CHIEF INFORMATION OFFICER

Classification specifications are only intended to present a descriptive summary of the range of duties and responsibilities associated with specified positions. Therefore, specifications *may not include all* duties performed by individuals within a classification. In addition, specifications are intended to outline the *minimum* qualifications necessary for entry into the class and do not necessarily convey the qualifications of incumbents within the position.

FLSA STATUS: Exempt

DEFINITION:

The Chief Information Officer oversees the Agency's information technology strategies and computer systems to ensure that they support the Agency's goals. This position is responsible for streamlining operations by implementing relevant technologies ensuring support and security, developing technological systems that will improve customer satisfaction, and managing the information technology department. Perform other duties as assigned.

DISTINGUISHING CHARACTERISTICS:

The Chief Information Officer is an executive management level class which is responsible for assisting the Executive Director in the overall management of the information technology operations of Tri-City Mental Health Authority. Administrative direction is provided by the Executive Director. Responsibilities include direct and indirect supervision of information technology staff.

EXAMPLES OF ESSENTIAL DUTIES: Essential duties include, but are not limited to, the following:

Strategic Business Development:

- Develop objectives and strategies to ensure the IT department runs smoothly and effectively.
- Stay informed of technology sector developments and evaluate potential Agency applications.
- Stay up to date with cybersecurity threats, trends, and technology.
- Select and implement suitable technology to streamline all internal operations and help optimize their strategic benefits.
- Analyze the costs, value and risks of information technologies to advise management and suggest actions.
- Collaborate with other executives and directors to measure system and resource use and allocation.

IT Infrastructure Development:

- Direct and organize the implementation of new IT systems with an emphasis on filling remote access needs.
- Create and adapt technological platforms to improve the client experience.
- Oversee the technological infrastructure (networks and computer systems) in the organization to ensure optimal performance.
- Establish ongoing change management capabilities to support major innovation and transformation programs.
- Approve purchases of technological equipment and software and establish partnerships with IT providers.
- Closely collaborate with the Chief Compliance Officer and the Best Practices Department to ensure optimization of the Electronic Health Record platform and related workflows.
- Work with the Chief Compliance Officer in establishing IT services frameworks and best practices and rolling out policies to users.

IT Department Management:

- Direct and establish IT-related projects.
- Provide leadership to the IT department and other staff within the Agency.
- Responsible for department staffing design and hiring for key roles in the department.
- Establish and monitor department budget, prepare cost-benefit analyses for changes IT workflows; design and monitor department KPIs.

Security Auditing and Legislative Education and Updates:

- Work with the Systems Administration and Security Officer to monitor compliance with security practices and consistent application of sanctions for failure to comply with security policies for all individuals in the practice's workforce and for all business associates (BAs).
- Maintain a current, up-to-date, knowledge of federal and state privacy laws and accreditation standards.
- Must maintain a working knowledge of legislative and regulatory initiatives for implementation.
- Ensure development of appropriate policies, standards, guidelines, and procedures for information security systems.

- Work with the Systems Administration and Security Officer to assemble an incident response team, with specifically designated roles and responsibilities for each member. The team should investigate the breach, including why or how it occurred, and then take actions to correct it.

- Direct and monitor the Systems Administration and Security Officer, Best Practices, and Operations in the establishment of a mechanism to track access to PHI within the practice, as required by state and federal regulation, and to allow qualified individuals to review or receive a report on access activity.

- Ensure that all access and distribution to protected health information is in compliance with federal, state, and agency regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and The Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH Act").

QUALIFICATIONS:

Any combination of education, training, and experience that provides the required knowledge, skills, and abilities to perform the essential duties of the position is qualifying. The incumbent will possess the most desirable combination of education, training, skills, and experience, as demonstrated in his/her past and current employment history. A typical example includes:

Education, Training, and Experience:

Bachelor's degree in Computer Science, Information Technology, System Administration, or a closely related field, or 10+ years equivalent work experience required; MSc/MA preferred. Must have proven experience as IT Director, CIO, or similar executive role; working with management and C-level executives; implementing and effectively developing helpdesk and IT operations best practices; managing an Electronic Health Records Systems and operation, usage, and modification of these systems; and working with Agencies regulated by the HIPAA and HITECH Acts is required. Experience implementing a new EHR is preferred.

Knowledge of:

- Excellent knowledge of IT systems and infrastructure.
- Proficiency in establishing IT services framework and IT security policies.
- Working knowledge of virtualization, VMWare, or equivalent.

Skill to:

- Analyze and problem solve superiorly.
- Strong strategic and business mindset.
- Excellent organizational and leadership skills.
- Outstanding written, oral, and interpersonal skills, with a focus on listening and questioning skills.

Ability to:

- Design/develop IT systems and planning IT implementation with a proven track record of doing so.
- Solid understanding of data analysis, budgeting and business operations.
- Ability to clearly articulate ideas in business-friendly and user-friendly language.

Special Requirements:

- Possess and maintain a current valid California Driver License, a satisfactory driving record, and a properly registered and insured vehicle.
- Receive satisfactory results from a background investigation, which includes fingerprinting; a pre-employment physical examination, which includes a drug/alcohol test; and an administrative review.
- In accordance with California Government Code Section 3100, Tri-City Mental Health Authority employees, in the event of a disaster, are considered disaster service workers and may be asked to protect the health, safety, lives, and property of the people of the State.

PHYSICAL STANDARDS:

The position requires prolonged sitting, reaching, twisting, turning, bending, stooping, lifting, and carrying paper and documents weighing up to 50 pounds in the performance of daily activities; body mobility to move from one work area to another, and operate a vehicle; grasping, repetitive hand movement and fine coordination in preparing reports, data entry, and using a computer keyboard; vision sufficient for observing work performed, reading correspondence and reports, statistical data, computer screen and other standard text; and communicating with others on the phone, in person, and in meetings.