
HealthCare Information Security
and Privacy Practitioner

# HCISPP℠

# Candidate Information Bulletin

(Exam Outline)

Effective Date: November 2013

(ISC)²

**Non-Discrimination**

ISC)² does not discriminate candidates based on their nationality, gender, religion, race, ethnicity, sexual orientation, age and disability. For further information on (ISC)²'s non-discrimination policy, please visit https://www.isc2.org/legal-info-policies.aspx.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

The HealthCare Information Security and Privacy Practitioner (HCISPP) are individuals who implement, manage, or assess security and privacy controls that address the unique data protection needs of healthcare information.

This Candidate Information Bulletin provides the following:

- Exam blueprint provides outlines of major topics and sub- topics within the HCISPP domains,
- Suggested reference list,
- Description of the format of the items on the exam, and
- Basic registration/administration policies

Candidates **must meet** the following requirements prior to taking the HCISPP examination:

- Submit the examination fee
- A candidate is required to have a minimum of two years of cumulative paid full-time work experience in one knowledge area of the credential that includes security, compliance & privacy:
  - legal experience may be substituted for compliance
  - information management experience may be substituted for privacy

  One year of the two-year cumulative paid full-time experience must be in the healthcare industry.
- Attest to the truth of his or her assertions regarding professional experience, and legally commit to abide by the (ISC)² Code of Ethics (Section 3).
- Before candidates are allowed to take the test at testing centers, they must respond "yes" or "No" to the following four questions regarding criminal history and related background:

  1. Have you ever been convicted of a felony; a misdemeanor involving a computer crime, dishonesty, or repeat offenses; or a Court Martial in military service, or is there a felony charge, indictment, or information now pending against you? (Omit minor traffic violations and offenses prosecuted in juvenile court).
  2. Have you ever had a professional license, certification, membership or registration revoked, or have you ever been censured or disciplined by any professional organization or government agency?
  3. Have you ever been involved, or publicly identified, with criminal hackers or hacking?
  4. Have you ever been known by any other name, alias, or pseudonym? (You need not include user identities or screen names with which you were publicly identified).



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

HCISPP professional experience includes but is not limited to:

| | |
|---|---|
| Applications Security Personnel | Information Risk Owner |
| Attorney/Compliance Manager | Information Security Manager |
| Bioinformatics Developer | Internal Audit Personnel |
| Clinical Engineer/ Medical Device Manager | Investigator |
| Clinical Informatics Team | Lead Clinical Data Guardian (UK) |
| Clinical Researcher Coordinator | Medical Information Process Designer |
| Compliance Personnel | Medical Records Supervisor |
| Computer Incident Response Team (CIRT) Engineer | Practice Manager |
| CSO/CISO/CIO/CPO | Regional Extension Center Implementation Specialist (US) |
| Data Loss Prevention Analyst | Release Information Specialist |
| Data Protection Officer | Risk Analyst |
| Discovery/ e-Discovery Officer | Security Governance and Privacy Analyst |
| EHR Design and Implementation Specialist | Security Operations Personnel |
| Enterprise Architect | Security, Risk, and Privacy Consultant |
| Health Information Management Specialist | Senior Information Risk Owner (UK) |
| Health IT Auditor/Investigator | Wellness Program Director |
| Identity and Access Managers | |



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

**HCISPP Professional Frequently Used Acronyms:**

- Canadian Institute for Health Information (CIHI)
- Centers for Medicare & Medicaid Services (CMS)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- CMS Federal Information Security Management Act (FISMA) Controls Tracking System (CFACTS)
- Common Security Framework (CSF)
- Corrective Action Plan (CAP)
- European Union Data Protection (EU DP)
- eXpedited Life Cycle (XLC)
- Federal Rules of Civil Procedure (FRCP)
- File Integrity Monitoring (FIM)
- Health Information Exchange (HIE)
- Health Information Trust Alliance (HITRUST)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- Host-based Intrusion Detection System (HIDS)
- Information Governance (IG)
- Information Security Governance (ISG)
- International Classification of Diseases (ICD)
- International Standards Organization (ISO) Public Key Cryptography (PKC)
- Notice of Privacy Practices (NPP)
- Personal Computer (PC)
- Personal Health Record (PHR)
- Picture Archiving and Communications System (PACS)
- Security Test Plan (STP)
- System Security Plan (SSP)
- Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT)
- The Joint Commission (TJC)
- United Kingdom (UK)
- United States (US)
- Vehicle Identification Number (VIN)



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 1: Healthcare Industry

## Overview

The healthcare industry is exceedingly diverse, consisting of various organizations such as small physician practices and large health systems, laboratories, pharmaceuticals, biomedical companies, private and public payers, regulators and public health organizations, all of which rely on the efficient and effective exchange of patient-related information.

HCISPP candidates should be able to understand the diversity of the healthcare industry, the types of technologies and flows of information that require various levels of protection, and how healthcare information is exchanged within the industry.

## Key Areas of Knowledge

### A. Understand the Healthcare Environment

- A.1 Types of Organizations in the Healthcare Sector (e.g., providers, pharma, payers, business associates)
- A.2 Health Information Technology (e.g., computers, medical devices, networks, health information exchanges, Electronic Health Record [EHR], Personal Health Record [PHR])
- A.3 Health Insurance (e.g., claims processing, payment models)
- A.4 Coding (e.g., SNOMED CT, ICD-9/10)
- A.5 Billing, Payment, and Reimbursement
- A.6 Workflow Management
- A.7 Regulatory Environment (e.g., security, privacy, oversight)
- A.8 Public Health Reporting
- A.9 Clinical Research (e.g., processes)
- A.10 Healthcare Records Management



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## B. Understand Third-Party Relationships

B.1 Vendors

B.2 Business Partners

B.3 Data Sharing

B.4 Regulators

## C. Understand Foundational Health Data Management Concepts

B.1 Information Flow and Life Cycle in the Healthcare Environments

B.2 Health Data Characterization (e.g., classification, taxonomy, analytics)

B.3 Data Interoperability and Exchange (e.g., HL7, HIE, DICOM)

B.4 Legal Medical Records



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 2: Regulatory Environment

## Overview

Patient treatment, payment, operations and related healthcare functions such as data analytics and research often require the routine exchange of sensitive patient health information. As a result, the healthcare industry receives a significant amount of oversight in many countries around the globe, and there are numerous laws, regulations, and best practice frameworks that specifically address the privacy and security of patient health information impacting what, when, how and with whom this information may be exchanged.

HCISPPcandidates should be able to identify and understand relevant legal and regulatory requirements related to health information, including requirements for trans-border data exchange, and help ensure their organization's policies and procedures are in compliance.

