Certified Healthcare IS Security Practitioner

KEY DATA

Course Title: Certified Healthcare Information Systems Security Practitioner

Duration: 4 days

Language: English

Class Format Options:

Instructor-led classroom
Live Online Training

Prerequisites:

- A minimum of 1 year of Healthcare Information Systems

Student Materials:

- Student Workbook
- Key Security Concepts & Definitions Book

Certification Exams:

- Mile2 C)HISSP
- Covers ISC2 HCISSP

CPEs: 32 Hours

WHO SHOULD ATTEND?

- Information System Security Officers
- Privacy Officers
- Health IS Managers
- Risk Managers
- Information Security Managers
- Compliance & Privacy Officers

COURSE OVERVIEW

Thevendor neutral **Certified Healthcare Information Systems Security Practitioner**certification coursecovers the skills and knowledge to implement the best IT Healthcare Practices, as well as, regulatory compliance and standards in the healthcare industry.

Because of growing industry regulations and privacy requirements in the healthcare industry,the **Certified Healthcare Information Systems Security Practitioner** was developed by mile2. The CHISSPs have become vital in managing and protecting healthcare data and are tasked to protect patient information by implementing, managing, and assessing proper IT controls for patient health information integrity.

Healthcare Career

C)SS™ CERTIFIED SECURITY SENTINEL

C)ISSO™ Certified Information Systems Security Officer

C)HISSP*

All Combos Includes:

- Online Video
- Electronic Book (Workbook/Lab guide*)

  *in all Technical classes only
- Exam Prep Questions
- Exam

C)HISSP

mile2
CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Upon completion, the student will be ready to take the Certified Healthcare Information Systems Security Practitioner exam by mile2. In addition, at the end of the CHISSP course, the student will be versed with best practices in the healthcare industry and will be able to establish a framework with current best practices in respects to privacy, regulation and risk management.

EXAM INFORMATION

The **Certified Healthcare Information Systems Security Practitioner**exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

COURSE CONTENT

I. **Intro to Healthcare Industry**
II. **Frameworks and Regulatory Environment**
III. **Healthcare Privacy & Security Policies**
IV. **Information Governance &Risk Assessment**
V. **Information Risk Assessment**
VI. **Third-Party Risk Management**

DETAILED MODULE DESCRIPTION

Module 1: Intro to the Healthcare Industry
- Healthcare Environment
- Third-Party Relationships
- Health Data Management Concepts

Module 2: Regulatory Environment

Applicable Regulations
- International Regulations and Controls
- Internal Practices Compared to New Policies and Procedures
- Compliance Frameworks
- Risk-Based Decisions
- Code of Conduct/Ethics

Module 3: Healthcare Privacy & Security Policies

- Security Objectives/Attributes
- Security Definitions/Concepts
- Privacy Principles
- Disparate Nature of Sensitive Data and Handling Implications

Module 4: Information Governance & Risk Management – How organizations manage information risk through security and privacy governance, risk management lifecycles, and principle risk activities
- Security and Privacy Governance
- Risk Management Methodology
- Information Risk Management Life Cycles
- Risk Management Activities

Module 5: Information Governance &Risk Assessment
- Risk Assessment
- Procedures from within Organization Risk Frameworks
- Risk Assessment Consistent with Role in Organization
- Efforts to Remediate Gaps

Module 6: Third-Party Risk Management
Definition of Third-Parties in Healthcare Context
- Third-Party Management Standards and Practices
- Third-Party Assessments and Audits
- Security/Privacy Events
- Third-Party Connectivity
- Third-Party Requirements

Remediation Efforts