ISC2 HCISPP

ISC2 HCISPP Certification Questions & Answers

Exam Summary – Syllabus –Questions

HCISPP

ISC2 Certified HealthCare Information Security and Privacy Practitioner (HCISPP)

125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your HCISPP Certification Well:

The HCISPP is best suitable for candidates who want to gain knowledge in the ISC2 Cybersecurity. Before you start your HCISPP preparation you may struggle to get all the crucial HCISPP materials like HCISPP syllabus, sample questions, study guide.

But don't worry the HCISPP PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the HCISPP syllabus?
- How many questions are there in the HCISPP exam?
- Which Practice test would help me to pass the HCISPP exam at the first attempt?

Passing the HCISPP exam makes you ISC2 Certified HealthCare Information Security and Privacy Practitioner (HCISPP). Having the HCISPP certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISC2 HCISPP Certification Details:

Exam Name	ISC2 Certified HealthCare Information Security and Privacy Practitioner (HCISPP)
Exam Code	HCISPP
Exam Price	$599 (USD)
Duration	180 mins
Number of Questions	125
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 HCISPP Sample Questions**
Practice Exam	**ISC2 HCISPP Certification Practice Exam**

HCISPP Syllabus:

Topic	Details
Healthcare Industry (12%)	
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
Understand Third-Party Relationships	- Vendors - Business Partners - Regulators - Other Third-Party Relationships
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
Information Governance in Healthcare (5%)	
Understand Information Governance Frameworks	- Security Governance (e.g., charters, roles, responsibilities) - Privacy Governance (e.g., charters, roles, responsibilities)
Identify Information Governance Roles and Responsibilities	

Topic	Details
Align Information Security and Privacy Policies, Standards and Procedures	- Policies - Standards - Processes and Procedures
Understand and Comply with Code of Conduct/Ethics in a Healthcare Information Environment	- Organizational Code of Ethics - (ISC)² Code of Ethics
Information Technologies in Healthcare (8%)	
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
Understand Data Life Cycle Management (e.g., create, store, use, share, archive, destroy)	
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))
Regulatory and Standards Environment (15%)	
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
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

Topic	Details
	Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA))
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))
Privacy and Security in Healthcare (25%)	
Understand Security Objectives/Attributes	- Confidentiality - Integrity - Availability
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
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

Topic	Details
Understand the Relationship Between Privacy and Security	- Dependency - Integration
Understand Sensitive Data and Handling	- Sensitivity Mitigation (e.g., de-identification, anonymization) - Categories of Sensitive Data (e.g., behavioral health)
Risk Management and Risk Assessment (20%)	
Understand Enterprise Risk Management	- Information Asset Identification - Asset Valuation - Exposure - Likelihood - Impact - Threats - Vulnerability - Risk - Controls - Residual Risk - Acceptance
Understand Information Risk Management Framework (RMF) (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))	
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
Identify Control Assessment Procedures Utilizing Organization Risk Frameworks	
Participate in Risk Assessment Consistent with the Role in Organization	- Information Gathering - Risk Assessment Estimated Timeline - Gap Analysis
Understand Risk Response (e.g., corrective action plan)	- Mitigating Actions - Avoidance

Topic	Details
	- Transfer - Acceptance - Communications and Reporting
Utilize Controls to Remediate Risk (e.g., preventative, detective, corrective)	- Administrative - Physical - Technical
Participate in Continuous Monitoring	
Third-Party Risk Management (15%)	
Understand the Definition of Third-Parties in Healthcare Context	
Maintain a List of Third-Party Organizations	- Third-Party Role/Relationship with the Organization - Health Information Use (e.g., processing, storage, transmission)
Apply Management Standards and Practices for Engaging Third-Parties	- Relationship Management
Determine When a Third-Party Assessment Is Required	- Organizational Standards - Triggers of a Third-Party Assessment
Support Third-Party Assessments and Audits	- Information Asset Protection Controls - Compliance with Information Asset Protection Controls - Communication of Results
Participate in Third-Party Remediation Efforts	- Risk Management Activities - Risk Treatment Identification - Corrective Action Plans - Compliance Activities Documentation
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
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
Promote Awareness of Third-Party Requirements	- Information Flow Mapping and Scope - Data Sensitivity and Classification - Privacy and Security Requirements - Risks Associated with Third-Parties

ISC2 HCISPP Sample Questions:

Question: 1

You are provided a network vulnerability scan of the hospital network. There are numerous critical unpatched vulnerabilities on many of the devices.

You work with the person who runs the centralized vulnerability patching team to develop a remediation approach that includes automated security patching of systems.

Which of these steps would you take next?

a) Contact system owners to advise them of the updates.
b) Schedule the remediation patching after clinical hours.
c) Exclude medical devices from the updates.
d) Quarantine vulnerable systems per policy.

Answer: c

Question: 2

At what stage of information lifecycle management are you most likely to have a data breach?

a) Create
b) Store
c) Use
d) Dispose

Answer: d

Question: 3

To protect health information in an e-mail sent to a colleague, which would be a proper security control?

a) Logical controls
b) Strong authentication
c) Encryption
d) Least privilege

Answer: c

Question: 4

How does the U.S. HIPAA privacy and U.S. HIPAA security rule differ?

a) No difference exists; they mandate the same requirements
b) The privacy rule applies to electronic transmissions while the security rule applies to physical and verbal matters.
c) The security rule applies to electronic transmissions while the privacy rule applies to physical and verbal matters
d) The privacy rule contradicts the security rule regarding electronic health records

Answer: c

Question: 5

You receive an overnight package to your data center. The invoice describes an encrypted hard drive containing contents of a physician’s office that is part of your healthcare network. There are directions for you to degauss the media and transfer it to the radiology department.

Which phase in data lifecycle management would you consider the data?

a) Archive
b) Store
c) Share
d) Destroy

Answer: d

Question: 6

A good sanctions policy will contain which two basic components?

a) Names of person responsible and person reporting
b) Alternative punishments considered and precedents
c) Type of offense and the type of punishment
d) Amount of fines allowed by law and criminal penalties prescribed

Answer: c

Question: 7

Which of the following is a set of documents that outlines expectations between two organizations to address items such as technical specifications and configuration responsibilities for interconnection?

a) SLA
b) MOU
c) BAA
d) ISA

Answer: d

Question: 8

A security management process is BEST described by which set of controls?

a) Administrative / managerial
b) Operational / physical
c) Technical
d) Detective

Answer: a

Question: 9

Which of the following would BEST help a HCISPP determine if a third party has met an external attestation for information security or privacy?

a) ISO or SSAE No. 16 certifications
b) Length of time vendor has been in business
c) Financial soundness
d) Past performance reviews

Answer: a

Question: 10

Which risk management framework specifically tailors its approach to healthcare?

a) ISO/IEC 27001
b) HITRUST
c) NIST RMF
d) Common Criteria

Answer: b

Study Guide to Crack ISC2 HCISPP Exam:

- Getting details of the HCISPP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the HCISPP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISC2 provided training for HCISPP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the HCISPP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on HCISPP practice tests is must. Continuous practice will make you an expert in all syllabus areas.