## Key Areas of Knowledge

### A. Identify Applicable Regulations

- A.1 Legal Issues that Pertain to Information Security and Privacy for Healthcare Organizations
- A.2 Data Breach Regulations
- A.3 Personally Identifiable Information
- A.4 Information Flow Mapping
- A.5 Jurisdiction Implications
- A.6 Data Subjects
- A.7 Data Owners/Controllers/Custodians/Processors

### B. Understand International Regulations and Controls

- B.1 Treaties (e.g., Safe Harbor)
- B.2 Regulations
- B.3 Industry Specific Laws
- B.4 Legislative (e.g., EU Data Privacy Directive, HIPAA/HITECH)

### C. Compare Internal Practices Against New Policies and Procedures

- C.1 Policies (information security and privacy)
- C.2 Standards (information security and privacy)
- C.3 Procedures (information security and privacy)



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

**D. Understand Compliance Frameworks (e.g., ISO, NIST, Common Criteria, IG Toolkit, Generally Accepted Privacy Principles [GAPP])**

**E. Understand Responses for Risk-Based Decision**

- E.1 Compensating Controls
- E.2 Control Variance Documentation
- E.3 Residual Risk Tolerance

**F. Understand and Comply With Code of Conduct/Ethics in a Healthcare Information Environment**

- F.1 Organizational Code of Ethics
- F.2 (ISC)² Code of Ethics



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 3: Privacy and Security in Healthcare

## Overview

Healthcare organizations continue to face a multitude of challenges, not the least of which is the need to apply a reasonable standard of due care and due diligence to safeguard the confidentiality, integrity and availability of healthcare information and comply with the inherent right of patients and their families to privacy—the freedom from unwanted intrusion into one's personal affairs.

HCISPP candidates should have a basic understanding of security and privacy concepts and principles, the relationship of security and privacy, and the types of information requiring protection in the healthcare industry.

## Key Areas of Knowledge

### A. Understand Security Objectives/Attributes

A.1 Confidentiality

A.2 Integrity

A.3 Availability

### B. Understand General Security Definitions/Concepts

B.1 Access Control

B.2 Data Encryption

B.3 Training and Awareness

B.4 Logging and Monitoring

B.5 Vulnerability Management

B.6 Systems Recovery

B.7 Segregation of Duties

B.8 Least Privilege (Need to Know)

B.9 Business Continuity

B.10 Data Retention and Destruction



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## C. Understand General Privacy Principles (e.g., OECD Privacy Principles, GAPP, PIPEDA, UK Data Protection Act 1998)

C.1 Consent/Choice

C.2 Limited Collection/Legitimate Purpose/Purpose Specification

C.3 Disclosure Limitation/Transfer to Third Parties/Trans-Border Concerns

C.4 Access Limitation

C.5 Security

C.6 Accuracy, Completeness, Quality

C.7 Management, Designation of Privacy Officer, Supervisor Re-authority, Processing Authorization, Accountability

C.8 Transparency, Openness

C.9 Proportionality, Use and Retention, Use Limitation

C.10 Access, Individual Participation

C.11 Notice, Purpose Specification

C.12 Additional Measures for Breach Notification

## D. Understand the Relationship Between Privacy and Security

D.1 Dependency

D.2 Integration

## E. Understand the Disparate Nature of Sensitive Data and Handling Implications

E.1 Personal and Health Information protected by Law

E.2 Sensitivity mitigation (e.g., de-identification, anonymization)

E.3 Categories of sensitive data (e.g., mental health)

E.4 Understand Security and Privacy Terminology Specific to Healthcare



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 4: Information Governance and Risk Management

## Overview

The healthcare environment can be exceedingly complex due to escalating threats and the myriad ways in which information must be utilized to provide patient-centered care, improve clinical outcomes, and support business goals and objectives. These challenges exist for all types of healthcare organizations, whether a large insurance conglomerate or small physician practice group, and the cost of managing information-related risk continues to grow.

Organizations must formally establish and be actively engaged with their security and privacy programs to address these challenges and ensure appropriate levels of due diligence and due care are provided for the cost-effective protection of sensitive health-related information.

HCISPP candidates should understand how organizations manage information risk through security and privacy governance, basic risk management methodology and lifecycles, and the principle risk activities they are likely to support.

## Key Areas of Knowledge

### A. Understand Security and Privacy Governance

A.1 Information governance

A.2 Governance structures

### B. Understand Basic Risk Management Methodology

B.1 Approach (e.g., qualitative, quantitative)

B.2 Information Asset Identification

B.3 Asset Valuation

B.4 Exposure

B.5 Likelihood

B.6 Impact

B.7 Threats

B.8 Vulnerability

B.9 Risk

B.10 Controls

B.11 Residual Risk



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

B.12 Acceptance

## C. Understand Information Risk Management Life Cycles (e.g., NIST, CMS, ISO)

## D. Participate in Risk Management Activities

D.1 Remediation Action Plans

D.2 Risk Treatment (e.g., mitigation/remediation, transfer, acceptance, avoidance)

D.3 Communications

D.4 Exception Handling

D.5 Reporting and Metrics



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 5: Information Risk Assessment

## Overview

One of the most important aspects of risk management is the assessment of risk. It occurs early in the risk management lifecycle in the initial selection of security and privacy safeguards, when those safeguards are initially implemented, periodically thereafter, and when risk treatments are considered due to a loss of effectiveness or when new risks are identified.

HCISPP candidates should understand risk assessment concepts, and be able to identify and participate in risk assessment practices and procedures in their organization.

## Key Areas of Knowledge

### A. Understand Risk Assessment

- A.1 Definition
- A.2 Intent
- A.3 Lifecycle/Continuous Monitoring
- A.4 Tools/Resources/Techniques
- A.5 Desired Outcomes
- A.6 Role of Internal and External Audit/Assessment

### B. Identify Control Assessment Procedures From Within Organization Risk Frameworks

### C. Participate in Risk Assessment Consistent With Role in Organization

- C.1 Information Gathering
- C.2 Risk Assessment Estimated Timeline
- C.3 Gap Analysis
- C.4 Corrective Action Plan
- C.5 Mitigation Actions

### D. Participate in Efforts to Remediate Gaps

- D.1 Types of Controls
- D.2. Controls Related to Time



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# Domain 6: Third Party Risk Management

## Overview

The flow of information between a healthcare organization and external third parties can present significant security, privacy and compliance-related risks due to the complex relationships required to support patient treatment, payment, operations and related healthcare functions such as data analytics and research. As such, organizations should proactively manage third party risks through a robust third party risk management program.

HCISPP candidates should be able to identify third party relationships based on their use of health information, help manage third party relationships, and determine when additional security and privacy assurances are required. Candidates should also be able to support the assessment of third parties, respond to third party security and privacy events, and participate in the mitigation of third party risks.

