

---

# **HIPAA CERTIFICATIONS**

## **1. Certified HIPAA Privacy Associate (CHPA)**

- Introduction
- Target Audience
- Course Learning Objectives / Course Outline
- HIPAA Certification Test
- Training Options to pursue Certified HIPAA Privacy Associate (CHPA) certification

## **2. Certified HIPAA Privacy Expert (CHPE)**

- Introduction
- Target Audience
- Course Learning Objectives / Course Outline
- HIPAA Certification Test
- Training Options to pursue Certified HIPAA Privacy Expert (CHPE) certification

## **3. Certified HIPAA Security Expert (CHSE)**

- Introduction
- Target Audience
- Course Learning Objectives / Course Outline
- HIPAA Certification Test
- Training Options to pursue Certified HIPAA Security Expert (CHSE) certification

## **4. Certified HIPAA Privacy Security Expert (CHPSE)**

- Introduction
- Target Audience
- Course Learning Objectives / Course Outline
- HIPAA Certification Test
- Training Options to pursue Certified HIPAA Privacy Security Expert (CHPSE) certification

## Certified HIPAA Privacy Associate (CHPA)



### Introduction:

HIPAA basic overview training prepares you for the HIPAA certification exam of Certified HIPAA Privacy Associate (CHPA). This is an ideal course for new hires, students and the common workforce who need a general awareness of HIPAA. It meets all the job role based training requirements as well. Every minute facet a healthcare worker needs to know about HIPAA Privacy and Security is covered in this comprehensive 120 minute course. This course is entirely online and is updated with the latest HIPAA changes under ARRA's HITECH act in 2009.

### Target Audience:

- Lab Technicians
- Pharmacy Staff
- Covered entity general employees
- Business Associates general employees
- Volunteers
- New Hires in Healthcare organization
- Medical students
- Nurse
- Employees who need a general awareness of HIPAA
- Medical Observers

### Course Learning Objectives / Course Outline:

The length of the Course is 2 Hours audio and it covers 82 slides. The topics discussed are:

#### Chapter - HIPAA overview & HIPAA privacy rule

- What is protected health information (phi)

- What information is covered
- What is minimum necessary & when it does not apply
- The notice of privacy practices (npp)
- What is mandatory requirements
- What is use and disclosure of phi
- Required disclosures
- Disclosure of phi for treatment, payment and health care operations (TPO)
- TPO use - Psychotherapy notes
- When authorization not required
- Organizational requirements
- Documentation requirement
- Required policies, procedures & sanctions
- Sanctions
- Individual privacy rights
- When record access can be denied.
- Rights to request amendment
- Privacy breaches
- Business associates & examples
- Other privacy laws, HIPAA & state law

## **Chapter - HIPAA Security Rule – Overview**

- Administrative safeguards overview
  - Security management process
  - Workforce security
  - Information access management
  - Security awareness and training
  - Password management
  - Contingency plan
  - Additional standards
- Physical safeguards standards
  - Facility access controls
  - Device and media controls
  - Other standards
- Technical safeguards standards

- Access control
  - Transmission security
  - Remote Access
  - Other standards
- 
- Breach Notification
  - Organizational requirements
  - Business associates contracts
  - Other arrangements
  - Policy and documentation requirement

## HIPAA Certification Test:

With a view of making things more comprehensible, you are tested on the completion of every chapter. You have to pass the 12 questions test (6 questions per chapter) with 70%. At end of each chapter, you need to answer a set of questions. If you answer them correctly then you can move to the next chapter. You are tested at end of each chapter and NOT at the end of the course. The time duration of this test is 20 minutes only. You get 10 minutes per chapter to answer six questions from each chapter.

You need to clear the Tests of all the respective chapters with 70% marks to receive the HIPAA certification of Certified HIPAA Privacy Associate (CHPA).

