Appendix A

WORK PROCESS SCHEDULE

AND

RELATED INSTRUCTION OUTLINE

Health Information Management (HIM) Privacy and Security Officer
O*NET-SOC CODE: **11-9199.02**
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: 11-9199.02
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

Four (4) apprentices 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), Master's or related degree (such as MBA, MPH, MS, JD, MD, or PhD).

ON THE JOB COMPETENCIES:

COMPETENCY	***MEASURED BY***	***Score***	***COMMENTS***
Maintains current knowledge of applicable federal and state privacy laws and accreditation standards.	Demonstrates understanding of HIPAA laws, standards and state privacy laws.	Meets or Does Not Meet	Comment on **Does Not Meet**
Provides guidance and assistance in the identification, development, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management.	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
Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities. Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements.	Conducts audits of internal and external privacy functions	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds

COMPETENCY	***MEASURED BY***	***Score***	***COMMENTS***
Establishes a preventative program to detect, prevent and mitigates privacy/security breaches.	Develops performance measures and reports to monitor and improve organizational performance and report to appropriate organizational body.	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds
Establishes an incident/complaint/breach investigation response, develops response plan and oversees investigations of incidents/complaints/ breaches. Determines corrective action/remediation, sanctions and disciplinary actions.	Coordinates with the Corporate Compliance Officer or legal re: procedures for documenting and reporting any evidence of privacy violation	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds
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 & Training Program	1 2 3 4 5 N/A	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds
Establishes a mechanism to track access to Protected Health Information (PHI), within the purview of the organization and as required by law.	Monitors Access and Disclosure Verification Procedures	Meets or Does Not Meet	Comment on **Does Not Meet**

COMPETENCY	*MEASURED BY*	*Score*	*COMMENTS*
Oversees processes 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**
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.	Establishes and/or monitors an internal privacy audit program	Meets or Does Not Meet	Comment on **Does Not Meet**
Reviews security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.	Establish and monitor internal privacy and security audit programs	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactory 4 – Proficient 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 minimum necessary protocols, 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

COMPETENCY	*MEASURED BY*	*Score*	*COMMENTS*
Participates in the development and maintenance of the inventory of software, hardware and all information assets to protect information assets and to facilitate risk analysis.	Provides input to mitigate information security risk	1 2 3 4 5	1 – Below expectation 2 – Needs improvement 3 – Satisfactorily 4 – Demonstrates proficiency 5 – Exceeds
Monitors advancements in information privacy technologies to ensure organizational adaptation	Demonstrates current knowledge of information privacy technologies	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). Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.	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

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 "*Introduction to Health Information Privacy and Security"* 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
CHPS Domains 1 & 4: Ethics Regulation, Investigation and Compliance (H0EPCHPS14)	Online self-directed	This course reviews the competencies of ethical, legal, and regulatory issues/external environment including investigation, compliance, and enforcement principles and strategies.	12
Read Chapters 3 and 6 in "*Introduction to Health Information Privacy and Security"* 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
CHPS Domain 2: Program Management and Administration (H0EPCHPS2)	Online and self-directed	This course reviews privacy and security program planning, including areas such as policy and procedure development, access authorization, and de-identification methods.	12
Read Chapters 4 and 5 in "*Introduction to Health Information Privacy and Security"* 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
CHPS Domain 3: Information Technology/Physical and Technology Safeguards (H0EPCHPS3)	Online self-directed	Learn best practices to develop and manage a strategic information security plan and implementing optimal technical safeguards including assessing security risks, identifying threats and vulnerabilities. Identify security requirements and appropriate measurements to protect the confidentiality and integrity of ePHI.	12
AHIMA Breach Management Toolkit	Online self-directed	A comprehensive guide for compliance which addresses planning, implementing, and maintaining a breach management process.	12

Item	Type	Content	Hours
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: • 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 Coding Trainers	WebEx	Review activities, provide feedback and instruction	4
Total Immersion Training/Related Instruction hours			**146**

TOTAL MINIMUM HOURS **146**