Help me Select HIPAA Certification

Please use following workflow to help you decide which ideal HIPAA Certification training is for you. If you are need to discuss or clarify your doubts then feel free to call Supremus Group at 515-865-4591 to help you select the right HIPAA Credential for your job role.

START HERE
Do you have exposure to PHI?

No

Do you have physical access to location storing PHI?

No

Will you be working with other employees having access to PHI?

No

Contact your HIPAA privacy officer to decide if you need basic HIPAA training

Yes

Take one hour HIPAA overview training of $25

Yes

Take Basic HIPAA Training of CHPA

Are you going to work on company’s HIPAA compliance project?

No

Are you HIPAA privacy officer OR HIPAA security officer OR HIPAA compliance officer?

Yes

Are you part of company’s core HIPAA compliance team?

No

Are you part of company’s HIPAA security team?

Yes

Are you part of company’s HIPAA privacy team?

No

Take HIPAA privacy training of CHPE

Yes

Take HIPAA security training of CHSE

Take HIPAA compliance training of CHPSE
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
   - CHPA Testimonial

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
   - CHPE Testimonial

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
   - CHSE Testimonial

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
   - CHPSE Testimonial

5. **One Hour Employee Training for:**
   - Healthcare Providers
   - Mental Health Providers
   - Employer Health Plans
   - Business Associates
   - Insurance/Broker Agent
   - Call Center Organization
   - Research Organizations
   - Law Enforcement & Public Safety
6. **Other Courses**
   - The Globally Harmonized System for Hazard Communication Training
   - Healthcare Fraud, Waste and Abuse in Medicare and Medicaid
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 course. This course is entirely online and is updated with the latest HIPAA changes under ARRA’s HITECH act in 2009 are incorporated in the course and Omnibus rule of 2013.

CHPA Course & exam now available in Spanish

Target Audience:
- Covered Entity General Employees
- Healthcare Professional
- Business Associates General Employees
- Interns
- Medical students & Medical observers
- Volunteers
- New Hires in a Healthcare Organization
- Pharmaceutical Sales Representative
- Medical Device Sales Representative
- Insurance Broker
- Lab Technicians
- Pharmacy Staff

Course Learning Objectives/Course Outline:
The length of the Course is almost 1 hour 40 minutes audio and it covers 100 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 are 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
  o Security management process
  o Workforce security
  o Information access management
  o Security awareness and training
  o Password management
  o Contingency plan
  o Additional standards
• Physical safeguards standards
  o Facility access controls
  o Device and media controls
  o Other standards
• Technical safeguards standards
  o Access control
  o Transmission security
  o Remote Access
  o Other standards
• Omnibus Rule
• Breach Notification
• Organizational requirements
• Business associates contracts
• Other arrangements
• Policy and documentation requirement
Training Options to pursue Certified HIPAA Privacy Associate (CHPA) Certification:

**Online Anytime Training – Certified HIPAA Privacy Associate (CHPA).**

$99 (Additional Options to buy: $19.99 full color 56 pages reference manual and $75 unlimited CHPA® exam attempts)

**HIPAA Certification Test:**

With a view of making things more comprehensible, you are tested after you complete the full course. You need to pass the 12 questions test (6 questions per chapter) with 70% to receive the HIPAA certification of Certified HIPAA Privacy Associate (CHPA).

This test is for 20 minutes only. Ten minutes per chapter are allotted to answer six.

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

**Certificate for Continuing Education Credits:**

Students can buy CE credits certificate for this course at the time of registration. You will receive 2 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

**CHPA Testimonials**

LinkedIn  
HIPAATraining.net
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) and Omnibus rule of 2013 are adequately included in this course. This training will prepare you comprehensively for HIPAA certification test of Certified HIPAA Privacy Expert (CHPE).

Target Audience:
- Healthcare Provider & Payer Privacy Compliance Employees
- Privacy Lawyers Involved in Health Care
- Compliance teams for HIPAA Privacy
- HR Staff & Manager
- Privacy Auditors
- Privacy Consultants
- Clinical Physicians and Office Managers
- Head Nurse
- Privacy Instructors

Course Learning Objectives / Course Outline:
The length of the Course is 15 Hours audio and it covers 507 slides in all. The topics discussed under informative 14 Chapters are:

Chapter 1 - HIPAA Basics
- Understand the purpose of 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

Chapter 13 - The Omnibus Rule
Omnibus Rule Background
Breach Notification Rule
New Limits on Uses and Disclosures of PHI
Business Associates
Increased Patient Rights
Notice of Privacy Practices
Increased Enforcement
Update Action Considerations

Chapter 14 - 2017 Annual HIPAA Certification CE Credits
The Year in Review – Breaches and Events
Rules, Issuances, and Issues in 2017
Today: Where Attention is Needed
Tomorrow: What the Future May Hold

Continuing Education (CE) Requirements after Getting Certified:
To maintain certification, the student has to take the update courses when they are released (normally in Jan-March). Students will receive a new certificate when their certificate expires if they are up to date on their CE courses. The student will NOT be required to take any test if you have taken the update courses regularly.