CHPA Certification test is only: **\$75** per attempt

[Buy Now](#)

## Training Options to pursue Certified HIPAA Privacy Associate (CHPA) certification:

[Online Anytime training - Certified HIPAA Privacy Associate \(CHPA\)](#)

**\$99** (includes cost for certification exam)

The above comprehensive and constructive training will prepare you for **HIPAA Certification of Certified HIPAA Privacy Associate**

## Certified HIPAA Privacy Expert (CHPE)



### Introduction:

This HIPAA Privacy course will help you to understand the HIPAA law requirement for Privacy rule & basic overview on HIPAA security rule and guide you on how to make your organization HIPAA compliant. All the amendments 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) are adequately included in this course. This training will prepare you comprehensively for HIPAA certification test of Certified HIPAA Privacy Expert (CHPE).

### Target Audience:

- HIPAA Privacy Compliance Officer of covered entity & business associate
- HR Managers
- Head Nurse
- Privacy Compliance Team members of covered entity & business associate
- Lawyers involved in healthcare
- Office manager for clinics
- Pharmaceutical company executives

### Course Learning Objectives / Course Outline:

The length of the Course is 13 Hours audio and it covers 411 slides in all. The topics discussed under informative 12 Chapters are:

---

## Chapter 1 - HIPAA Basics

- Understand the purpose for HIPAA legislation
- Review the HIPAA Administrative Simplification title
- Review non-compliance penalties (civil and criminal)
- Review key organizations associated with administering HIPAA Administrative Simplification provisions
- Review HIPAA-related terminology and definitions

## Chapter 2 - Transactions & Code Sets Overview

- Understand motivation and drivers behind requiring HIPAA standard transactions and code sets

## Chapter 3 - Transactions – ANSI X12 and NCPDP

- Examine the ANSI ASC X12 & NCPDP transactions

## Chapter 4 - Code Sets & National Identifiers

- Understand the code sets approved for use with HIPAA-covered transactions
- Understand national identifiers that have been adopted or may be adopted to identify entities or individuals in HIPAA-covered transactions

## Chapter 5 - HIPAA and Health Data – Security & Privacy Requirements

- Describe how HIPAA relates to health information exchange
- Identify the steps for compliance with the HIPAA Privacy Rule
- Identify the steps for compliance with the HIPAA Security Rule
- Review compliance framework

## Chapter 6 - HIPAA Privacy Rule

- Understand the core requirements, key terms, and concepts of the Privacy Rule

## Chapter 7 - Privacy Rule – Organizational & Individual Relationships, Rights & Responsibilities

- Understand Organizational Relationships
- Explain Individual Privacy Rights

---

## **Chapter 8 - Privacy Rule – Notice of Privacy Practices**

- Understand HIPAA Notice of Privacy Practices (Notice) and Authorization requirements and how to draft and distribute paper and electronic Notices of Privacy Practices and appropriately use an Authorization

## **Chapter 9 - Privacy Rule – Uses and disclosures of PHI**

- Understand the general rules regarding use and disclosure of PHI
- Understand the rules regarding disclosure for treatment, payment, and health care operations
- Understand the rules regarding disclosure for public purposes

## **Chapter 10 - Privacy Rule – Safeguards**

- Understand the necessary safeguards to comply with the HIPAA Privacy Rule security requirements and appropriate privacy practices

## **Chapter 11 - HIPAA Security Rule - Overview**

- Describe the scope of the HIPAA Security Rule.
- Understand threats and attacks health care enterprises are vulnerable to
- Define key security terminology, concepts, and categories
- Describe administrative safeguards implementation specifications.
- Describe physical safeguards implementation specifications.
- Explain technical safeguards implementation specifications.
- Describe organizational requirements.
- Describe the policies and procedures standards, as well as the documentation standards.

## **Chapter 12 - American Recovery & Reinvestment Act**

- American Recovery & Reinvestment Act (ARRA), Title XIII, Subpart D Overview (HITECH)
- Business Associates New Requirements
- Breach Notification Requirements
- New Privacy & Security Requirements
- Increased Enforcement & Penalties
- Federal Reporting & Resource Requirements
- Compliance Tips

## HIPAA Certification Test:

With a view of making things more comprehensible, you are tested on the completion of every chapter. You need to pass the 36 questions test (3 questions per chapter) with 70%. At end of each chapter, you need to answer a set of questions. If you answer them correctly then you can move to the next chapter. You are tested at end of each chapter and NOT at the end of the course. The time duration of this test is 1 Hour only. You get 5 minutes per chapter to answer three questions from each chapter.