## Key Areas of Knowledge

### A. Understand the Definition of Third Parties in Healthcare Context

### B. Maintain a List of Third-Party Organizations

- B.1 Health Information Use (e.g., processing, storage, transmission)
- B.2 Third-Party Role/Relationship With the Organization

### C. Apply Third-Party Management Standards and Practices for Engaging Third Parties Based Upon the Relationship With the Organization

- C.1 Relationship Management
- C.2 Comprehend Compliance Requirements

### D. Determine When Third-Party Assessment Is Required

- D.1 Organizational Standards
- D.2 Triggers of Third-Party Assessment

### E. Support Third-Party Assessments and Audits

- E.1 Information Asset Protection Controls
- E.2 Compliance with Information Asset Protection Controls
- E.3 Communication of Findings



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## F. Respond to Notifications of Security/Privacy Events

F.1 Internal Processes for Incident Response

F.2 Relationship between Organization and Third-Party Incident Response

F.3 Breach Recognition, Notification, and Initial Response

## G. Support Establishment of Third-Party Connectivity

G.1 Trust Models for Third-Party Interconnections

G.2 Technical Standards (e.g., physical, logical, network connectivity)

G.3 Connection Agreements

## H. Promote Awareness of the Third-Party Requirements (internally and externally)

H.1 Information Flow Mapping and Scope

H.2 Data sensitivity and Classification

H.3 Privacy Requirements

H.4 Security Requirements

H.5 Risks Associated with Third Parties

## I. Participate in Remediation Efforts

I.1 Risk Management Activities

I.2 Risk Treatment Identification

I.3 Corrective Action Plans

I.4 Compliance Activities Documentation

## J. Respond to Third-Party Requests Regarding Privacy/Security Events

J.1 Organizational Breach Notification Rules

J.2 Organizational Information Dissemination Policies and Standards

J.3 Risk Assessment Activities

J.4 Chain of Custody Principles



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# REFERENCES

This reference list is **NOT** intended to be an all-inclusive collection representing the HCISPP Core Body of Knowledge (CBK). Its purpose is to provide candidates a starting point for their studies in domains which need supplementary learning in order to complement their associated level of work and academic experience. Candidates may also consider other references, which are not on this list but adequately cover domain content.

***Note**: (ISC)² does not endorse any particular text or author and does not imply that any or all references be acquired or consulted. (ISC)² does not imply nor guarantee that the study of these references will result in an examination pass.*

