

Appendix A

WORK PROCESS SCHEDULE

AND

RELATED INSTRUCTION OUTLINE

Health Information Management (HIM) Privacy and Security Officer Apprenticeship

O*NET-SOC CODE:

RAPIDS CODE:

Type of Training: Competency-based

APPENDIX A

Sample Work Process Schedule and Related Instruction Outline

Health Information Management (HIM) Privacy and Security Officer Apprenticeship

O*NET-SOC CODE:

RAPIDS CODE:

This schedule is attached to and a part of these Standards for the above identified occupation.

1. TYPE OF OCCUPATION

Time-based Competency-based Hybrid

2. TERM OF APPRENTICESHIP

The term of the occupation shall be competency-based supplemented by a minimum of 144 hours of related instruction.

3. RATIO OF APPRENTICES TO JOURNEYWORKERS

Two (2) apprentice(s) to **One (1)** mentor.

4. APPRENTICE WAGE SCHEDULE

Apprentices may be paid a progressively increasing schedule of wages based on a percentage of the current Privacy and Security Professional wage rate of \$_____.

1 Year Term (example):

1st 1000hrs = \$ _____
2nd 500hrs = \$ _____
3rd 500hrs +CHPS = \$ _____

5. WORK PROCESS SCHEDULE (See below Work Process Schedule)

(Customized at point of hire by the Employer and Sponsor)

The Employer may modify the work processes to meet local needs prior to submitting these Standards to the appropriate Registration Agency for approval.

6. RELATED INSTRUCTION OUTLINE (See below Work Process Schedule)

(Customized at point of hire by the Employer and Sponsor)

Position Description:

The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization’s policies and procedures covering the privacy of, and access to, patient health information in compliance with federal and state laws and the healthcare organization’s information privacy practices. Privacy officers demonstrate competence in designing, implementing, and administering comprehensive privacy and security protection programs in all types of healthcare organizations. Job requirements include an Associate’s or Bachelor’s degree with previous healthcare experience. Preferred candidates will hold an Associate’s Degree or higher in Health Information Management with current credential such as RHIA (Registered Health Information Administrator), RHIT (Registered Health Information Technician) OR Bachelor’s degree or higher with previous experience in healthcare privacy and/or security management.

ON THE JOB COMPETENCIES:

COMPETENCY	MEASURED BY	Score	COMMENTS
Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee, ³ and legal counsel.	Coordinates the development of privacy risk assessment policies and procedures	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 5 – Exceeds expectation
Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.	Coordinates with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violation	1 2 3 4 5 N/A	1 – Below expectation 2 – Needs improvement 3 – Demonstrates basic understanding 4 – Demonstrates proficiency 5 – Excels

COMPETENCY	MEASURED BY	Score	COMMENTS
Serves in a leadership role for the Privacy Oversight Committee's activities.	Demonstrates leadership in the Privacy Oversight Committee	Meets or Does Not Meet	Comment on Does Not Meet
Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.	Collaborates on cyber privacy and security policies and procedures.	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds
Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.	Monitors systems development and operations for security and privacy compliance.	Meets or Does Not Meet	Comment on Does Not Meet
Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.	Develop and implement a corporate-wide Privacy Training Program -- in conjunction with the Security Officer Oversight, Cyber Security Awareness &	1 2 3 4 5 N/A	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds

COMPETENCY	MEASURED BY	Score	COMMENTS
	Training Program		
Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.	Periodically revises the privacy program in light of changes in laws, regulatory or company policy	Meets or Does Not Meet	Comment on Does Not Meet
Establishes with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.	Monitors Access and Disclosure Verification Procedures	Meets or Does Not Meet	Comment on Does Not Meet
Works cooperatively with the HIM Director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.	Provides support for organizational processes for use and disclosure of PHI including amendments, corrections, and accounting for disclosures	Meets or Does Not Meet	Comment on Does Not Meet

COMPETENCY	MEASURED BY	Score	COMMENTS
Establishes and administers a process for receiving, documenting, tracking, investigating, and takes action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	Meets or Does Not Meet	Comment on Does Not Meet
Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.	Establish an internal privacy audit program	Meets or Does Not Meet	Comment on Does Not Meet
Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.	Develops, implements and regularly updates a corporate-wide privacy training program	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 5 – Exceeds expectation
Reviews all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a	Establish and monitor internal privacy and	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient

COMPETENCY	MEASURED BY	Score	COMMENTS
liaison to the information systems department.	security audit programs		5 – Exceeds expectation
Works with all organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements.	Periodically revise the privacy program in light of changes in laws, regulatory or company policy	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 5 – Exceeds expectation
Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance. Serves as information privacy consultant to the organization for all departments and appropriate entities.	Coordinate external audit processes of business Partners	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 5 – Exceeds expectation
Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.	Develops appropriate sanctions for failure to comply with the corporate privacy policies and procedures	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 5 – Exceeds expectation

COMPETENCY	MEASURED BY	Score	COMMENTS
Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.			