You need to clear the Tests of all the respective chapters with 70% marks to receive the HIPAA certification of Certified HIPAA Privacy Expert (CHPE).

Certified HIPAA Privacy Expert (CHPE) certification exam will validate HIPAA Privacy knowledge of employees and consultants at expert level.

CHPE Certification test is only: **\$150** per attempt

[Buy Now](#)

## Training Options to pursue Certified HIPAA Privacy Expert (CHPE) certification:

- [Online Anytime training – Certified HIPAA Privacy Expert \(CHPE\)](#).  
**\$549** per person (includes exam cost)
- [HIPAA Training- Instructor Led for HIPAA Privacy Training \(level 1\)](#)  
This training not required will prepare you for CHPE certification test **\$1500** per person (Does NOT include exam cost)
- [Online HIPAA Training with Instructor for Online HIPAA Privacy Training \(level 1\)](#)  
This training not required will prepare you for CHPE certification test **\$1800** per person (Does NOT include exam cost)

This inclusive course will prepare you for **HIPAA Certification of Certified HIPAA Privacy Expert**.

---

## Certified HIPAA Security Expert (CHSE)



### Introduction:

This HIPAA Security course will help you to understand the HIPAA law requirement for Security rule & basic overview on HIPAA privacy rule and guide you on how to make your organization HIPAA compliant. Our Training also includes changes to the HIPAA regulation due to Health Information Technology for Economic and Clinical Health (HITECH) Act which is part of American Recovery and Reinvestment Act of 2009 (ARRA). This training will prepare you thoroughly for HIPAA certification test of Certified HIPAA Security Expert (CHSE).

### Target Audience:

- HIPAA Security Compliance Officer of covered entity & business associate
- IT Managers
- IT staff
- HIPAA Security Compliance Team members of covered entity & business associate
- IT Consultants involved in healthcare Industry.
- Software developers in Healthcare Industry

### Course Learning Objectives / Course Outline:

The length of the Course is 15 Hours audio it covers 516 slides in all. The topics covered under instructive 17 Chapters are:

#### Chapter 1 - HIPAA Basics

- Understand the purpose for HIPAA legislation
- Review the HIPAA Administrative Simplification title
- Review non-compliance penalties (civil and criminal)

- Review key organizations associated with administering HIPAA Administrative Simplification provisions
- Review HIPAA-related terminology and definitions

## **Chapter 2 - Transactions & Code Sets Overview**

- Understand motivation and drivers behind requiring HIPAA standard transactions and code sets

## **Chapter 3 - Transactions – ANSI X12 and NCPDP**

- Examine the ANSI ASC X12 & NCPDP transactions

## **Chapter 4 - Code Sets & National Identifiers**

- Understand the code sets approved for use with HIPAA-covered transactions
- Understand national identifiers that have been adopted or may be adopted to identify entities or individuals in HIPAA-covered transactions

## **Chapter 5 - HIPAA and Health Data – Security & Privacy Requirements**

- Describe how HIPAA relates to health information exchange
- Identify the steps for compliance with the HIPAA Privacy Rule
- Identify the steps for compliance with the HIPAA Security Rule
- Review compliance framework

## **Chapter 6 - HIPAA Privacy Rule**

- Understand the core requirements, key terms, and concepts of the Privacy Rule

## **Chapter 7 - HIPAA Security Rule - Overview**

- Describe the scope of the HIPAA Security Rule.
- Understand threats and attacks health care enterprises are vulnerable to
- Define key security terminology, concepts, and categories
- Describe administrative safeguards implementation specifications.
- Describe physical safeguards implementation specifications.
- Explain technical safeguards implementation specifications.
- Describe organizational requirements.

- Describe the policies and procedures standards, as well as the documentation standards.