## REFERENCES


| |
|---|
| Access to Health Records Act 1990, Chapter 23. (1990). http://www.legislation.gov.uk/ukpga/1990/23/pdfs/ukpga_19900023_en.pdf. |
| Allen, J. (2001). The CERT Guide to System and Network Security Practices. Boston: Addison-Wesley Professional |
| American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, "Health Information Technology for Economic and Clinical Health Act (HITECH)", § 13600 (2009). http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf. |
| Anderson, R. (Ed.). (1997). Personal Medical Information: Security, Engineering, and Ethics. New York: Springer-Verlag |
| Benson, T. (2009). Principles of Health Interoperability HL7 and SNOMED. New York: Springer-Verlag. |
| Brandt, Mary (2009). The Privacy Officer's Handbook (2nd ed.). Marblehead, MA: HCPro, Inc. |
| Brown, S. A. and Brown, M. (2010). Ethical Issues and Security Monitoring Trends in Global Healthcare: Technological Advancements. Hershey, PA: Medical Information Science References |
| Brzezinski, R. (2013). HIPAA Privacy and Security Compliance – Simplified: Practical Guide for Healthcare Providers and Practice Managers. Columbus, OH: BizWit, LLC. |
| BS ISO/IEC 20000-2:2005 Information technology. Service management. Code of practice. |
| Camp, L. J. and Johnson, M. E. (2012). The Economics of Financial and Medical Identity Theft. New York, NY: Springer-Verlag. |
| Camp, L. J. and Johnson, M. E. (2012). The Economics of Financial and Medical Identity Theft. New York: Springer-Verlag. |
| Carroll, R. (2012). Risk Management Handbook for Healthcare Organizations (Vols. 1, 2 & 3) (6th ed.). San Francisco: John Wiley & Sons, Inc. |
| Center for Democracy and Technology (2013). Health Privacy (Web page). https://www.cdt.org/issue/health-privacy. |
| Center for Disease Control (2003). HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services. Washington, DC: Author. http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Ciampa, M. and Revels, M. (2012). Introduction to Healthcare Information Technology. Boston: Cengage Learning |
| Committee of Sponsoring Organizations of the Treadway Commission (2011). Internal Control – Integrated Framework. Durham, NC: Author. http://www.coso.org/documents/coso_framework_body_v6.pdf. |
| Crouhy, M., Galai, D., and Mark, R. (2006). The Essentials of Risk Management. New York: McGraw-Hill |
| Dark, M. J. (2010). Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives. Hershey, PA: Information Science Reference |
| Data Protection Act 1998, Chapter 29. (1998). http://www.legislation.gov.uk/ukpga/1998/29/data.pdf. |
| Determann, L. (2012). Determann's Field Guide to International Data Privacy Law Compliance. Cheltenham, UK: Edward Elgar Publishing, Inc. |
| DoD Directive 5220.22-M: National Industrial Security Program Operating Manual, http://www.fas.org/sgp/library/nispom/nispom2006.pdf |
| ECRI Institute (2009). Medical Technology for the IT Professional: An Essential Guide for Working in Today's Healthcare Setting. Plymouth Meeting, PA: Author. |
| El Emam, K. (Ed.). (2013). Risky Business: Sharing Health Data while Protecting Privacy. Bloomington, IN: Trafford Publishing. |
| Frasier, J. and Simkins, B. (2010). Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives (Robert W. Kolb Series). Hoboken, NJ: John Wiley & Sons, Inc. |
| Gartee, R. (2010). Health Information Technology and Management. Upper Saddle River, NJ: Prentice Hall |
| Gkoulalaas-Divanis, A., Loukides, G. (2012). Anonymization of Electronic Medical Records to Support Clinical Analysis (Springer Briefs in Electrical and Computer Engineering). New York: Springer-Verlag. |
| Hasib, H. (2013). Impact of Security Culture on Security Compliance in Healthcare in the United States of America: Strategic Solutions for Security Breaches. Laurel, MD.: Capitol College |
| Health & Human Services (2003). Summary of the HIPAA Privacy Rule. Washington, D.C. Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. |
| Health & Human Services (2006). HIPAA Administrative Simplification: Regulation Text, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf |
| Health & Human Services (2012). Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf. |
| Health & Human Services (2012). Guide to Privacy and Security of Health Information. Washington, D.C.: Author. http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. |
| Health and Human Services (2008). Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. Washington, DC: Author. http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. |
| Health and Human Services (2008). Personal Health Records and the HIPAA Privacy Rule. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Introduction. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Correction Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/correction.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Open and Transparency Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/opennesstransparency.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Individual Choice Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Collection, Use, and Disclosure Limitation Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/collectionusedisclosure.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Safeguards Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Accountability Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule's Right of Access and Health Information Technology. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf. |
| Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 42 U.S.C. § 13001-13424 (2009). http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf. |
| Health Insurance and Portability Act of 1996. Pub. L. No. 104-191, § 110 Stat. 1936 (1996). https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/HIPAALaw.pdf. |
| Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. Subtitle F (1996). https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/HIPAALaw.pdf. |
| Hebda, T. L. and Czar, P. (2012). Handbook of Informatics for Nurses and Healthcare Professionals (5th ed.). Upper Saddle River, NJ: Prentice Hall |
| Hermann, D. (2007). Complete Guide to Security and Privacy Metrics Measuring Regulatory Compliance, Operational Resilience, and ROI. Boca Raton, FL: Auerbach Publications |
| Herzig, T. (2010). Information Security in Healthcare: Managing Risk. Chicago, IL: HIMSS |
| Herzig, T., Walsh, T., and Gallagher, L. (2013). Implementing Information Security in Healthcare: Building a Security Program. Chicago, IL: HIMSS |
| HITECH Act Enforcement Interim Final Rule, 74 Fed. Reg. 56123 (Oct. 30, 2009) (to be codified at 45 CFR Part 160). http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Hopkin, P. (2012). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management (2nd ed.). Philadelphia: Kogan Page Ltd. |
| Hoyt, R. and Yoshihashi, A. (2010). Medical Informatics Practical Guide for Healthcare and Information Technology Professionals (4th ed.). Raleigh, NC: Lulu.com |
| Hoyt, R., Bailey, N., and Yoshihashi, A. (2012). Health Informatics: Practical Guide for Healthcare and Information Technology Professionals (5th ed.). Raleigh, NC: Lulu.com |
| Information Commissioner's Office (2008). Data Protection Act 1998 -The Eighth Data Protection Principle and international data transfers. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf |
| International Health Terminology Standards Development Organization (IHTSDO) (2013). SNOMED CT (Systematized Nomenclature Of Medicine Clinical Terms) User Guide. Copenhagen: Author. http://ihtsdo.org/fileadmin/user_upload/doc/download/doc_UserGuide_Current-en-US_INT_20130131.pdf. |
| International Standards Organization (2005). ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. Geneva: Author. |
| International Standards Organization (2005). ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management. Geneva: Author. |
| International Standards Organization (2008). ISO 277992008 Health Informatics – Information security management in health using ISO/IEC 27002. Geneva: Author. |
| International Standards Organization (2008). ISO/TS 25237:2008 Health Informatics – Pseudonymization. Geneva: Author. |
| International Standards Organization (2011). ISO/IEC 27005: 2011 Information Technology – Security techniques – Information security risk management. Geneva: Author. |
| Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Upper Saddle River, NJ: Addison-Wesley. |
| Jay, R. (2012). Data Protection Law and Practice (4th ed.). London: Sweet & Maxwell |
| Joint Task Force Transformation Initiative Interagency Working Group (2013). NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |
| Joint Task Force Transformation Initiative Interagency Working Group (2010). NIST Special Publication 800-37 (Rev. 1), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. |
| Joint Task Force Transformation Initiative Interagency Working Group (2010). NIST Special Publication 800-30 (Rev. 1), Guide for Conducting Risk Assessments. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. |
| Center for Medicare and Medicaid Services CMSR control document http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html |
| Kavaler, F. and Alexander, R. S. (2012). Risk Management in Health Care Institutions (3rd ed.). Burlington, MA: Jones & Bartlett Learning |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Kissel, R., Scholl, M., Skolachenko, S. and Li, X. (2006). NIST Special Publication 800-88, Guidelines for Media Sanitization. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf. |
| Kudyba, S. P. (2010). Healthcare Informatics: Improving Efficiency and Productivity. Boca Raton, FL: CRC Press |
| LaTour, K. (2009). Health Information Management: Concepts, Principles and Practice. (3rd ed.) Chicago, IL: American Health Information Management Association. |
| Lowrance, W. (2012). Privacy, Confidentiality, and Health Research (Cambridge Bioethics and Law). Cambridge, MA: Cambridge University Press |
| Markle Foundation (2006). The Common Framework: Overview and Principles (The Connecting for Health Common Framework). New York: Author. http://www.markle.org/sites/default/files/Overview_Professionals.pdf. |
| McWay, D. C. (2009). Legal and Ethical Aspects of Health Information Management (3rd ed.). Boston: Cengage Learning |
| Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (HIPAA Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 CFR Parts 160 and 164). http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. |
| Murphy, M. and Waterfill, M. (2010). The New HIPAA Guide for 2010: 2009 ARRA ACT for HIPAA Security and Compliance Law & Hitech Act Your Resource Guide to the New Security & Privacy Requirements. Bloomington, IN: AuthorHouse. |
| National Health Service (2009). NHS Information Risk Management. London: Author. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/inforiskmgtgpg.pdf. |
| National Health Service (NHS) Information Governance (IG) Toolkit Published Requirements https://www.igt.connectingforhealth.nhs.uk/RequirementsList.aspx?tk=414078609082725&lnv=2&cb=a47763cf-d3ee-4546-bead-9f7f4a47062f&sViewOrgType=2&sDesc=Acute%20Trust |
| Nin, J. and Herranz, J. (Eds.). (2010). Privacy and Anonymity in Information Management Systems: New Techniques for New Practical Problems (Advanced Information and Knowledge Processing). New York, NY: Springer-Verlag New York, LLC. |
| Organization for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: Author. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. |
| Quigley, M. (2007). Encyclopedia of Information Ethics and Security. Hershey, PA: Information Science Reference |
| Reynolds, G. (2011). Ethics in Information Technology (4th ed.). Boston: Cengage Learning |
| Scarfone, K., Souppaya, M., and Sexton, M. (2007). NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf. |
| Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., and Steinberg, D. I. (2008). NIST Special Publication 800-66 (Rev.1), An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf. |
| Shoniregun, C. (2010). Electronic Healthcare Information Security (10th ed.). New York: Springer-Verlag. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Shoniregun, C., Dube, K., & Menzi, F. (2012). Electronic healthcare information security. New York: Springer-Verlag. |
| Spooner, B., Reese, B., and Konschak, C. (Eds.). (2012). Accountable Care Bridging the Health Information Technology Divide. Virginia Beach, VA: Convurgent Publishing. |
| Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., and Lynes, D. (2010). NIST Special Publication 800-34 (Rev. 1), Contingency Planning Guide for Federal Information Systems. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. |
| Sweeney, L. (2002). k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570. http://arbor.ee.ntu.edu.tw/archive/ppdm/Anonymity/SweeneyKA02.pdf. |
| Swire, P., McQuay, T., and Ahmad, K. (2012). Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws, and Practices. Portsmouth, NH: International Association of Privacy Professionals. |
| The European Data Protection Directive 2001. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF. |
| The Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 124 Stat. 119 (2010). http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf |
| The Privacy Act of 1974. 5 U.S.C. § 552a (as amended). (1974). http://www.justice.gov/opcl/privstat.htm. |
| Trotter, F. and Uhlman, D. (2011). Hacking Healthcare: A Guide to Standards, Workflows, and Meaningful Use. Sebastopol, CA: O'Reilly Media, Inc. |
| Wellman, J., Jeffries, H., and Hagan, P. (2010). Leading the Lean Healthcare Journey: Driving Culture Change to Increase Value. Boca Raton, FL: CRC Press |
| Westby, J. R. (2012). Governance for Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks. Pittsburg: Carnegie Mellon University. http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf. |
| Westby, J. R. and Allen, J. H. (2007). Governing for Enterprise Security (GES) Implementation Guide (Technical Note CMU/SEI-2007-TN-020). Pittsburg: Carnegie Mellon University. http://www.cert.org/archive/pdf/07tn020.pdf. |
| Williams, B. (2013). Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. New York: CRC Press. |
| Wong, C. (2011). Security Metrics, A Beginners Guide. New York: McGraw-Hill. |