Find More information about CE Courses https://www.hipaatraining.net/continuing-education/

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 15 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

Training Options to pursue Certified HIPAA Privacy Expert (CHPE) certification:
Click on following blue heading to read more about the course.
- **Online Anytime training – Certified HIPAA Privacy Expert (CHPE)**
  $648 (Additional Options to buy: $300 printed manual, $75 CHPE practice test, $250 two hours of Instructor support, $150 unlimited CHPE exam attempts)
• **Instructor-Led Training in Classroom for HIPAA Privacy (level 1)**
  This training will prepare you for CHPE certification test $1500 per person (Includes printed manual & meals during training. Does NOT include exam cost, One attempt for CHPE test: $150, Unlimited attempts: $300)

• **Online Live Instructor-Led Training for HIPAA Privacy (level 1)**
  This training will prepare you for CHPE certification test $1800 per person (Includes printed manual. Does NOT include exam cost, One attempt for CHPE test: $150, Unlimited attempts: $300)

**HIPAA Certification Test:**
With a view of making things more comprehensible, you are tested after you complete the full course. You need to pass the 39 questions test (3 questions per chapter) with 70%. The time duration of this test is 1 hour 5 minutes only.

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

**CHPE Testimonial**
LinkedIn
HIPAATraining.net
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) and Omnibus rule of 2013. This training will prepare you thoroughly for HIPAA certification test of Certified HIPAA Security Expert (CHSE).

Target Audience:
- Healthcare Provider & Payer Security Compliance Employees
- IT Managers
- IT Staff
- Security Auditors
- Security Consultants
- Network Manager and Engineers
- Database Administrators
- Software Developers
- Consultants Who Provide Security Advice To Health Care Organizations
- Security Lawyers involved in Health Care

Course Learning Objectives / Course Outline:
The length of the Course is 17 Hours audio it covers 612 slides in all. The topics covered under instructive 19 Chapters are:

Chapter 1 - HIPAA Basics
- Understand the purpose of 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

Chapter 18 - The Omnibus Rule
• Omnibus Rule Background
• Breach Notification Rule
• New Limits on Uses and Disclosures of PHI
• Business Associates
• Increased Patient Rights
• Notice of Privacy Practices
• Increased Enforcement
• Update Action Considerations

**Chapter 19 - 2017 Annual HIPAA Certification CE Credits**

- The Year in Review – Breaches and Events
- Rules, Issuances, and Issues in 2017
- Today: Where Attention is Needed
- Tomorrow: What the Future May Hold

**Continuing Education (CE) Requirements after Getting Certified:**

To maintain certification, the student has to take the update courses when they are released (normally in Jan-March). Students will receive a new certificate when their certificate expires if they are up to date on their CE courses. The student will NOT be required to take any test if you have taken the update courses regularly.

Find More information about CE Courses [https://www.hipaatraining.net/continuing-education/](https://www.hipaatraining.net/continuing-education/)

**Certificate for Continuing Education Credits:**

Students can buy CE credits certificate for this course at the time of registration. You will receive 17 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

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

Click on following blue heading to read more about the course.

- **Online Anytime training - Certified HIPAA Security Expert (CHSE)**
  - $648 (Additional Options to buy: $300 printed manual, $75 CHSE practice test, $250 two hours of Instructor support, $150 additional CHSE exam attempt)

- **Instructor-Led Training in Classroom for HIPAA Security (level 2)**
  - This training will prepare you for CHSE certification test $1500 per person (Includes printed manual & meals during training. Does NOT include exam cost, One attempt for CHSE test: $150, Unlimited attempts: $300)

- **Online Live Instructor-Led Training for HIPAA Security (level 2)**
  - This training will prepare you for CHSE certification test $1800 per person (Includes printed manual. Does NOT include exam cost, One attempt for CHSE test: $150, Unlimited attempts: $300)
HIPAA Certification Test:
With a view of making things more comprehensible, you are tested after you complete the full course. You need to pass the 54 questions test (3 questions per chapter) with 70%. The time duration of this test is 90 minutes (1 hour 30 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