### **Chapter 8 - HIPAA Security Rule – Threats and Technology Options**

- Identify technical/electronic threats to the health care enterprise
- Explain security technology and electronic protections options that may meet Security Rule and Privacy Rule security provisions compliance requirements

### **Chapter 9 - Advanced Administrative Safeguards**

- Describe the requirements for the Security Awareness and Training standard
- Explain the requirements for the Security Incident Procedures standard
- Describe the requirements for the Contingency Plan standard
- Describe the requirements for the Evaluation standard
- Describe the Business Associate Contract and Other Written Arrangements standard

### **Chapter 10 - Physical Safeguards Overview**

- Explain key steps for a physical safeguards assessment based on the HIPAA Privacy Rule

### **Chapter 11 - Advanced Physical Safeguards**

- Describe physical safeguards requirements
- Review facility access control
- Describe workstation use and security standards
- Describe required and example policies, procedures and practices to reasonably ensure appropriate physical safeguards have been implemented

### **Chapter 12 - Physical Safeguards – Data & Media Management**

- Describe requirements for device and media controls

### **Chapter 13 - Security Technical Safeguards Overview**

- Describe the Security Rule defined Technical Safeguards
- Describe the Access Control standard
- Examine the Audit Control standard

- Describe the Integrity standard
- Identify key elements of the Person or Entity Authentication standard
- Review the Transmission Security standard

#### **Chapter 14 - Security Advanced Technical Safeguards**

- Describe the Transmission Security standard
- Examine the Transmission Control Protocol/Internet Protocol (TCP/IP) architecture and its key protocols
- Analyze firewall systems and their role
- Examine Virtual Private Networks (VPNs)
- Describe wireless security requirements
- Identify types of encryption that may be supported by health care entities
- Describe core elements of Windows XP security.

#### **Chapter 15 - Digital Signatures and Certs**

- Explain the requirements of the proposed Security Rule's electronic signature requirements (not included in the final rule)
- Describe a digital signature
- Describe a digital certificate and its relationship to a digital signature
- Examine the role of a Public Key Infrastructure (PKI) in supporting requirements for digital signatures

#### **Chapter 16 - Security Policy and Standards**

- Explain how identifying threats and vulnerabilities impacts risk management strategies and the development of appropriate security policies
- Describe ISO/IEC 27002 and ISO/IEC 27001 standards
- Identify factors that impact the development of an enterprise security policy
- Describe security policy documents that address areas, such as acceptable use policies

#### **Chapter 17 - American Recovery & Reinvestment Act**

- American Recovery & Reinvestment Act (ARRA), Title XIII, Subpart D Overview (HITECH)
- Business Associates New Requirements
- Breach Notification Requirements
- New Privacy & Security Requirements

- Increased Enforcement & Penalties
- Federal Reporting & Resource Requirements
- Compliance Tips

## HIPAA Certification Test:

With a view of making things more comprehensible, you are tested on the completion of every chapter. You need to pass the 51 questions test (3 questions per chapter) with 70%. At end of each chapter, you need to answer a set of questions. If you answer them correctly then you can move to the next chapter. You are tested at end of each chapter and NOT at the end of the course. The time duration of this test is 85 minutes (1 hour 25 minutes). You get 5 minutes per chapter to answer three questions from each chapter.

You need to clear the Tests of all the respective chapters with 70% marks to receive the HIPAA certification of Certified HIPAA Security Expert (CHSE).

CHSE Certification Test only: **\$150** per attempt

[Buy Now](#)

## Training Options to pursue Certified HIPAA Security Expert (CHSE) certification:

- [Online Anytime training - Certified HIPAA Security Expert \(CHSE\)](#).  
**\$549** per person (includes exam cost)
- [HIPAA Training - Instructor Led for HIPAA Security Training \(level 2\)](#)  
This training prepare you for CHSE certification test **\$1500** per person (Does NOT include exam cost)
- [Online HIPAA Training with Instructor for Online HIPAA Security Training \(level 2\)](#)  
This training prepare you for CHSE certification test **\$1800** per person (Does NOT include exam cost)

This constructive and valuable course will prepare you for **HIPAA Certification of Certified HIPAA Security Expert (CHSE)**.

