HCISPP®

HealthCare Information Security and Privacy Practitioner

Certification **Exam Outline**

Effective Date: September 1, 2019

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About HCISPP

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

Experience Requirements

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/experience-requirements.

Accreditation

HCISPP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the HCISPP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the HCISPP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing healthcare information security and privacy practitioners.

HCISPP Examination Information

Length of exam	3 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

HCISPP Examination Weights

Domains	Weight
1. Healthcare Industry	12%
2. Information Governance in Healthcare	5%
3. Information Technologies in Healthcare	8%
4. Regulatory and Standards Environment	15%
5. Privacy and Security in Healthcare	25%
6. Risk Management and Risk Assessment	20%
7. Third-Party Risk Management	15%
Total:	**100%**

Domain 1: Healthcare Industry

1.1 Understand the Healthcare Environment Components

- Types of Organizations in the Healthcare Sector (e.g., providers, pharma, payers)
- Health Insurance (e.g., claims processing, payment models, health exchanges, clearing houses)
- Coding (e.g., Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT), International Classification of Diseases (ICD) 10)
- Revenue Cycle (i.e., billing, payment, reimbursement)
- Workflow Management
- Regulatory Environment
- Public Health Reporting
- Clinical Research (e.g., processes)
- Healthcare Records Management

1.2 Understand Third-Party Relationships

- Vendors
- Business Partners
- Regulators
- Other Third-Party Relationships

1.3 Understand Foundational Health Data Management Concepts

- Information Flow and Life Cycle in the Healthcare Environments
- Health Data Characterization (e.g., classification, taxonomy, analytics)
- Data Interoperability and Exchange (e.g., Health Level 7 (HL7), International Health Exchange (IHE), Digital Imaging and Communications in Medicine (DICOM))
- Legal Medical Records

Domain 2:
Information Governance in Healthcare

2.1 Understand Information Governance Frameworks

» Security Governance (e.g., charters, roles, responsibilities)
» Privacy Governance (e.g., charters, roles, responsibilities)

2.2 Identify Information Governance Roles and Responsibilities

2.3 Align Information Security and Privacy Policies, Standards and Procedures

» Policies
» Standards
» Processes and Procedures

2.4 Understand and Comply with Code of Conduct/Ethics in a Healthcare Information Environment

» Organizational Code of Ethics
» (ISC)² Code of Ethics

Domain 3:
Information Technologies in Healthcare

3.1 Understand the Impact of Healthcare Information Technologies on Privacy and Security

- Increased Exposure Affecting Confidentiality, Integrity and Availability (e.g., threat landscape)
- Oversight and Regulatory Challenges
- Interoperability
- Information Technologies

3.2 Understand Data Life Cycle Management (e.g., create, store, use, share, archive, destroy)

3.3 Understand Third-Party Connectivity

- Trust Models for Third-Party Interconnections
- Technical Standards (e.g., physical, logical, network connectivity)
- Connection Agreements (e.g., Memorandum of Understanding (MOU), Interconnection Security Agreements (ISAs))

Domain 4:
Regulatory and Standards Environment

4.1 Identify Regulatory Requirements

- Legal Issues that Pertain to Information Security and Privacy for Healthcare Organizations
- Data Breach Regulations
- Protected Personal and Health Information (e.g., Personally Identifiable Information (PII), Personal Health Information (PHI))
- Jurisdiction Implications
- Data Subjects
- Research

4.2 Recognize Regulations and Controls of Various Countries

- Treaties
- Laws and Regulations (e.g., European Union (EU) Data Protection Directive, Health Insurance Portability and Accountability Act /Health Information Technology for Economic and Clinical Health (HIPAA/HITECH), General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA))

4.3 Understand Compliance Frameworks

- Privacy Frameworks (e.g., Organization for Economic Cooperation and Development (OECD) Privacy principles, Asia-Pacific Economic Cooperation (APEC), Generally Accepted Privacy Principles (GAPP))
- Security Frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Common Criteria (CC))