CHSE Testimonials
LinkedIn     HIPAATraining.net
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) Omnibus rule of 2013 and Electronic Health Records (EHR) & meaningful use incentives 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 Privacy Officer, HIPAA Security Officer, and HIPAA Compliance Officer
- Core Compliance employees
- IT Professionals servicing Healthcare Industry
- Chief Information Officers
- Risk Managers
- Lawyers involved in Healthcare
- Software Architect
- Business Analyst
- Team Lead of Software Developers
- Health Care Quality Assurance and Risk Managers
- Business Associates of Covered Entities
- Project Manager
- IT Auditors
- Senior Consultants

Course Learning Objectives / Course Outline:
The length of the Course is 25 Hours audio and it covers 921 slides in all. The topics discussed under informative 27 Chapters are:

Chapter 1 - HIPAA Basics
- Understand the purpose of 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 Omnibus Rule
  • Omnibus Rule Background
  • Breach Notification Rule
  • New Limits on Uses and Disclosures of PHI
  • Business Associates
  • Increased Patient Rights
  • Notice of Privacy Practices
  • Increased Enforcement
  • Update Action Considerations

Chapter 23 - The Meaningful Use
  • ARRA Overview
  • Meaningful Use Rule Overview
  • Vendor Certification
  • Medicare Incentives
  • EHR Technical and Meaningful Use Requirements
  • Privacy & Security Requirements
  • Proposed Meaningful Use Stage 2 Requirements

Chapter 24 - 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 25 - HIPAA Solutions Part 1
  • Risk Analysis
• Audit Program – Annual and Periodic

Chapter 26 - HIPAA Solutions Part 2
• Secure Transmission of PHI
• Policy & Procedure Development
• Training – More Than Just an Annual Workshop
• Disaster Recovery/Emergency Mode Operations Plan

Chapter 27 - 2017 Annual HIPAA Certification CE Credits
• The Year in Review – Breaches and Events
• Rules, Issuances, and Issues in 2017
• Today: Where Attention is Needed
• Tomorrow: What the Future May Hold

Continuing Education (CE) Requirements after Getting Certified:
To maintain certification, the student has to take the update courses when they are released (normally in Jan-March). Students will receive a new certificate when their certificate expires if they are up to date on their CE courses. The student will NOT be required to take any test if you have taken the update courses regularly.

Find More information about CE Courses [https://www.hipaatraining.net/continuing-education/](https://www.hipaatraining.net/continuing-education/)

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 25 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

Training Options to pursue Certified HIPAA Privacy Security Expert (CHPSE) certification:
Click on following blue heading to read more about the course.

• **Online Anytime training – Certified HIPAA Privacy Security Expert (CHPSE)**
  $1200 (Additional Options to buy: $300 printed manual, $99 CHPSE practice test, $250 two hours of Instructor support, $180 additional CHPSE exam attempt)

• **Instructor-Led Training in Classroom for HIPAA Compliance (level 1 & 2)**
  This training will prepare you for CHPSE certification test $2700 per person (Includes printed manual & meals during training. Does NOT include exam cost, One attempt for CHPSE test: $180, Unlimited attempts: $360)
Online Live Instructor-Led Training for HIPAA Compliance (level 1 & 2)
This training will prepare you for CHPSE certification test $3200 per person
(Includes printed manual. Does NOT include exam cost, One attempt for
CHPSE test: $180, Unlimited attempts: $360)

HIPAA Certification Test:
With a view of making things more comprehensible, you are tested after you complete the full
course. You need to pass the 78 questions test (3 questions per chapter) with 70% marks. The time
duration of this test is 2 Hours 10 minutes only.

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

CHPSE Testimonial
LinkedIn
HIPAATraining.net
One Hour HIPAA Employee Training

Choose Your Version

Healthcare Providers
Mental Health Providers
Employer Health Plans
Business Associates

Insurance/Broker Agent
Call Center Organization
Research Organizations
Law Enforcement & Public Safety

Course Features:

- 24 x 7 access from anywhere for self-paced online courses
- One course for $25 to meet privacy and security awareness training requirement
- Courses created by HIPAA Expert with practical compliance experience and security expert
- Course updated for HITECH, Omnibus rule, meaningful use, and breach notification
- Instantly print or download Nationally Recognized Certificates
- Complete your course in one hour and get certification
- Online course with audio and PowerPoint slides for easy understanding of training
- American Disability Act (ADA) complaint course format and delivery
- 56 pages printed color manual available for purchase
- Online courses compatible with windows, apple, iPad and other tablets
- Complete compliance solution available based on your specific needs
- Group, university and Colleges discounts available
- Unlimited Phone and email Support

