Comprehensive HIPAA Privacy and Security Training (Level 1 and 2)

The focus of this 4 days HIPAA compliance classroom training program is to better understand the implications of HIPAA legislation and identify critical compliance requirements for your business/client. It helps you better understand HIPAA's Administrative Simplification Act as well as how to create a framework for initiating and working towards a blueprint for Privacy and 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 2013 Omnibus Rule final changes. Our HIPAA Instructors are HIPAA consultants who help organizations meet the HIPAA audit checklist requirements issued by the DHHS. Learn from the Instructor what your next steps are to meet these newly issued audit requirements by the Department 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 & privacy compliance.

This HIPAA compliance training will prepare you for HIPAA certification of Certified HIPAA Privacy Security Expert (CHPSE).

Learning Objectives:

This training helps you better understand HIPAA's Administrative Simplification Act as well as how to create a framework for initiating and working towards a blueprint for Privacy and HIPAA Security compliance and regular audit to avoid violation of regulations. From this training you will learn the following about HIPAA:

- Understand what HIPAA means, how it affects your organization, and what significant changes in policies, procedures & processes within the organization in the handling of patient records.
- Understand the changes to HIPAA rules due to ARRA 2009 HITECH Act and 2013 Omnibus Rule final changes.
- Understand the federal program for meaningful use and incentives for adopting electronic health records.
- Understand the current and potential uses of social media, mobile technologies and big data in health care with the privacy and security risks and challenges.

- Identify the main reasons behind HIPAA, specifically, to provide continuity/portability of health benefits to individuals between jobs; to combat fraud/abuse in health insurance and healthcare delivery; to reduce administrative costs in healthcare; to provide uniform standards for electronic healthcare transactions; and, to ensure security and privacy of patient health information.
- Have an in-depth understanding of HIPAA Security, Privacy and Transaction rule.
- Understand who Business Associates are and what will they have to do to ensure HITECH HIPAA compliance.
- Examine how implementing HIPAA will affect the way healthcare entities organize and staff to achieve and monitor compliance with patient privacy/confidentiality needs.
- Understand the new Enforcement rule.
- 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.
- Review core elements of a security policy document for a health care entity.
- Review specific requirements and implementation features within each security category.
- Identify core elements of a compliance plan that every health care entity is required to develop for business continuity and disaster recovery.
- Analyze international security standards, NIST, ISO's 27002 and the BS 7799.
- Cross walk between NIST, SOX, ISO and HIPAA requirements.

Target Audience

- HIPAA Privacy Officer, HIPAA Security Officer and HIPAA Compliance Officer
- Compliance team for HIPAA Privacy and Security
- IT Professionals servicing Healthcare Industry
- Business Associates employees looking to comply with HITECH & Omnibus requirements
- Healthcare executives & Healthcare service bureau executives
- Chief Information Officers, Managers, Compliance officers, risk managers, Senior network engineers, Database administrators, Clinical physicians and office managers
- Lawyers involved in healthcare
- Pharmaceutical company executives and HIPAA compliance staff
- Insurance executives

- Software Architect, Business Analyst, Team lead of software developers
- Computer security technical staff of any organization that retains personal healthcare information
- Consultants who provide security advice to healthcare organizations

Cost:

Cost for each student is $2700. The cost includes:

- HIPAA Training Manual (worth $450)
- HIPAA Security Policy Templates (sent by e-mail) (worth $495)

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 Transactions, Code Sets and Identifiers

- Transactions
- Impacted Health Care Transactions
- Target Entities
- Scope
- Penalties
- ASCA

ANSI ASC X12 Standard

- Transaction Type 270
- Transaction Type 271
- Transaction Type 276
- Transaction Type 277
- Transaction Type 278 Request and Response
- Transaction Type 820
- Transaction Type 834
- Transaction Type 835
- Transaction Type 837 - Professional
- Transaction Type 837 - Institute
- Transaction Type 837 - Dental

HIPAA Code Sets

- ICD-9-CM Volumes 1 and 2
- CPT-4
- CDT
- ICD-9-CM Volume 3
- NDC
- HCPC

HIPAA National Health Care Identifiers

- Provider Identifier
- Employer Identifier
- Health Plan Identifier

- Individual Identifier

HIPAA Privacy Rule Part 1

- Introduction: Overview of the HIPAA Privacy Rule
  - Who is Impacted (e.g., definition of covered entities, business associates)?
  - Scope (Activities covered by the rule)
  - Exceptions (Specifically included or referenced exceptions that allow use and disclosure of patient/health plan member protected health information (PHI))
  - Timeline (Effective date of the rule, timelines related to certain requirements identified in the privacy rule such as accounting of disclosures, document retention requirements, etc.)
- Key Definitions: Review of key definitions associated with the privacy rule and how they apply to rule application and compliance.
  - IIHI
  - PHI
  - Deidentified Information
  - Use
  - Disclosure
  - Treatment
  - Payment
  - Health Care Operations
- Notice Requirement: Review of the requirements to draft and make available a notice of privacy practices, the content of such notice, revision requirements and availability requirements.
  - Core Elements
  - Changes to a Notice
  - First Interaction
- Authorization versus Consent Requirement: Review the legal definitions of consent and authorization and what they would be used for. Review of the legal requirements related to obtaining authorization, the form of such authorization and content requirements.
  - Definition of “consent”
  - Definition of “authorization”
  - Legal differences between “consent” and “authorization”
  - Core Data Elements and Required Statements
  - Defective Authorizations
  - Revocations
- Key Parties Impacted: A discussion of all entities or individuals directly or indirectly impacted by the rule and why.
- Minimum Necessary: Discussion of the definition of minimum necessary and when it applies to the use and disclosure of PHI (internally and externally)

- Oral and Other Non-electronic Communications: A discussion of what constitutes PHI pursuant to the rule and the related requirements to protect non-electronic PHI, including oral PHI.