| World Health Organization (1992). The ICD-10 Classification of Mental and Behavioural Disorders: Clinical Descriptions and Diagnostic Guidelines. http://www.who.int/classifications/icd/en/bluebook.pdf. |
| World Health Organization (2010). International Statistical Classification of Diseases and Related Health Problems (10th Rev.) (ICD-10). http://apps.who.int/classifications/icd10/browse/2010/en. |
| Young, C. (2010). Metrics and Methods for Security Risk Management. Amsterdam: Elsevier. |
| Allen, J. (2001). The CERT Guide to System and Network Security Practices. Boston: Addison-Wesley Professional |
| American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, "Health Information Technology for Economic and Clinical Health Act (HITECH)", § 13600 (2009). http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Anderson, R. (Ed.). (1997). Personal Medical Information: Security, Engineering, and Ethics. New York: Springer-Verlag |
| Benson, T. (2009). Principles of Health Interoperability HL7 and SNOMED. New York: Springer-Verlag. |
| Brandt, Mary (2009). The Privacy Officer's Handbook (2nd ed.). Marblehead, MA: HCPro, Inc. |
| Brown, S. A. and Brown, M. (2010). Ethical Issues and Security Monitoring Trends in Global Healthcare: Technological Advancements. Hershey, PA: Medical Information Science References |
| Brzezinski, R. (2013). HIPAA Privacy and Security Compliance – Simplified: Practical Guide for Healthcare Providers and Practice Managers. Columbus, OH: BizWit, LLC. |
| BS ISO/IEC 20000-2:2005 Information technology. Service management. Code of practice. |
| Camp, L. J. and Johnson, M. E. (2012). The Economics of Financial and Medical Identity Theft. New York, NY: Springer-Verlag. |
| Camp, L. J. and Johnson, M. E. (2012). The Economics of Financial and Medical Identity Theft. New York: Springer-Verlag. |
| Carroll, R. (2012). Risk Management Handbook for Healthcare Organizations (Vols. 1, 2 & 3) (6th ed.). San Francisco: John Wiley & Sons, Inc. |
| Center for Democracy and Technology (2013). Health Privacy (Web page). https://www.cdt.org/issue/health-privacy. |
| Center for Disease Control (2003). HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services. Washington, DC: Author. http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm. |
| Ciampa, M. and Revels, M. (2012). Introduction to Healthcare Information Technology. Boston: Cengage Learning |
| Committee of Sponsoring Organizations of the Treadway Commission (2011). Internal Control – Integrated Framework. Durham, NC: Author. http://www.coso.org/documents/coso_framework_body_v6.pdf. |
| Crouhy, M., Galai, D., and Mark, R. (2006). The Essentials of Risk Management. New York: McGraw-Hill |
| Dark, M. J. (2010). Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives. Hershey, PA: Information Science Reference |
| Data Protection Act 1998, Chapter 29. (1998). http://www.legislation.gov.uk/ukpga/1998/29/data.pdf. |
| Determann, L. (2012). Determann's Field Guide to International Data Privacy Law Compliance. Cheltenham, UK: Edward Elgar Publishing, Inc. |
| DoD Directive 5220.22-M: National Industrial Security Program Operating Manual, http://www.fas.org/sgp/library/nispom/nispom2006.pdf |
| ECRI Institute (2009). Medical Technology for the IT Professional: An Essential Guide for Working in Today's Healthcare Setting. Plymouth Meeting, PA: Author. |
| El Emam, K. (Ed.). (2013). Risky Business: Sharing Health Data while Protecting Privacy. Bloomington, IN: Trafford Publishing. |
| Frasier, J. and Simkins, B. (2010). Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives (Robert W. Kolb Series). Hoboken, NJ: John Wiley & Sons, Inc. |
| Gartee, R. (2010). Health Information Technology and Management. Upper Saddle River, NJ: Prentice Hall |
| Gibson, D. (2011). SSCP Systems Security Certified Practitioner All-in-One Exam Guide. San Francisco: McGraw-Hill Osborne Media |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Gkoulalaas-Divanis, A., Loukides, G. (2012). Anonymization of Electronic Medical Records to Support Clinical Analysis (Springer Briefs in Electrical and Computer Engineering). New York: Springer-Verlag. |
| Hasib, H. (2013). Impact of Security Culture on Security Compliance in Healthcare in the United States of America: Strategic Solutions for Security Breaches. Laurel, MD.: Capitol College |
| Health & Human Services (2003). Summary of the HIPAA Privacy Rule. Washington, D.C. Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. |
| Health & Human Services (2006). HIPAA Administrative Simplification: Regulation Text, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf |
| Health & Human Services (2012). Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf. |
| Health & Human Services (2012). Guide to Privacy and Security of Health Information. Washington, D.C.: Author. http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. |
| Health and Human Services (2008). Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. Washington, DC: Author. http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. |
| Health and Human Services (2008). Personal Health Records and the HIPAA Privacy Rule. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Introduction. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Correction Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/correction.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Open and Transparency Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/opennesstransparency.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Individual Choice Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Collection, Use, and Disclosure Limitation Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/collectionusedisclosure.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Safeguards Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf. |
| Health and Human Services (2008). The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Accountability Principle and FAQs. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Health and Human Services (2008). The HIPAA Privacy Rule's Right of Access and Health Information Technology. Washington, DC: Author. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf. |
| Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 42 U.S.C. § 13001-13424 (2009). http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf. |
| Health Insurance and Portability Act of 1996. Pub. L. No. 104-191, § 110 Stat. 1936 (1996). https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/HIPAALaw.pdf. |
| Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. Subtitle F (1996). https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/HIPAALaw.pdf. |
| Hebda, T. L. and Czar, P. (2012). Handbook of Informatics for Nurses and Healthcare Professionals (5th ed.). Upper Saddle River, NJ: Prentice Hall |
| Hermann, D. (2007). Complete Guide to Security and Privacy Metrics Measuring Regulatory Compliance, Operational Resilience, and ROI. Boca Raton, FL: Auerbach Publications |
| Herzig, T. (2010). Information Security in Healthcare: Managing Risk. Chicago, IL: HIMSS |
| Herzig, T., Walsh, T., and Gallagher, L. (2013). Implementing Information Security in Healthcare: Building a Security Program. Chicago, IL: HIMSS |
| HITECH Act Enforcement Interim Final Rule, 74 Fed. Reg. 56123 (Oct. 30, 2009) (to be codified at 45 CFR Part 160). http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. |
| Hopkin, P. (2012). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management (2nd ed.). Philadelphia: Kogan Page Ltd. |
| Hoyt, R. and Yoshihashi, A. (2010). Medical Informatics Practical Guide for Healthcare and Information Technology Professionals (4th ed.). Raleigh, NC: Lulu.com |
| Hoyt, R., Bailey, N., and Yoshihashi, A. (2012). Health Informatics: Practical Guide for Healthcare and Information Technology Professionals (5th ed.). Raleigh, NC: Lulu.com |
| Information Commissioner's Office (2008). Data Protection Act 1998 -The Eighth Data Protection Principle and international data transfers. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf |
| International Health Terminology Standards Development Organization (IHTSDO) (2013). SNOMED CT (Systematized Nomenclature Of Medicine Clinical Terms) User Guide. Copenhagen: Author. http://ihtsdo.org/fileadmin/user_upload/doc/download/doc_UserGuide_Current-en-US_INT_20130131.pdf. |
| International Standards Organization (2005). ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. Geneva: Author. |
| International Standards Organization (2005). ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management. Geneva: Author. |
| International Standards Organization (2008). ISO 277992008 Health Informatics – Information security management in health using ISO/IEC 27002. Geneva: Author. |
| International Standards Organization (2008). ISO/TS 25237:2008 Health Informatics – Pseudonymization. Geneva: Author. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| International Standards Organization (2011). ISO/IEC 27005: 2011 Information Technology – Security techniques – Information security risk management. Geneva: Author. |
| Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Upper Saddle River, NJ: Addison-Wesley. |
| Jay, R. (2012). Data Protection Law and Practice (4th ed.). London: Sweet & Maxwell |
| Joint Task Force Transformation Initiative Interagency Working Group (2013). NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |
| Joint Task Force Transformation Initiative Interagency Working Group (2010). NIST Special Publication 800-37 (Rev. 1), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. |
| Joint Task Force Transformation Initiative Interagency Working Group (2010). NIST Special Publication 800-30 (Rev. 1), Guide for Conducting Risk Assessments. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. |
| Kavaler, F. and Alexander, R. S. (2012). Risk Management in Health Care Institutions (3rd ed.). Burlington, MA: Jones & Bartlett Learning |
| Kissel, R., Scholl, M., Skolachenko, S. and Li, X. (2006). NIST Special Publication 800-88, Guidelines for Media Sanitization. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf. |
| Kudyba, S. P. (2010). Healthcare Informatics: Improving Efficiency and Productivity. Boca Raton, FL: CRC Press |
| LaTour, K. (2009). Health Information Management: Concepts, Principles and Practice. (3rd ed.) Chicago, IL: American Health Information Management Association. |
| Lowrance, W. (2012). Privacy, Confidentiality, and Health Research (Cambridge Bioethics and Law). Cambridge, MA: Cambridge University Press |
| Markle Foundation (2006). The Common Framework: Overview and Principles (The Connecting for Health Common Framework). New York: Author. http://www.markle.org/sites/default/files/Overview_Professionals.pdf. |
| McWay, D. C. (2009). Legal and Ethical Aspects of Health Information Management (3rd ed.). Boston: Cengage Learning |
| Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (HIPAA Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 CFR Parts 160 and 164). http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. |
| Murphy, M. and Waterfill, M. (2010). The New HIPAA Guide for 2010: 2009 ARRA ACT for HIPAA Security and Compliance Law & Hitech Act Your Resource Guide to the New Security & Privacy Requirements. Bloomington, IN: AuthorHouse. |
| National Health Service (2009). NHS Information Risk Management. London: Author. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/inforiskmgtgpg.pdf. |
| National Health Service (NHS) Information Governance (IG) Toolkit Published Requirements https://www.igt.connectingforhealth.nhs.uk/RequirementsList.aspx?tk=414078609082725&lnv=2&cb=a47763cf-d3ee-4546-bead-9f7f4a47062f&sViewOrgType=2&sDesc=Acute%20Trust |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Nin, J. and Herranz, J. (Eds.). (2010). Privacy and Anonymity in Information Management Systems: New Techniques for New Practical Problems (Advanced Information and Knowledge Processing). New York, NY: Springer-Verlag New York, LLC. |
| Organization for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: Author. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. |
| Quigley, M. (2007). Encyclopedia of Information Ethics and Security. Hershey, PA: Information Science Reference |
| Reynolds, G. (2011). Ethics in Information Technology (4th ed.). Boston: Cengage Learning |
| Scarfone, K., Souppaya, M., and Sexton, M. (2007). NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf. |
| Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., and Steinberg, D. I. (2008). NIST Special Publication 800-66 (Rev.1), An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf. |
| Shoniregun, C. (2010). Electronic Healthcare Information Security (10th ed.). New York: Springer-Verlag. |
| Shoniregun, C., Dube, K., & Menzi, F. (2012). Electronic healthcare information security. New York: Springer-Verlag. |
| Spooner, B., Reese, B., and Konschak, C. (Eds.). (2012). Accountable Care Bridging the Health Information Technology Divide. Virginia Beach, VA: Convurgent Publishing. |
| Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., and Lynes, D. (2010). NIST Special Publication 800-34 (Rev. 1), Contingency Planning Guide for Federal Information Systems. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. |
| Sweeney, L. (2002). k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570. http://arbor.ee.ntu.edu.tw/archive/ppdm/Anonymity/SweeneyKA02.pdf. |
| Swire, P., McQuay, T., and Ahmad, K. (2012). Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws, and Practices. Portsmouth, NH: International Association of Privacy Professionals. |
| The European Data Protection Directive 2001. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF. |
| The Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 124 Stat. 119 (2010). http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf |
| The Privacy Act of 1974. 5 U.S.C. § 552a (as amended). (1974). http://www.justice.gov/opcl/privstat.htm. |
| Trotter, F. and Uhlman, D. (2011). Hacking Healthcare: A Guide to Standards, Workflows, and Meaningful Use. Sebastopol, CA: O'Reilly Media, Inc. |
| Wellman, J., Jeffries, H., and Hagan, P. (2010). Leading the Lean Healthcare Journey: Driving Culture Change to Increase Value. Boca Raton, FL: CRC Press |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