ASK FOR VOLUME DISCOUNT FOR MORE THAN 10 EMPLOYEES

HIPAA Training for Healthcare Providers

Audience:
Any single individual who works for an organization that provides preventive, curative, promotional or rehabilitative health care services in a systematic way to patients, people, families or communities.
Examples:
Hospitals, Private Clinics, Doctors, podiatrist, Physicians, Neurosurgeons, Ophthalmologist, Nurses, psychologist, Medical Schools, Plastic Surgeon, Medical Students, Orthopedist, Pediatrician, Medical Office Staff, clinical optometrist, Pharmacies, Dentists, nurse practitioner, Chiropractors, Allergist, Anesthesiologist, Physical Therapists, ENT Specialist, Massage Therapists, Dermatologist, Radiologists, nurse-midwife, Cardiologists, Hospice, Gastroenterologist, Nursing Homes, Gynecologist, General Psychiatrist, Home Health, Gynecologist, Durable Medical Equipment providers, clinical social worker, Audiologist, Gastroenterologist, Psychiatrists, Rheumatologist etc.

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 1 Hour / Course
Format: Online Self-Paced Training
Number of Total Slides: 30
Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 2 Years
License: Single user license cannot be transferred once a login is assigned.

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

HIPAA Training for Mental Health Providers

Audience:
Any single individual who works or will work in future for an organization involved in the direct medical treatment of patients involving mental health.

Examples:
Psychologists, Mental health counselor, Psychiatrists, Addiction counselor, Psychoanalyst, Clinical social workers, Psychiatric nurses, Behavioral services, Psychotherapist, Mental health programs, Family and marriage counselor, Religious counselor, Art therapist, Psychiatric Pharmacists etc.

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 2 Hours / Course
Format: Online Self-Paced Training
HIPAA Training for Employer Health Plans

**Audience:**
Any single individual who works in the HR benefits staff for an organization involved in sponsoring and managing group health plan benefits for its employees.

**Examples:**
HR benefits staff for employers who sponsor group health plans (self-insured and fully insured) for their employees such as medical health plans, dental, vision, flexible spending accounts, etc.

**Course Overview:**
- Slides with Audio: Yes
- Self-Paced: Yes
- Avg Completion Time: 1.5 Hours / Course
- Format: Online Self-Paced Training
- Number of Total Slides: 67

<table>
<thead>
<tr>
<th>COURSE OUTLINE</th>
<th>REGISTER NOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost: $25 per employee</td>
<td></td>
</tr>
</tbody>
</table>

**Certificate for Continuing EducationCredits:**
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.
HIPAA Training for Business Associates

Audience:
Any single individual who works or will work in future for a company that offers services or products to health care entities, health plans, health insurance providers, or other business associates and will have access to protected health information (PHI).

Examples:
Medical couriers, Medical billing, Business processing outsourcing (BPO) provider, Document/record storage, Medical transcription services, Insurance brokers (take course designed for insurance brokers), Document disposal (shredding) companies, Answering services, CPAs, Third party administrator (TPA), Software companies, Patient safety or accreditation organizations, Pharmaceutical representatives, e-prescribing gateways and other HIOs, Medical device manufacturers, Pharmacy benefit managers, Collection agencies, Attorneys, Health information exchanges (HIEs), Actuaries, Marketing services, Cleaning services, Asset recyclers, Researchers (if performing HIPAA functions for a covered entity), Accounting services firm, Auditors, Healthcare consultants, Financial institutions (if engaging in accounts receivable or other functions extending beyond payment processing), Cloud vendors, etc

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 2 Hours / Course
Format: Online Self-Paced Training
Number of Total Slides: 67

Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 2 Years
License: Single user license cannot be transferred once a login is assigned.

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.
HIPAA Training for Insurance/Broker Agent

**Audience:**
Any single individual who works for an organization that provides health insurance brokerage or administration services for employer group health plans.

**Examples:**

**Course Overview:**
- Slides with Audio: Yes
- Self-Paced: Yes
- Avg Completion Time: 1.5 Hours / Course
- Format: Online Self-Paced Training
- Number of Total Slides: 66
- Access: Online Access for 60 Days

**Certificate of Completion:**
- Yes

**Certificate Expiry:**
- 2 Years

**License:**
- Single user license cannot be transferred once a login is assigned.

---

**Cost:** $25 per employee

---

**Certificate for Continuing Education Credits:**
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

---

HIPAA Training for Call Center Organization

**Audience:**
Any single individual who works for an organization that provides preventive, curative, promotional or rehabilitative health care services in a systematic way to patients, people, families or communities.

