restrictions: An overview of the enhanced restrictions related to the use and disclosure of PHI where the entity or individual is paid for such use and disclosure and stricter prohibitions against using PHI for marketing purposes.

5. Enforcement Provisions: A discussion of the new enforcement provisions, entities/individuals covered and how such enforcement relates to the HIPAA Enforcement Rule and current compliance audits. The discussion also includes a discussion of changes in penalties and the addition of a newly defined criminal act (formerly a civil violation).

6. Reporting Requirements: A discussion of new requirements for the reporting of breaches to HHS and/or the FTC and annual reports relating to compliance, rule violations, breaches, etc. to Congress and the public.

Omnibus Rule of January 2013

- Background
- Breach Notification Rule
- New Limits on Uses and Disclosures of PHI
- Business Associates
- Increased Patient Rights

- Notice of Privacy Practices
- Increased Enforcement

Certified HIPAA Security Expert (CHSE) Online Exam

CHSE is online test and can be taken at any time and from anywhere. Once the Exam is started, it cannot be stopped till it is completed. This is time bound test. You need to pass the 54 questions test (3 questions per chapter, 5 minutes maximum per chapter to answer the questions) with 70% to receive the HIPAA certification of Certified HIPAA Security Expert (CHSE).

This test is for 1 hour 30 minutes. You get 5 minutes per chapter to answer three questions from each chapter.

The passing grade is calculated based on total % of all chapters and NOT individual chapter score. You can fail individual chapters but still pass the test on overall score.

After you pass the test, you will be allowed to print the certification on your own. View sample of certificate http://www.hipaatraining.net/images/CHSE-1.jpg

Continuing Education Requirements After Getting Certified:

Once a year all students will have to go through one hour of update course which will include relevant regulation changes and other OCR/HHS activities on compliance and enforcement.
To maintain your certification, you will continue taking update courses when they are released. You will receive new certificate when your certificate will expire if you have taken all required update courses. You will NOT be required to take any test if you have taken the update courses regularly.

CHSE Testimonials

Testimonials on LinkedIn and Classroom Training Testimonials

Our Clients

View the list of our clients.

Questions?

Bob Mehta: Bob@training-hipaa.net
Phone: 515-865-4591