Certified Healthcare IS Security Practitioner

Duration: *4 Day(s)*

Course Overview

The vendor neutral Certified Healthcare Information Systems Security Practitioner certification course covers 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.

Mile2 Accreditations:

1. Accredited by the **NSA CNSS 4011-4016**
2. Is approved and has been placed on Homeland Security's National Initiative for Cyber Security Careers and Studies (**NICCS) training providers** and maps to the **National Cybersecurity Workforce Framework**
3. Preferred cyber certification for the **FBI**

Review this course online at https://www.alta3.com/courses/C)HISSP

Objectives

- Implement IT healthcare best practices and regulatory standards.
- Manage and protect healthcare data integrity.
- Assess and improve IT controls for patient information protection.
- Understand privacy-related IT requirements in the healthcare sector.

Who Should Attend

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

Prerequisites

A minimum of 1 year of Healthcare Information Systems

Course Outline

Module 1: Intro to the Healthcare Industry

1. Healthcare Environment
2. Third-Party Relationships

3. Health Data Management Concepts

Module 2: Regulatory Environment

4. Applicable Regulations
5. International Regulations and Controls
6. Internal Practices Compared to New Policies and Procedures
7. Compliance Frameworks
8. Risk-Based Decisions

Module 3: Healthcare Privacy & Security Policies

9. Security Objectives/Attributes
10. Security Definitions/Concepts
11. Privacy Principles
12. Disparate Nature of Sensitive Data and Handling Implications

Module 4: Information Governance & Risk Management

13. Security and Privacy Governance
14. Risk Management Methodology
15. Information Risk Management Life Cycles
16. Risk Management Activities

Module 5: Information Governance & Risk Assessment

17. Risk Assessment
18. Procedures from within Organization Risk
19. Risk Assessment Consistent with Role in Organization
20. Efforts to Remediate Gaps

Module 6: Third-Party Risk Management

21. Definition of Third-Parties in Healthcare Context
22. Third-Party Management Standards and Practices
23. Third-Party Assessments and Audits
24. Security/Privacy Events
25. Third-Party Connectivity
26. Third-Party Requirements Remediation Efforts