| |
|---|
| Westby, J. R. (2012). Governance for Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks. Pittsburg: Carnegie Mellon University. http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf. |
| Westby, J. R. and Allen, J. H. (2007). Governing for Enterprise Security (GES) Implementation Guide (Technical Note CMU/SEI-2007-TN-020). Pittsburg: Carnegie Mellon University. http://www.cert.org/archive/pdf/07tn020.pdf. |
| Williams, B. (2013). Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. New York: CRC Press. |
| Wong, C. (2011). Security Metrics, A Beginners Guide. New York: McGraw-Hill. |
| World Health Organization (1992). The ICD-10 Classification of Mental and Behavioural Disorders: Clinical Descriptions and Diagnostic Guidelines. http://www.who.int/classifications/icd/en/bluebook.pdf. |
| World Health Organization (2010). International Statistical Classification of Diseases and Related Health Problems (10th Rev.) (ICD-10). http://apps.who.int/classifications/icd10/browse/2010/en. |
| Young, C. (2010). Metrics and Methods for Security Risk Management. Amsterdam: Elsevier. |




© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# SAMPLE EXAM QUESTIONS

1. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule

(A) requires safeguards to protect the privacy of Protected Health Information (PHI).

(B) sets limits and conditions on the uses and disclosures that may be made of PHI without patient authorization.

(C) contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

(D) requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

**Answer - D**

2. When shall individuals be notified without unreasonable delay as required by the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule?

(A) No later than 60 days following the discovery of a breach.

(B) No later than 120 days following the discovery of a breach.

(C) No later than 90 days following the discovery of a breach.

(D) Immediately following the discovery of a breach.

**Answer - A**

3. The typical function of Secure Sockets Layer (SSL) in securing Wireless Application Protocol (WAP) is to protect transmissions

(A) between the WAP gateway and the wireless device.