Domain 5:
Privacy and Security in Healthcare

5.1 Understand Security Objectives/Attributes

- Confidentiality
- Integrity
- Availability

5.2 Understand General Security Definitions and Concepts

- Identity and Access Management (IAM)
- Data Encryption
- Training and Awareness
- Logging, Monitoring and Auditing
- Vulnerability Management
- Segregation of Duties
- Least Privilege (Need to Know)
- Business Continuity (BC)
- Disaster Recovery (DR)
- System Backup and Recovery

5.3 Understand General Privacy Definitions and Concepts

- Consent/Choice
- Limited Collection/Legitimate Purpose/Purpose Specification
- Disclosure Limitation/Transfer to Third-Parties/ Trans-border Concerns
- Access Limitation
- Accuracy, Completeness and Quality
- Management, Designation of Privacy Officer, Supervisor Re-authority, Processing Authorization and Accountability
- Training and Awareness
- Transparency and Openness (e.g., notice of privacy practices)
- Proportionality, Use and Disclosure, and Use Limitation
- Access and Individual Participation
- Notice and Purpose Specification
- Events, Incidents and Breaches

5.4 Understand the Relationship Between Privacy and Security

- Dependency
- Integration

5.5 Understand Sensitive Data and Handling

- Sensitivity Mitigation (e.g., de-identification, anonymization)
- Categories of Sensitive Data (e.g., behavioral health)

Domain 6:
Risk Management and Risk Assessment

6.1 Understand Enterprise Risk Management

- Information Asset Identification
- Asset Valuation
- Exposure
- Likelihood
- Impact
- Threats
- Vulnerability
- Risk
- Controls
- Residual Risk
- Acceptance

6.2 Understand Information Risk Management Framework (RMF) (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))

6.3 Understand Risk Management Process

- Definition
- Approach (e.g., qualitative, quantitative)
- Intent
- Life Cycle/Continuous Monitoring
- Tools/Resources/Techniques
- Desired Outcomes
- Role of Internal and External Audit/Assessment

6.4 Identify Control Assessment Procedures Utilizing Organization Risk Frameworks

6.5 Participate in Risk Assessment Consistent with the Role in Organization

- Information Gathering
- Risk Assessment Estimated Timeline
- Gap Analysis

- Mitigating Actions
- Avoidance
- Transfer
- Acceptance
- Communications and Reporting

6.6 Understand Risk Response (e.g., corrective action plan)

6.7 Utilize Controls to Remediate Risk (e.g., preventative, detective, corrective)

- Administrative
- Physical
- Technical

6.8 Participate in Continuous Monitoring

Domain 7:
Third-Party Risk Mangament

7.1 Understand the Definition of Third-Parties in Healthcare Context

7.2 Maintain a List of Third-Party Organizations

- Third-Party Role/Relationship with the Organization
- Health Information Use (e.g., processing, storage, transmission)

7.3 Apply Management Standards and Practices for Engaging Third-Parties

- Relationship Management

7.4 Determine When a Third-Party Assessment Is Required

- Organizational Standards
- Triggers of a Third-Party Assessment

7.5 Support Third-Party Assessments and Audits

- Information Asset Protection Controls
- Compliance with Information Asset Protection Controls
- Communication of Results

7.6 Participate in Third-Party Remediation Efforts

- Risk Management Activities
- Risk Treatment Identification
- Corrective Action Plans
- Compliance Activities Documentation

7.7 Respond to Notifications of Security/Privacy Events

- Internal Processes for Incident Response
- Relationship Between Organization and Third-Party Incident Response
- Breach Recognition, Notification and Initial Response

7.8 Respond to Third-Party Requests Regarding Privacy/Security Events

- Organizational Breach Notification Rules
- Organizational Information Dissemination Policies and Standards
- Risk Assessment Activities
- Chain of Custody Principles

7.9 Promote Awareness of Third-Party Requirements

- Information Flow Mapping and Scope
- Data Sensitivity and Classification
- Privacy and Security Requirements
- Risks Associated with Third-Parties