**Examples:**
The call center is a centralized office used for receiving or transmitting a large volume of requests by telephone. Different types of healthcare related call centers are for: Billing, Collection, Patient communication, Medical insurance, Dental insurance, Vision insurance, medical answering services.
Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 1.5 Hours / Course
Format: Online Self-Paced Training
Number of Total Slides: 63
Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 2 Years
License: Single user license cannot be transferred once a login is assigned.

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

HIPAA Training for Research Organizations and Activities

Audience:
For HIPAA purposes “Research” is defined as any systematic investigation (including research development, testing, and evaluation) that has as its primary purpose the development of, or contribution to, generalizable knowledge. This is intended to cover human subject research involving PHI, not research on data that have been de-identified in accordance with 45 CFR 164.502(d), and 164.514(a)-(c).

Examples:
A university that conducts human subject research projects, an independent research organization, medical schools, Laboratories doing research, pharmaceutical companies and others.

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 1 Hour / Course
Format: Online Self-Paced Training
Number of Total Slides: 42
Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 2 Years
License: Single user license cannot be transferred once a login is assigned.
Cost: $25 per employee

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

HIPAA Training for Law Enforcement and Public Safety Professional

Audience:
Law Enforcement and Public Safety professional is a government employee who is a sworn officer of the city or county or state who acts in an organized manner to enforce the law by prevention, investigation, apprehension, discovering, deterring, rehabilitating or punishing people who violate the rules and norms governing that society.

Examples:
Government employees & contractors working in the fire department, Law enforcement, Emergency medical technicians, Public health officials, Hazardous materials professionals, Public safety communications representatives, Public works officials, Emergency managers, Justice & court employees, Department of corrections, FEMA, FBI, U.S. Marshals and others.

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 1 Hour / Course
Format: Online Self-Paced Training
Number of Total Slides: 30
Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 2 Years
License: Single user license cannot be transferred once a login is assigned.

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.
The Globally Harmonized System for Hazard Communication Training

**Audience:**
Any individual working in Business Associates or Covered Entities.

**Examples:**
Hospitals, Private Clinics, Doctors, podiatrist, Physicians, Neurosurgeons, Ophthalmologist, Nurses, psychologist, Medical Schools, Plastic Surgeon, Medical Students, Orthopedist, Pediatrician, Medical Office Staff, clinical optometrist, Pharmacies, Dentists, nurse practitioner, Chiropractors, etc.

**Course Overview:**
- Slides with Audio: Yes
- Self-Paced: Yes
- Avg Completion Time: 1 Hour / Course
- Format: Online Self-Paced Training
- Number of Total Slides: 53
- Access: Online Access for 60 Days
- Certificate of Completion: Yes
- Certificate Expiry: 1 Year
- License: Single user license cannot be transferred once a login is assigned.

**Certificate for Continuing Education Credits:**
Students can buy CE credits certificate for this course at the time of registration. You will receive 1 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.

---

Healthcare Fraud, Waste and Abuse in Medicare and Medicaid

**Audience:**
All Part C and D first tier, downstream, related entities (FDR), including Medicare Advantage organization (MAO) who administer the Part D drug benefit or provide health care services to Medicare Advantage enrollees.
Examples:
Hospitals, Private Clinics, Doctors, Physicians, Nurses, Medical Schools, Medical Students, Medical Office Staff, Dentists, Chiropractors, Physical Therapists, Massage Therapists, Radiologists, Cardiologists, Hospice, Nursing Homes, Home Health, Durable Medical Equipment providers, etc., Mental Health Providers, Pharmacy Benefit Managers (PBMs), Pharmacies and pharmacists, Medical health plans, dental, vision, flexible spending accounts that work with MA part D programs and Claim Processing Firms.

Course Overview:
Slides with Audio: Yes
Self-Paced: Yes
Avg Completion Time: 1.5 Hours / Course
Format: Online Self-Paced Training
Number of Total Slides: 66
Access: Online Access for 60 Days
Certificate of Completion: Yes
Certificate Expiry: 1 Year
License: Single user license cannot be transferred once a login is assigned.

Certificate for Continuing Education Credits:
Students can buy CE credits certificate for this course at the time of registration. You will receive 1.5 CE credits for this course through Approved Provider of California Board of Registered Nursing after completing the course.