(B) between the web server and WAP gateway.

(C) from the web server to the wireless device.

(D) between the wireless device and the base station.

**Answer – B**



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

# GENERAL EXAMINATION INFORMATION

## Computer Based Testing (CBT)

### *Registering for the Exam*

#### Process for Registration Overview

This section describes procedures for candidates registering to sit for a Computer Based Test (CBT). The test is administered at Pearson VUE Testing centers in the US, Canada, and other parts of the world.

1. Go to www.pearsonvue.com/isc2 to register for a test appointment.
2. Select the most convenient test center
3. Select an appointment time.
4. Pay for your exam appointment.
5. Receive confirmation from Pearson VUE with the appointment details, test center location and other relevant instructions, if any.

Please note that your registration information will be transferred to (ISC)² and all communication about the testing process from (ISC)² and Pearson VUE will be sent to you via email.

#### Fees

Please visit the (ISC)² website https://www.isc2.org/certification-register-now.aspx for the most current examination registration fees.

#### U.S. Government Veteran's Administration G.I. Bill

The U.S. Department of Veterans Affairs has approved reimbursement to veterans under the G.I. Bill for the cost of the Certified Information System Security Professional (CISSP), the CISSP Concentrations (ISSAP, ISSEP, ISSMP), the Certification and Accreditation Professional (CAP), and the System Security Certified Practitioner (SSCP) examinations. Please refer to the U.S. Department of Veterans Affairs Website at www.va.gov for more details.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

### CBT Demonstration

Candidates can experience a demonstration and tutorial of the CBT experience on our Pearson VUE web page. The tutorial may be found at

**www.pearsonvue.com/isc2**.

## *Scheduling a Test Appointment*

### Process for Registration Overview

Candidates may register for a testing appointment directly with Pearson VUE ( www.pearsonvue.com/isc2 ). Candidates who do not pass the test will be subject to the retake policy and must wait the applicable time before they are allowed to re-sit for the examination.

### Exam Appointment

Test centers may fill up quickly because of high volume and previously scheduled special events. Pearson VUE testing centers also serve candidates from other entities; thus waiting to schedule the testing appointment may significantly limit the options for candidate's desired testing dates at the closest center available.

### Scheduling for a Testing Appointment

Candidates may schedule their appointment online at (ISC)² CBT Website located at www.pearsonvue.com/isc2. Candidates will be required to create a Pearson VUE account in order to complete registration. Candidates profile will be transferred to (ISC)² and becomes part of the candidate's permanent record. Candidates will be able to locate test centers and select from a choice of available examination appointment times at the Pearson VUE website.

Candidates may also register over the telephone with a CBT registration specialist. Please refer to 'Contact Information' for local telephone numbers for your region.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## Rescheduling or Cancellation of a Testing Appointment

If you wish to reschedule or cancel your exam appointment, you must contact Pearson VUE at least **48 hours** before the exam date by contacting **Pearson VUE online** (www.pearsonvue.com/isc2), OR at least **24 hours** prior to exam appointment time by contacting Pearson VUE **over the phone**. Canceling or rescheduling an exam appointment less than 24 hours via phone notification, or less than 48 hours via online notification is subject to a forfeit of exam fees. Exam fees are also forfeited for no-shows. Please note that Pearson VUE charges a 50 USD/35 £/40 € fee for reschedules, and 100 USD/70 £/80 € fee for cancellations.

Reschedules and cancellations may be done at the (ISC)² CBT Candidate Website (www.pearsonvue.com/isc2) or via telephone. Please refer to 'Contact Information' for more information and local telephone numbers for your region.

## Late Arrivals or No Shows

If the candidate does not arrive within 15 minutes of the scheduled exam starting time, he or she has technically forfeited his or her assigned seat.

If the candidate arrives late (after 15 minutes of his/her scheduled appointment), it is up to the discretion of the testing center as to whether or not the candidate may still take the exam. If the test administrator at the testing location is able to accommodate a late arriving candidate, without affecting subsequent candidates' appointments, he/she will let the candidate to sit for the exam and launch his/her exam.

Any/all attempts are made to accommodate candidates who arrive late. However, if the schedule is such that the test center is not able to accommodate a late arrival, the candidate will be turned away and his/her exam fees will be forfeited.

If a candidate fails to appear for a testing appointment, the test result will appear in the system as a No-Show and the candidate's exam fees will be forfeited.

## Procedure for Requesting Special Accommodations

Pearson VUE Professional Centers can accommodate a variety of candidates' needs, as they are fully compliant with the Americans with Disability Act (ADA), and the equivalent requirements in other countries.

Requests for accommodations should be made to (ISC)² in advance of the desired testing appointment. Once (ISC)² grants the accommodations request, the candidate may schedule the testing appointment using Pearson VUE's special accommodations number. From there, a Pearson VUE coordinator will handle all of the arrangements.

PLEASE NOTE: Candidates that request special accommodations should not schedule their appointment online or call the main CBT registration line.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## What to Bring to the Test Center

### Proper Identification

(ISC)² requires two forms of identification, a primary and a secondary, when checking in for a CBT test appointment at a Pearson VUE Test Center. All candidate identification documents must be valid (not expired) and must be an original document (not a photocopy or a fax).

Primary IDs: Must contain a permanently affixed photo of the candidate, along with the candidate's signature.

Secondary IDs: Must have the candidate's signature.

| **Accepted Primary ID (photograph and signature, not expired)** |
|---|
| • Government issued Driver's License or Identification Card |
| • U.S. Dept of State Drivers License |
| • U.S. Learner's Permit (card only with photo and signature) |
| • National/State/Country Identification Card |
| • Passport |
| • Passport Cards |
| • Military ID |
| • Military ID for spouses and dependents |
| • Alien Registration Card (Green Card, Permanent Resident Visa) |
| • Government Issued local language ID (plastic card with photo and signature |
| • Employee ID |
| • School ID |
| • Credit Card* (A credit card can be used as a primary form of ID only if it contains both a photo and a signature and is not expired. Any credit card can be used as a secondary form of ID, as long as it contains a signature and is not expired. This includes major credit cards, such as VISA, MasterCard, American Express and Discover. It also includes department store and gasoline credit cards. |
| **Accepted Secondary ID (contains signature, not expired)** |
| • U.S. Social Security Card |
| • Debit/(ATM) Card |
| • Credit Cards |
| • Any form of ID on the primary list |



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

### Name Matching Policy

Candidate's first and last name on the presented identification document must exactly match the first and last name on the registration record with Pearson VUE. If the name the candidate has registered with does not match the name on the identification document, proof of legal name change must be brought to the test center on the day of the test. The only acceptable forms of legal documentation are marriage licenses, divorce decrees, or court sanctioned legal name change documents. All documents presented at the test center must be original documents. If a mistake is made with a name during the application process, candidates should contact (ISC)² to correct the information well in advance of the actual test date. Name changes cannot be made at the test center or on the day of the exam. Candidates who do not meet the requirements presented in the name matching policy on the day of the test may be subject to forfeiture of testing fees and asked to leave the testing center.