---

## Certified HIPAA Privacy Security Expert (CHPSE)



### Introduction:

This HIPAA Compliance training will help you to understand the HIPAA law requirement for HIPAA Privacy & HIPAA security rule and guide you on how to make your organization HIPAA compliant. All the modifications 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) are adequately included in this course. This training will prepare you comprehensively for HIPAA certification test of Certified HIPAA Privacy Security Expert (CHPSE).

### Target Audience:

- HIPAA Compliance Officer of covered entity & business associate
- Managers
- Healthcare Consultant
- Compliance Team members of covered entity & business associate
- Lawyers involved in healthcare
- Business Analyst for Software
- Software development Project Manager
- Healthcare quality assurance and risk managers

### Course Learning Objectives / Course Outline :

The length of the Course is 22 Hours audio and it covers 767 slides in all. The topics discussed under informative 24 Chapters are:

---

## Chapter 1 - HIPAA Basics

- Understand the purpose for HIPAA legislation
- Review the HIPAA Administrative Simplification title
- Review non-compliance penalties (civil and criminal)
- Review key organizations associated with administering HIPAA Administrative Simplification provisions
- Review HIPAA-related terminology and definitions

## Chapter 2 - Transactions & Code Sets Overview

- Understand motivation and drivers behind requiring HIPAA standard transactions and code sets

## Chapter 3 - Transactions – ANSI X12 and NCPDP

- Examine the ANSI ASC X12 & NCPDP transactions

## Chapter 4 - Code Sets & National Identifiers

- Understand the code sets approved for use with HIPAA-covered transactions
- Understand national identifiers that have been adopted or may be adopted to identify entities or individuals in HIPAA-covered transactions

## Chapter 5 - HIPAA and Health Data – Security & Privacy Requirements

- Describe how HIPAA relates to health information exchange
- Identify the steps for compliance with the HIPAA Privacy Rule
- Identify the steps for compliance with the HIPAA Security Rule
- Review compliance framework

## Chapter 6 - HIPAA Privacy Rule

- Understand the core requirements, key terms, and concepts of the Privacy Rule

## Chapter 7 - Privacy Rule – Organizational & Individual Relationships, Rights & Responsibilities

- Understand Organizational Relationships
- Explain Individual Privacy Rights

---

## **Chapter 8 - Privacy Rule – Notice of Privacy Practices**

- Understand HIPAA Notice of Privacy Practices (Notice) and Authorization requirements and how to draft and distribute paper and electronic Notices of Privacy Practices and appropriately use an Authorization

## **Chapter 9 - Privacy Rule – Uses and disclosures of PHI**

- Understand the general rules regarding use and disclosure of PHI
- Understand the rules regarding disclosure for treatment, payment, and health care operations
- Understand the rules regarding disclosure for public purposes

## **Chapter 10 - Privacy Rule – Safeguards**

- Understand the necessary safeguards to comply with the HIPAA Privacy Rule security requirements and appropriate privacy practices

## **Chapter 11 - HIPAA Security Rule - Overview**

- Describe the scope of the HIPAA Security Rule.
- Understand threats and attacks health care enterprises are vulnerable to
- Define key security terminology, concepts, and categories
- Describe administrative safeguards implementation specifications.
- Describe physical safeguards implementation specifications.
- Explain technical safeguards implementation specifications.
- Describe organizational requirements.
- Describe the policies and procedures standards, as well as the documentation standards.

## **Chapter 12 - HIPAA Security Rule – Threats and Technology Options**

- Identify technical/electronic threats to the health care enterprise
- Explain security technology and electronic protections options that may meet Security Rule and Privacy Rule security provisions compliance requirements

## **Chapter 13 - Advanced Administrative Safeguards**

- Describe the requirements for the Security Awareness and Training standard
- Explain the requirements for the Security Incident Procedures standard

- Describe the requirements for the Contingency Plan standard
- Describe the requirements for the Evaluation standard
- Describe the Business Associate Contract and Other Written Arrangements standard