HIPAA Privacy Rule Part 1 (continued)

- Health-Related Communications, Fund Raising and Marketing: Review of the requirements related to the use of PHI for communications other than treatment, payment and health care operations. Also, a review of the strict requirements relating to the use of PHI for marketing and fund raising.
- Research: A review of the requirements related to the use of PHI for research including what processes must be followed prior to allowing the use of PHI in research without the patient/health plan member's authorization.

Day 2 -

HIPAA Privacy Rule Part 2

- Policy & Training Requirements: A review of the implied and explicit requirements to develop, implement and maintain privacy policies and procedures and the requirement to provide initial and on-going staff training.
- Preemption Requirements: A review of state law preemption. This includes a discussion regarding when state law may preempt the rule without specific authorization from the US Department of Health and Human Services (HHS) and when authorization is required prior to state law preemption of HIPAA.
- State Privacy Laws: A general review of state privacy laws that preempt HIPAA (categorized as specially protected health information) with specific reference to select California state laws.
- Federal Privacy Law – 42 CFR Pt. 2: A discussion of the more stringent requirements found in 42 CFR Pt. 2 relating to alcohol and chemical dependency
- Statutory/Rule Conflict Resolution: Discussion of how to respond when federal and/or state law conflicts.
- Case Law: A review of general case law that has impacted the application of HIPAA, state privacy laws and impacts legal risks.

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
- Security Services
- Security Mechanisms

HIPAA Security Rule Part 1

2. General (continued):
   - 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

3. 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

Day 3:

4. 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

5. 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

6. 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 Security

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.

Day 4:

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

1. Privacy Provision Overview
2. Business Associates – New Requirements
3. National Identity Theft Protection Provisions
4. Marketing Prohibitions and Restrictions
5. Enforcement Provisions
6. Reporting Requirements

Red Flag Rules

With identity theft and other problems on the increase, additional effort needed to be made to combat this new avenue of fraud against healthcare. With so much information available and in the hands of some many people delivering care, processing payment, and handling the operational and regulatory uses of this information, it was inevitable that healthcare would become a target for exploitation. Changes to the law have helped, and this chapter covers the following topics to better protect your information resources:

- Red Flag Rule Overview
- Definition of "red flags" and how to spot them
- State Identity Theft Protection Laws & ARRA Breach Notification Requirements
- Identity Theft Protection Program Requirements
- Implementation Tips

HIPAA Solutions - Parts 1 & 2

One of the cornerstones of a successful HIPAA security program is the performance of a risk analysis and the creation of a risk management program. These two chapters will walk you through a program of risk analysis and show your how to perform one that focuses on the specific areas that HIPAA requires. You will learn techniques to set a severity scale that is specific to your organization; evaluate and compare risk elements against it; identify and quantify your assets; clarify threats and vulnerabilities that can compromise those assets; develop a strategy to protect against those threats that is both operationally effective and economically efficient. When you complete this section, you will be ready to help get your organization compliant now, and keep it that way into the future.

Meaningful Use

Meaningful Use is one of the hottest current topics in Healthcare. In stages, the Meaningful Use program lays out a series of accomplishments and metrics that over time lead to achieving the objective of securely automating healthcare institutions and providers. In addition to having a program of steps over the years of 2011-2016, the US Government has outlined a financial incentive program to further encourage participation and compliance, and reduce the impact of this pervasive change. This module covers:

- ARRA & Meaningful Use Rule Overview
- Meaningful Use Requirements - Stage 1 & 2
- Privacy & Security Related Measures
- Meeting Core Requirement 15 (HIPAA Compliance)

- Vendor Requirements
- How to Prepare

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

Day 5 – OPTIONAL IF TRAINING IS DONE ONSITE

HIPAA Review

A review of the previous four days of training and Q&A session. Prepare for the certification test.

IT Security Requirements

- Risk Analysis – Inventory generation and prioritization
- Risk Analysis – Identification of threats, vulnerabilities and existing security controls
- Risk Analysis – Risk identification and prioritization
- Risk Analysis – Mitigation strategies and requirements

IT Security Requirements

- Audit – General requirements
- Audit – Annual compliance audit
- Audit – Periodic audits
    - Information systems activity review
    - Login monitoring
    - Audit log generation and review

IT Security Requirements

- Remote access requirements
- Securing and accounting for media and hardware
- Life cycle management requirements (including patch management)

- Data center physical and technical security requirements
- Data leakage prevention

Certified HIPAA Privacy Security Expert (CHPSE) Online Exam

CHPSE 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 78 questions test (3 questions per chapter, 5 minutes per chapter to answer the questions) with 70% to receive the HIPAA certification of Certified HIPAA Privacy Security Expert (CHPSE)

This Online HIPAA Certification test is for 2 hours 10 minutes only. 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/CHPSE-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.

CHPSE Testimonial

Testimonials on LinkedIn and Classroom Training Testimonials

Our Clients

View the list of our clients.