Hewlett Packard Enterprise

Course Datasheet

HCISPP - HealthCare Information Security and Privacy Practitioner

Education Services course product number – H0DU7s
Course length – 5 days

This Official (ISC)² course provides a comprehensive review of healthcare security and privacy concepts and industry best practices, covering the 6 domains of the HCISPP CBK: Healthcare Industry, Regulatory Environment, Privacy and Security in Healthcare, Information Governance and Risk Management, Information Risk Assessment, Third Party Risk Management

Audience

This course is intended for practitioners who have at least 2 years of recent full-time professional work experience in 1 or more of the 6 domains of the HCISPP CBK and are pursuing HCISPP training and certification to validate their ability to implement, manage, or assess the appropriate security and privacy controls for a healthcare organization. The training seminar is ideal for those working in positions such as, but not limited to:

- Compliance officer
- Information security manager
- Privacy officer
- Compliance auditor
- Risk analyst
- Medical records supervisor
- Information technology manager
- Privacy and security consultant
- Health information manager
- Practice manager

Course Description

In this course you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

Course Objectives

c04755694, Created July 2015; Updated January 2016, Rev. 1
H0DU7s A.00

- Conceptualize the diversity in the healthcare industry. In order to achieve this, learners will gain knowledge of the diverse types of healthcare organizations, types of technologies, how information and data flows and is managed, how data is exchanged, and the levels of protection required for that data.
- Identify and describe the relevant legal and regulatory requirements regarding healthcare information. These requirements are necessary in order to ensure that the organizations policies and procedures are in compliance and that all trans-border data exchange procedures are followed.
- Describe security and privacy concept principals as they relate to the Healthcare industry. Learners will be able to understand the relationship of security and privacy, and how to manage and handle all information requiring data protection in the healthcare industry.
- Identify how organizations manage information risk, and what security and privacy governance means for that information. The learners will be introduced to basic risk management methods and lifecycles, and the activities that support these concepts.
- Describe risk assessment, and the risk assessment practices and procedures for an organization.
- Identify concepts for managing third-party relationships. Learners will gain knowledge regarding concepts pertaining to their use of information, any additional security and privacy assurances, third-party assessments, third-party security and privacy events, and recognize the mitigation process of third-party risks.

Benefits to you

This course helps candidates review and refresh their healthcare information security and privacy knowledge and help identify areas they need to study for the HCISPP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Detailed Course Outline

This course provides a comprehensive review of information security concepts and industry best practices, covering the following 6 domains of the HCISPP CBK:

- Domain 1: Healthcare Industry
  - Understand the Healthcare Environment
  - Understand Third-Party Relationships
  - Understand Foundational Health Data Management Concepts

- Domain 2: Regulatory Environment
  - Identify Applicable Regulations
  - Understand International Regulations and Controls
  - Compare Internal Practices Against New Policies and Procedures
  - Understand Compliance Frameworks (e.g., ISO, NIST, Common Criteria, IG Toolkit, Generally Accepted Privacy Principles [GAPP])
  - Understand Responses for Risk-Based Decision
  - Understand and Comply with Code of Conduct/Ethics in a Healthcare Information Environment

- Domain 3: Privacy & Security in Healthcare
  - Understand Security Objectives / Attributes
  - Understand General Security Definitions/ Concepts
  - Understand General Privacy Principles (e.g., OECD Privacy Principles, GAPP, PIPEDA, UK Data Protection Act 1998)
  - Understand the Relationship Between Privacy and Security
  - Understand the Disparate Nature of Sensitive Data and Handling Implications

- Domain 4: Information Governance and Risk Management
  - Understand Security and Privacy Governance
  - Understand Basic Risk Management Methodology
  - Understand Information Risk Management Lifecycles (e.g., NIST, CMS, ISO)
  - Risk Management Activities
  - Participate in Risk Management Activities

- Domain 5: Information Risk Assessment
  - Understand Risk Assessment
  - Identify Control Assessment Procedures From Within Organization Risk Frameworks
  - Participate in Risk Assessment Consistent with Role in Organization
  - Participate in Efforts to Remediate Gaps

- Domain 6: Third Party Risk Management
  - Understand the Definition of Third Parties in Healthcare Context
  - Maintain a List of Third-Party Organizations
  - Apply Third-Party Management Standards and Practices for Engage in Third Parties Based Upon the Relationship With the Organization
  - Determine When Third-Party Assessment Is Required
  - Support Third-Party Assessments and Audits
  - Respond to Notifications of Security/Privacy Events
  - Support Establishment of Third-Party Connectivity
  - Promote Awareness of the Third-Party Requirements (Internally and Externally)
  - Participate in Remediation Efforts
  - Respond to Third-Party Requests Regarding Privacy/Security Events

c04755694, Created July 2015; Updated January 2016, Rev. 1
H0DU7s A.00