#### **Chapter 14 - Physical Safeguards Overview**

- Explain key steps for a physical safeguards assessment based on the HIPAA Privacy Rule

#### **Chapter 15 - Advanced Physical Safeguards**

- Describe physical safeguards requirements
- Review facility access control
- Describe workstation use and security standards
- Describe required and example policies, procedures and practices to reasonably ensure appropriate physical safeguards have been implemented

#### **Chapter 16 - Physical Safeguards – Data & Media Management**

- Describe requirements for device and media controls

#### **Chapter 17 - Security Technical Safeguards Overview**

- Describe the Security Rule defined Technical Safeguards
- Describe the Access Control standard
- Examine the Audit Control standard
- Describe the Integrity standard
- Identify key elements of the Person or Entity Authentication standard
- Review the Transmission Security standard

#### **Chapter 18 - Security Advanced Technical Safeguards**

- Describe the Transmission Security standard
- Examine the Transmission Control Protocol/Internet Protocol (TCP/IP) architecture and its key protocols
- Analyze firewall systems and their role
- Examine Virtual Private Networks (VPNs)
- Describe wireless security requirements
- Identify types of encryption that may be supported by health care entities

- Describe core elements of Windows XP security.

## **Chapter 19 - Digital Signatures and Certs**

- Explain the requirements of the proposed Security Rule's electronic signature requirements (not included in the final rule)
- Describe a digital signature
- Describe a digital certificate and its relationship to a digital signature
- Examine the role of a Public Key Infrastructure (PKI) in supporting requirements for digital signatures

## **Chapter 20 - Security Policy and Standards**

- Explain how identifying threats and vulnerabilities impacts risk management strategies and the development of appropriate security policies
- Describe ISO/IEC 27002 and ISO/IEC 27001 standards
- Identify factors that impact the development of an enterprise security policy
- Describe security policy documents that address areas, such as acceptable use policies

## **Chapter 21 - American Recovery & Reinvestment Act**

- American Recovery & Reinvestment Act (ARRA), Title XIII, Subpart D Overview (HITECH)
- Business Associates New Requirements
- Breach Notification Requirements
- New Privacy & Security Requirements
- Increased Enforcement & Penalties
- Federal Reporting & Resource Requirements
- Compliance Tips

## **Chapter 22 - The Red Flag Rules & Healthcare**

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

---

## Chapter 23 - HIPAA Solutions Part 1

- Risk Analysis
- Audit Program – Annual and Periodic

## Chapter 24 - HIPAA Solutions Part 2

- Secure Transmission of PHI
- Policy & Procedure Development
- Training – More Than Just an Annual Workshop
- Disaster Recovery/Emergency Mode Operations Plan

## HIPAA Certification Test:

With a view of making things more comprehensible, you are tested on the completion of every chapter. You need to pass the 72 questions test (3 questions per chapter) with 70%. At end of each chapter, you need to answer a set of questions. If you answer them correctly then you can move to the next chapter. You are tested at end of each chapter and NOT at the end of the course. The time duration of this test is 3 Hours only. You get 5 minutes per chapter to answer three questions from each chapter.

You need to clear the Tests of all the respective chapters with 70% marks to receive the HIPAA certification of Certified HIPAA Privacy Security Expert (CHPSE)

CHPSE Certification Test Only: **\$180** per attempt

[Buy Now](#)

## Training Options to pursue Certified HIPAA Privacy Security Expert (CHPSE) certification:

- [Online Anytime training – Certified HIPAA Privacy Security Expert \(CHPSE\)](#). **\$999** per person (includes exam cost)
- [HIPAA Training- Instructor Led for HIPAA Compliance Training \(level 1 & 2\)](#)  
This training not required will prepare you for CHPSE certification test **\$2700** per person (Does NOT include exam cost)



- 
- [Online HIPAA Training with Instructor for Online HIPAA Compliance Training \(level 1 & 2\)](#)

This training not required will prepare you for CHPSE certification test **\$3200** per person (Does NOT include exam cost)

This inclusive and comprehensive Course will prepare you for **HIPAA certification of Certified HIPAA Privacy Security Expert (CHPSE)**