Note: *On the job competencies will be evaluated as competency-based achievements. Each of the competencies will have objectives and all competencies will be verified and signed off by assigned journeyworker/mentors/trainers/supervisors.*

All related instruction and supplementary training will be structured in accordance with the Certified in Healthcare Privacy and Security (CHPS) domains.

RELATED INSTRUCTION OUTLINE

Health Information Management Privacy and Security Officer

Immersion Training (Related Instruction) Outline

Item	Type	Content	Hours
Program orientation	WebEx	Program overview	1
VLab tutorial	WebEx	VLab training	1
Pre-immersion assessment	Online assessment	Retired CHPS exam questions	4
Read Chapters 1 and 2 in <i>“Introduction to Health Information Privacy and Security”</i> textbook and complete online assessments.	Online and self-directed.	How health information is regulated, review of federal laws, state laws and accrediting and certifying bodies. Professional ethical standards and codes of conduct. HIPAA basics for privacy and security.	18
Online course: <i>The Pillars of a Privacy Program</i> (PSPILLARS)	Online self-directed	This course provides an orientation to HIPAA, types of covered entities, definition of protected health information (PHI), de-identified PHI, HIPAA enforcement, and the pillars of a privacy program.	6
Read Chapters 3 and 6 in <i>“Introduction to Health Information Privacy and Security”</i> textbook and complete online assessments.	Online and self-directed.	HIPAA privacy rule concepts to include use and disclosure, marketing and fundraising, and administrative requirements. Key changes under HITECH for privacy provisions.	18
Online course: <i>HIPAA Privacy: Rights and Responsibilities</i> (PSPRIVACY)	Online and self-directed	This course discusses the rights patients have regarding their PHI and responsibilities of organizations required by the HIPAA Privacy Rule regarding the use and disclosure of PHI.	6
Read Chapters 4 and 5 in <i>“Introduction to Health Information Privacy and Security”</i> textbook and complete online assessments.	Online and self-directed.	HIPAA security rule concepts to include physical safeguards, technical safeguards, organizational requirements and policies, procedures and documentation. Threat identification, risk analysis and disaster recovery/business continuity.	18
Online course: <i>HIPAA Security: Safeguarding PHI</i> (PSSECURITY)	Online self-directed	This course begins with a discussion of the scope of the Security Rule’s coverage and its basic structure in terms of safeguards, standards, and implementation specifications.	6
Online course: <i>HIPAA Privacy and Security for Business Associates</i> (HIPAABAPS)	Online self-directed	This course provides information about the HIPAA requirements for business associates (BA).	8

Item	Type	Content	Hours
Online course: <i>HIPAA Privacy and Security for Covered Entities</i> (HIPAA CEPS)	Online self-directed	This course provides information about the HIPAA privacy and security essentials for covered entities (CE).	8
AHIMA Breach Management Toolkit	Online self-directed	A comprehensive guide for compliance which addresses planning, implementing, and maintaining a breach management process.	12
AHIMA External HIPAA Audit Readiness Toolkit	Online self-directed	Understand the requirements for HIPAA Phase 2 audits and guidance regarding audit preparation and practices.	12
Common employability modules	Online self-directed	Common employability skills to include: <ul style="list-style-type: none"> • Communicating Effectively • Telephone Etiquette • The Mindful Leader • Leveraging Diversity and Strengths in the Workplace • Inspirational Leadership • Social Media Awareness • Excellence in Customer Service 	18
Post-immersion assessment	Online assessment	Retired CHPS exam questions	4
Meetings with Apprentice Staff	WebEx	Review activities, provide feedback and instruction	4
Total Immersion Training/Related Instruction hours			144

TOTAL MINIMUM HOURS

144