

**Chief Information Security Officer
Apex Medical Center**

Job Description: With limited supervision from the Chief Compliance Officer identifies, investigates, resolves and develops processes, procedures and associated documentation relative to security of computer systems, networks and telecommunications along with addressing privacy, confidentiality and standards administration. Serves as a leader for teams investigating and addresses various health information security and privacy issues.

Typical Activities:

Reviews and studies all information published by DHHS, HCFA and other regulatory bodies relative to health information security and privacy, particularly relating to special legislation such as HIPAA.

Establishes and maintains technical computer and network security systems and protocols.

Establishes and maintains administrative computer and network security systems and protocols.

Establishes and maintains health information release of information and associated written policies and procedures.

Subscribes to and reviews various publications both in written form and through the Internet relative to health information privacy and security.

Reviews, assesses, studies, analyzes the procedures and documentation relative to privacy and security issues including electronic signatures, claims development and transmission, use of health identifiers, etc.

Uses a systematic approach for the identification and resolution of complex privacy and security issues.

Works with health information management, patient accounts, information system and other medical center personnel to solve and implement solutions to maintain a proper privacy and security stance.

Works with the Chief Compliance Officer and medical center legal counsel relative to difficult privacy and security issues.

Works with the Chief Compliance Officer and other medical center personnel in conducting audits and tests of various security systems.

Monitors and reviews logs of computer systems and network activities for possible unauthorized intrusion.

Develops and presents training courses for medical center personnel at all levels relative to the privacy and security of health information.

Develops and directs technical teams in the investigation and resolution of complex privacy and security problems.

Chief Information Security Officer

Writes and assists others in writing various types of policies and procedures in order to maintain proper compliance relative to health information security and privacy.

Attends workshops and seminars to maintain a high level of knowledge and capabilities.

Studies and recommends acquisition of various hardware and software in order to properly implement health information privacy and security.

Recommends and coordinates the use of consultants for specialized activities relative to health information privacy and security.

Coordinates and facilitates problem resolution sessions where multiple departments and/or service areas are involved.

Works with upper management and the Chief Compliance Officer relative to presentations and briefing of the Board of Directors

Addresses special projects as assigned.

Knowledge, Skills, Abilities and Personal Characteristics:

Extensive knowledge of various health care privacy, security and associated laws, rules and regulations including all applicable standards.

Extensive knowledge of the various sources and resources for information at the federal, state and local level in the privacy and security areas.

Extensive knowledge of computer systems, computer network systems, telecommunications and all associated hardware, software and associated protocols.

Extensive knowledge of the Internet, intranet and extranet technologies and applications.

Extensive knowledge of computer based patient record systems and various protocols relative to privacy and confidentiality of health information.

Extensive knowledge of risk analysis and the development of security systems and protocols.

Knowledge of various encryption techniques and their proper utilization.

Knowledge of specialized telecommunication techniques such Virtual Private Networks and associated secure telecommunication techniques.

Knowledge of various health care related code sets such as CPT-4, ICD-9, HCPCS, SNOMED, etc.

Knowledge of the various payment systems including DRGs, APCs/APGs, RBRVS, RUGs-III and various managed care and capitated arrangements.

Knowledge of the charge master, its use, design, revenue center codes, relationship to CPT/HCPCS coding and overall impact on the coding, billing and reimbursement process.

Knowledge of computer hardware and software its use, function and design relative to coding, billing and reimbursement.

Knowledge of general hospital operations.

Knowledge of physician clinic operations.

Chief Information Security Officer

Knowledge of the auditing process including various techniques relative to auditing and problem resolution.

Knowledge of team dynamics and the process of building consensus.

An overall understanding of financial management and reporting in health care.

Ability to participate with upper management in a decision support mode through the development of appropriate management information.

Ability to effectively work with and coordinate the activities of outside consultants.

Ability to work with outside auditors relative to formal privacy and security auditing situations.

Ability and skill to influence personnel through a matrix organization as opposed to line management authority.

Ability to develop and lead teams toward stated objectives and goals.

Skill in using personal computers for financial analysis (spreadsheets), data base development and report generation.

Skill in performing research with bibliographic data bases and Internet access to associated information resources.

Skill in networking both directly through colleagues and professional organizations along with the ability to utilize networking capabilities through Internet news groups and list servers.

Interpersonal communication skills for training and working with personnel in sometimes tense situations.

Ability to facilitate diverse disciplines and personnel with disparate technical backgrounds.

Educational Background and Certifications:

Masters Degree in Healthcare Administration or Business Administration is highly desirable.

Masters Degree in Information Systems and Information Technology is highly desirable.

Certification(s) in the information security areas such as the CISSP (Certified Information Systems Security Specialist) is desirable.

Appropriate certification in risk management and/or health care compliance desirable.

Five to ten years progressive experience in health information security management, health information management, information systems and/or health risk management is required.

Reports To:

Chief Compliance Officer. (See Notes below)

Subordinate Personnel:

Subordinate staff is provided as needed and/or may be provided on a special project basis.

Notes:

1. This is a highly responsible position that requires both quantitative and interpersonal skills.
2. Depending upon the size of the organization being considered, this position may have an extensive subordinate staff. Typical job positions that may be under the management of the CISO include:
 - a. System Security Analyst (Associate, Senior)
 - b. System Security Engineer
 - c. System Security Administrator
3. The CSIO may report to the Chief Compliance Officer (COO) or this position may reside in the information systems area with the CSIO reporting to the CIO (Chief Information Officer). Alternative organizational structures are quite possible since health care privacy and security is an interdisciplinary area.