## Non Disclosure

Prior to starting the exam, all candidates are presented with (ISC)² non-disclosure agreement (NDA), and are required in the computer to accept the agreement prior to being presented with exam questions. If the NDA is not accepted by the candidate, or refused to accept within the time allotted, the exam will end, and the candidate will be asked to leave the test center. No refund of exam fees will be given. For this reason, all candidates are strongly encouraged to review the non-disclosure agreement prior to scheduling for, or taking the exam.

The agreement is located at www.pearsonvue.com/isc2/isc2_nda.pdf.

## Day of the Exam

### Check-In Process

Plan to arrive at the Pearson VUE testing center at least 30 minutes before the scheduled testing time. If you arrive more than 15 minutes late to your scheduled appointment, you may lose your examination appointment. For checking-in:

- You will be required to present two acceptable forms of identification.
- You will be asked to provide your signature, submit to a palm vein scan, and have your photograph taken. Hats, scarves and coats may not be worn in the testing room, or while your photograph is being taken.
- You will be required to leave your personal belongings outside the testing room. Secure storage will be provided. Storage space is small, so candidates should plan appropriately. Pearson Professional Centers assume no responsibility for candidates' personal belongings.
- The Test Administrator (TA) will give you a short orientation, and then will escort you to a computer terminal. You must remain in your seat during the examination, except



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

when authorized to leave by test center staff. You may not change your computer terminal unless a TA directs you to do so.

Raise your hand to notify the TA if you

- believe you have a problem with your computer.
- need to change note boards.
- need to take a break.
- need the administrator for any reason.

## Breaks

You will have up to **six hours** to complete the **CISSP**, and up to **four hours** to complete the **CSSLP and CCFP** up to **three hours** to complete the following examinations:

- **SSCP**
- **CAP**
- **HCISPP**
- **ISSAP**
- **ISSEP**
- **ISSMP**

Total examination time includes any unscheduled breaks you may take. All breaks count against your testing time. You must leave the testing room during your break, but you may not leave the building or access any personal belongings unless absolutely necessary (e.g. for retrieving medication). Additionally, when you take a break, you will be required to submit to a palm vein scan before and after your break.

## Examination Format and Scoring

- The CISSP® examination consists of 250 multiple choice questions with four (4) choices each.
- The CSSLP® examination consists of 175 multiple choice questions with four (4) choices each.
- The HCISPP examination contains 125 multiple choice questions with four (4) choices each.
- The CCFP examination contains 125 multiple choice questions with four (4) choices each.
- The SSCP® examination contains 125 multiple choice questions with four (4) choices each.
- The ISSAP®, ISSEP®, and ISSMP® concentration examinations contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.
- The Certified Authorization Professional (CAP®) examination contains 125 multiple choice questions with four (4) choices each. Also, administered in computers.

There may be scenario-based items which may have more than one multiple choice question associated with it. These items will be specifically identified in the test booklet.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

Each of these exams contains 25 questions which are included for research purposes only. The research questions are not identified; therefore, answer all questions to the best of your ability. There is no penalty for guessing, so candidates should not leave any item unanswered. Examination results will be based only on the scored questions on the examination. There are several versions of the examination. It is important that each candidate have an equal opportunity to pass the examination, no matter which version is administered. Subject Matter Experts (SMEs) have provided input as to the difficulty level of all questions used in the examinations. That information is used to develop examination forms that have comparable difficulty levels. When there are differences in the examination difficulty, a mathematical procedure called equating is used to make the difficulty level of each test form equal. Because the number of questions required to pass the examination may be different for each version, the scores are converted onto a reporting scale to ensure a common standard. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

## Technical Issues

On rare occasions, technical problems may require rescheduling of a candidate's examination. If circumstances arise causing you to wait more than 30 minutes after your scheduled appointment time, or a restart delay lasts longer than 30 minutes, you will be given the choice of continuing to wait, or rescheduling your appointment without an additional fee.

- If you choose to wait, but later change your mind at any time prior to beginning or restarting the examination, you will be allowed to take exam at a later date, at no additional cost.
- If you choose not to reschedule, but rather test after a delay, you will have no further recourse, and your test results will be considered valid.
- If you choose to reschedule your appointment, or the problem causing the delay cannot be resolved, you will be allowed to test at a later date at no additional charge. Every attempt will be made to contact candidates if technical problems are identified prior to a scheduled appointment.

## Testing Environment

Pearson Professional Centers administer many types of examinations including some that require written responses (essay-type). Pearson Professional Centers have no control over typing noises made by candidates sitting next to you while writing their examination. Typing noise is considered a normal part of the computerized testing environment, just as the noise of turning pages is a normal part of the paper-and pencil testing environment. Earplugs are available upon request.

## When the Exam is Finished

After you have finished the examination, raise your hand to summon the TA. The TA will collect and inventory all note boards. The TA will dismiss you when all requirements are fulfilled.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

If you believe there was an irregularity in the administration of your test, or the associated test conditions adversely affected the outcome of your examination, you should notify the TA before you leave the test center.

## Results Reporting

Candidates will receive their unofficial test result at the test center. The results will be handed out by the Test Administrator during the checkout process. (ISC)² will then follow up with an official result via email.

In some instances, real time results may not be available. A comprehensive statistical and psychometric analysis of the score data is conducted during every testing cycle before scores are released. A minimum number of candidates are required to take the exam before this analysis can be completed. Depending upon the volume of test takers for a given cycle, there may be occasions when scores are delayed for approximately 6-8 weeks in order to complete this critical process. Results WILL NOT be released over the phone. They will be sent via email from (ISC)² as soon as the scores are finalized. If you have any questions regarding this policy, you should contact (ISC)² prior to your examination.

## Retake Policy

Test takers who do not pass the exam the first time will be able to retest after 90 days. Test takers that fail a second time will need to wait 90 days prior to sitting for the exam again. In the unfortunate event that a candidate fails a third time, the next available time to sit for the exam will be 180 days after the most recent exam attempt. Candidates are eligible to sit for (ISC)² exams a maximum of 3 times within a calendar year.

## Recertification by Examination

Candidates and members may recertify by examination for the following reasons ONLY;

- The candidate has become decertified due to reaching the expiration of the time limit for endorsement.
- The member has become decertified for not meeting the number of required continuing professional education credits.



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15

## *Logo Usage Guidelines*

(ISC)² is a non-profit membership organization identified as the leader in certifying individuals in information security.

Candidates who successfully complete any of the (ISC)² certification requirements may use the appropriate Certification Mark or the Collective Mark, where appropriate, and the logo containing the Certification Mark or the Collective Mark, where appropriate (the "Logo") to identify themselves as having demonstrated the professional experience and requisite knowledge in the realm of information system security. Please visit the following link (URL) for more information on logo use:

https://www.isc2.org/uploadedfiles/(ISC)2_Public_Content/Legal_and_Policies/LogoGuidleines.pdf

## Any questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759
Phone: 1.866.331.ISC2 (4722) in the United States
1.727.785.0189 all others
Fax: 1.727.683.0785



© 2013 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1.16.14 V15


HealthCare Information Security
and Privacy Practitioner