

# Preparing for the Examination

## Competency Statements

A certification examination is based on an explicit set of competencies. These competencies have been determined through a job analysis study conducted with current

practitioners. The competencies are subdivided into domains, and subdomains as shown in the tables below. The examination tests only content outlined in the following competencies.

## Competency Statements

<b>Certified in Healthcare Privacy and Security</b>	Cognitive Level			
	Recall	Application	Analysis	Total
<b>1. Management and Administration</b>	<b>6</b>	<b>14</b>	<b>10</b>	<b>30</b>
A. Provide guidance regarding applicable standards of accreditation agencies (Joint Commission, AAAHC, AOA, NCQA).				
B. Administer an appropriate organizational infrastructure for privacy and information security				
C. Create, document, and communicate company privacy and security policies, procedures, and guidelines.				
D. Review relationships to identify business associates.				
E. Ensure appropriate contract development and management procedures comply with business associate requirements.				
F. Ensure the maintenance of the inventory of software, hardware, and all information assets.				
G. Participate in business continuity planning for planned downtime and contingency planning for emergencies and disaster recovery.				
H. Perform data criticality analysis.				
I. Establish and maintain facility security plan to safeguard unauthorized physical access to information and prevent theft or tampering.				
J. Participate in analysis, implementation, and decisions regarding privacy and security solutions.				
K. Develop, deliver, evaluate, and document training and awareness of privacy and security				
L. Work with appropriate organization officials to ensure information used or disclosed for research complies with applicable privacy regulations.				
M. Facilitate ongoing assessments of organizational policies, procedures, and practices related to privacy and security.				

Preparing for the Examination

<b>Certified in Healthcare Privacy and Security</b>	Cognitive Level			
	Recall	Application	Analysis	Total
<b>2. Regulatory Requirements, Investigation, and Compliance</b>	<b>8</b>	<b>16</b>	<b>10</b>	<b>34</b>
A. Assess and communicate risks and ramifications of breaches of privacy and security, including those by business associates to leadership				
B. Establish incident response plan and identify team members (for example, Human Resources, Legal, Risk Management, Physical Security, Legal Law Enforcement, Public Relations).				
C. Coordinate privacy and security compliance documentation required by law.				
D. Ensure and monitor compliance with state and federal laws and regulations related to privacy and security.				
E. Coordinate the organization's response to inquiries and investigations from external entities relating to privacy and security.				
F. Develop system to maintain and retain applicable documentation.				
G. Establish compliance indicators and develop methods to measure compliance to improve organizational performance.				
H. Coordinate incident investigations and response.				
I. Develop, implement, and ensure follow-through on a system to evaluate risk.				
J. Enforce privacy and security policies, procedures, and guidelines to enable compliance with federal, state, and other regulatory or accrediting bodies.				
K. Monitor appropriateness of access to identifiable health information.				
L. Establish a complaint investigation and resolution process.				
<b>3. Information Technology</b>	<b>11</b>	<b>18</b>	<b>8</b>	<b>37</b>
A. Monitor data backup plan.				
B. Develop and manage strategic information security plan.				
C. Assess security risks and identify threats and vulnerabilities.				
D. Establish audit controls (for example, logging guidelines, administrative access).				

**Certified in Healthcare Privacy and Security (CHPS)**

<b>Certified in Healthcare Privacy and Security</b>	<b>Cognitive Level</b>			
	<b>Recall</b>	<b>Application</b>	<b>Analysis</b>	<b>Total</b>
E. Ensure technical safeguards such as configuration management, intrusion detection, and preventive countermeasures are adequate for the organization.				
F. Ensure the documentation of the maintenance of software, hardware, and all information assets.				
G. Ensure that preventive measures are in place to prevent attacks (for example, malicious code, hacking).				
H. Establish internal standards to determine compliance to security requirements by system, network, application, and user.				
I. Ensure that the transmission of secure and private information is protected appropriately.				
J. Implement disaster recovery plan as needed after disaster has occurred.				
K. Establish guidelines, procedures, and controls to ensure the integrity, availability and confidentiality of communication across networks (for example, wireless Internet, secure sockets, VPNs, and PKI).				
L. Ensure the use of event triggering to notify abnormal conditions within a system (for example, intrusion detection, denial of service, and invalid log-on attempts).				
M. Establish and manage process for verifying and controlling access authorizations and privileges including emergency access (for example, context-based access, role-based access, and user-based access).				
N. Establish and manage authentication mechanisms (for example, guidelines, unique user ID, password, biometrics, PIN, token, telephone call back).				
O. Develop process for the use of cryptography, digital signatures, and public and private key infrastructure technologies.				
P. Provide forensic services (for example, data recovery, evidence preservation, and event tracing).				

Certified in Healthcare Privacy and Security	Cognitive Level			
	Recall	Application	Analysis	Total
<b>4. Physical Safeguards</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>12</b>
A. Establish media control practices that govern the receipt, removal, or disposal (internal and external destruction) of any media containing data.				
B. Establish physical security mechanisms to limit the access to authorized personnel for approved activities (for example, workstation placement, fax machine control, printer control).				
C. Establish reasonable safeguards to reduce incidental disclosure.				
D. Ensure use of generally accepted physical and system security principles.				
<b>5. Health Information Management</b>	<b>8</b>	<b>18</b>	<b>11</b>	<b>37</b>
A. Recommend appropriate de-identification methodologies.				
B. Ensure that recipients of secure and private information are permitted to receive the information (subpoena, court orders, search warrants).				
C. Ensure the rights of the individual who is a subject of individually identifiable health information. (amendments, access, restrictions, confidential communications).				
D. Define HIPAA-designated record sets for the organization.				
E. Identify information and record sets requiring special privacy protections.				
F. Identify permitted disclosures (for example, research, marketing, fund development, valid authorizations).				
G. Identify permitted uses of health information (for example, treatment, payment, healthcare operations, minimum necessary, need-to-know).				
H. Ensure protocols are in place to verify identity of recipients of health information.				