HCISPP - HealthCare Information Security and Privacy Practitioner

The HealthCare Information Security and Privacy Practitioner (HCISPP) is the ideal certification for those with the core knowledge and experience needed to implement, manage or assess the appropriate security and privacy controls of a healthcare organization. HCISPP provides confirmation of a practitioner's knowledge of best practices and techniques to protect organizations and sensitive data against emerging threats and breaches.

The broad spectrum of topics included in the HCISPP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security.

Successful candidates are competent in the following seven domains:

- Healthcare Industry
- Information Governance in Healthcare
- Information Technologies in Healthcare
- Regulatory and Standards Environment
- Privacy and Security in Healthcare
- Risk Management and Risk Assessment
- Third-Party Risk Management

Who Should Attend

The HCISPP is ideal for information security professionals charged with guarding protected health information (PHI), including those in the following positions:

- 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

Candidates must have a minimum of two years cumulative paid work experience in one or more knowledge areas of the HCISPP Common Body of Knowledge (CBK) that includes security, compliance and privacy. Legal experience may be substituted for compliance and information management experience may be substituted for privacy. Of the two years of experience, one of those years must be in the healthcare industry. A candidate that doesn't have the required experience to become a HCISPP may become an Associate of (ISC)² by successfully passing the HCISPP examination. The Associate of (ISC)² will then have three years to earn the two years of required experience. You can learn more about HCISPP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/HCISPP/experiencerequirements.

Course Agenda

- Domain 1: Healthcare Industry
- Domain 2: Information Governance in Healthcare
- Domain 3: Information Technologies in Healthcare
- Domain 4: Regulatory and Standards Environment
- Domain 5: Privacy and Security in Healthcare
- Domain 6: Risk Management and Risk Assessment
- Domain 7: Third-Party Risk Management

Course Objectives

After completing this course, the student will be able to:

- Understand the Healthcare Environment Components
- Understand Foundational Health Data Management Concepts
- Understand how to protect assets of the organization as they go through their lifecycle
- Identify Information Governance Roles and Responsibilities
- Align Information Security and Privacy Policies, Standards and Procedures
- Understand and Comply with Code of Conduct/Ethics in a Healthcare Information Environment
- Understand the Impact of Healthcare Information Technologies on Privacy and Security
- Identify Regulatory Requirements including Legal Issues that Pertain to Information Security and Privacy for Healthcare Organizations, Data Breach Regulations, Jurisdiction Implications, Protected Personal and Health Information (e.g., Personally Identifiable Information (PII), Personal Health nformation (PHI))
- Recognize Regulations and Controls of Various Countries
- Understand Information Risk Management Framework (RMF) (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))
- Identify Control Assessment Procedures Utilizing Organization Risk Frameworks
- Participate in Risk Assessment Consistent with the Role in Organization
- Utilize Controls to Remediate Risk (e.g., preventative, detective, corrective)
- Apply Management Standards and Practices for Engaging Third-Parties
- Understand the Definition of Third-Parties in Healthcare Context
- Determine When a Third-Party Assessment Is Required – Organizational Standards and Triggers of a Third-Party Assessment