

POSITION ANNOUNCEMENT
Chief Information Security Officer
Tennessee Department of Health
Information Technology Services Division

(Grade 045 Salary Range: \$6,597 - \$10,555 monthly)

The Mission of the Tennessee Department of Health (TDH) is to Protect, Promote and Improve the health and prosperity of people in Tennessee. The Department provides services to overall 6.45 million Tennesseans, along with those who visit our state directly or indirectly. One in five people, some 1.4 million people, are directly served each year through a network of 89 rural and six metropolitan county health departments, while others are impacted by inspections of restaurants, healthcare and related facilities; registration or receipt of vital records; protection from communicable illness; licensing of health professionals; specialized laboratory testing and many other services and programs.

Job Overview:

The Chief Information Security Office is responsible for establishing and maintaining Department wide information security program to ensure that "information assets" (protected health information (PHI), data, software, personal identifiable information (PII)) are adequately protected and compliant with federal and state laws. Additionally, the position is responsible for structuring both centralized IT security management and decentralized identity management activities as they relate to Department-wide information. This position is responsible for identifying, evaluating and reporting on information security risks in a manner that meets compliance and regulatory requirements, reduces risk and improves productivity.

Job Responsibilities:

The Chief Information Security Officer will report directly to the Agency Chief Information Officer in the Information Technology Services Division (ITSD).

- Ensures the development and implementation of policies and procedures related to the security of protected health information, including the risk analysis, sanctions policy, and information systems activity review required by the HIPAA Security Regulations. Ensures information risk assessments and system evaluations are conducted when required by law or the business needs of the organization. Leads information security training and awareness programs to educate the workforce.
- Ensures appropriate access controls to protected health information. Ensures compliance with security related policies and procedures. Addresses and ensures disaster recovery and business continuity of protected health information, including establishing data backup plans and disaster recovery plans required by the HIPAA Security Regulations. In the instance of a breach of information systems: assist the Chief Privacy Officer to establish, implement, and lead an incident response team to contain, investigate and prevent future breaches of protected health information.

- Serves as information security consultant to the Department. Represents the Department's information security interests with external parties. Reviews all system-related information security plans throughout the Department to ensure alignment between security and privacy practices. Initiates, facilitates and promotes activities to foster information security awareness within the organization and related entities.

Minimum Qualifications:

A four -year college degree is required. Advanced degree is preferred.

Professional certifications, e.g. CISSP

A minimum 5 years of experience in a HIPAA compliant organization.

This is an executive service position reporting to the Agency Chief Information Officer. Interested applicants should send a resume to Carole Sumner (Carole.Sumner@tn.gov). The State of Tennessee is an equal opportunity, equal access, affirmative action employer.