CORPORATE PRIVACY OFFICIAL

JOB DESCRIPTION:

The privacy official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to SHC'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.

Serves as corporate resource for implementation of the privacy requirements under HIPAA and state laws. He/she serves as a member of the Corporate HIPAA Core Team and HIPAA Steering Committee and coordinates all corporate activities with privacy implications. Accountable for overseeing the development and implementation of corporate-wide privacy principles, policies and practices. Provides direction in the implementation of administrative, technical and physical procedures to protect the privacy of protected health information (PHI). Works with consultant(s) selected by the organization to assess the current state of privacy practices, conduct risk/gap analysis, develop new policies and procedures and training materials. Monitor the implementation of HIPAA-compliant privacy practices for network hospitals in the United States. Also, assists in privacy requirements for network hospitals that are located outside of the United States. Serves as a designated contact between Corporate headquarters and its hospitals in privacy practices. Coordinates with the Corporate Security Official and works closely with the hospital administrators, privacy officials and security officials in the development and monitoring of security practices. Advocates and protects patient privacy by serving as a key privacy advisor for patients, handling disputes and managing patient requests regarding their medical record that are elevated to the Corporate headquarters. Works with public relations, corporate departments, HIPAA Steering Committee and corporate leadership to assure that public communications and public understanding of privacy safeguards at the organization's entities is appropriately communicated.

REPORTING RELATIONSHIP:

Reports directly to the Corporate Executive Administrator.

RESPONSIBILITIES:

ORGANIZATIONAL DEVELOPMENT OF PRIVACY PROGRAMS

- Serves as the Corporate Privacy Official pursuant to the administrative requirements of 45 Code of Federal Regulation, Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule)
- Coordinates corporate privacy activities which includes overseeing the establishment, implementation and adherence to corporate policies on patient privacy, confidentiality and release of patient information

- Coordinates HIPAA project activities as required to include:
  - Project management
  - HIPAA consultant liaison
  - Process change management
  - Policies and procedures assessment and development
  - Contingency planning
  - Remediation planning
  - Equipment and system prioritization
- Member of the Corporate HIPAA Steering Committee and HIPAA Core Team
- Develops and manages HIPAA project teams; serves as a liaison between the Headquarters HIPAA groups and hospital HIPAA teams/committees
- Provides leadership in the planning, design, and evaluation of the organization's privacy and security related projects
- Serves as a liaison to regulatory and accrediting bodies for matters relating to privacy and security
- Responsible for documenting and communicating the progress of HIPAA privacy implementation at corporate and with the hospitals
- Works with legal counsel, management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices
- Works with the Legal Department to review new or revised healthcare laws and regulations (federal and sixteen states) pertaining to patient privacy and determine whether modifications or revisions of policies and procedures are needed
- Provides direction and guidance in special investigations or special projects. Reviews results and recommends actions in coordination with other interested company and outside parties
- Works closely with the Security Official, members of the electronic medical record implementation team, and other information technology personnel to ensure that the organization's privacy protections keep pace with technological advances
- Coordinates with management, Information Security Official, hospital security services, and others to assure physical safeguards to guard data integrity, confidentiality and availability
- Coordinates with senior management, operational managers, the IS Security Official, IT managers, and business support services to provide for a business continuity plan and disaster recovery service
- Reviews all system-related information 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
- Provides concise summaries to senior management of complex and detailed regulatory publications and prepares operational impact statements

PRIVACY EXPERTISE & RESOURCES

- 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
- Participates in outside healthcare organizations for keeping updated on privacy developments and "best practices" for patient privacy
- Maintains corporate library on Privacy regulations and requirements
- Maintains documentation of corporate privacy program
- Researches regulatory issues and is able to utilize a variety of research resources to assure that the most recent regulatory issuances and interpretations are available Communicates changes in regulatory issues to senior management and to the appropriate operational managers. Provides access to detailed regulations and assures that operational mangers understand the regulations

COMPLAINTS SYSTEM

- Establishes and administers, as appropriate, hospitals /corporate process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures

MEDICAL RECORDS MANAGEMENT AND DISCLOSURES

- Develops, implements, and administers a system-wide request for access/disclosure verification procedure that reasonably verifies the identity of the individual or entity requesting access or disclosures, and /or legal authority to request the protected health information
- Implements and oversees the development and application of corrective action procedures that are designed to mitigate any deleterious effects of use of disclosure of PHI by members of the entity's workforce or business partners
- Establishes policies/procedures that ensures that record custodians correctly protect and archive patient information
- Works cooperatively with the Corporate/Hospital leadership in establishing system to meet patient rights to inspect, amend, and restrict access to protected health information
- Directs the appropriate use of notices, postings, signs and information available to the public and to patients concerning corporate policies and procedures to protect individually identifiable health information and notices of restrictions that may be placed on the release of information

PUBLIC RELATIONS

- Increases the public's awareness of organization's efforts to preserve patient privacy
- Provide information in response to internal and external inquiries regarding the entity's corporate privacy polices and procedures or notice of information practices
- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.

RESEARCH & IRBs

- In coordination with Corporate Research Department, serves as privacy liaison, as appropriate, to local IRBs to ensure privacy awareness and proper authorizations are established where needed or required

TRAINING

- Oversees the development and delivery of privacy training and awareness to include Corporate staff, hospitals and other entities, as required
- Develops and implements a system-wide privacy training program and, in conjunction with the security official or other individuals charged with security oversight, a cyber security awareness and training program that includes the following components:
  - Initial training of all employees related to the privacy and cyber security program
  - Privacy training to all members of the workforce, including all employees, volunteers, trainees, and other persons under the direct control of the entity on an on an unpaid basis, who are not business partners but are likely to have contact with PHI
  - Upon changes in corporate privacy policy or procedure, retraining of directly affected employees
  - Mandated privacy retraining for all employees on a periodic basis, but, at a minimum, every three years

PRIVACY SANCTIONS

- Works with senior management to develop and apply appropriate sanctions against employees who fail to comply with the organization's privacy/security policies and procedures
- In cooperation with Human Resources, the Information Security Official, administration, and legal counsel, as applicable, ensures 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
- Coordinates with HR to ensure no intimidating, discriminatory, or other retaliatory actions occur against a person who files, testifies, assists, or participates in any investigation, compliance review, proceeding, or hearing related to a privacy violation, or opposes any unlawful act or practice.

CERTIFICATIONS AND AUDITS

- Establishes an internal privacy audit program to ensure enterprise-wide compliance to corporate privacy policies
- Works with departmental managers to assure that there is adequate auditing and monitoring of systems' access and activity and processes in place identify potential security violations
- Directs or conducts independent reviews and evaluations of any and all operations and activities to appraise:
  - Compliance with current regulations of federal, state, and other regulatory bodies

    - Possible errors and omissions that may violate current or future compliance
    - Compliance with internal policies, plans or standards which could impact compliance with external regulatory bodies
- Establishes a corporate-wide privacy program certification/recertification process
- Cooperates with the Office of Civil Rights, other legal entities, and organization officials in any compliance reviews or investigations.
- 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
- Provides assistance to legal, operational managers and staff during enforcement activities, surveys, and external investigations. Assists in the preparations of required documentation required by external agencies, corrective action plans, and future monitoring or auditing to assure compliance
- Maintains communications with external regulatory or review organizations and accrediting agencies to assure proper interpretations of regulations and impacts on operations. Coordinates work with others within the organization that have responsibility for process improvement, accreditation surveys or other regulatory activities
- Responds quickly to incidents and violations to reduce the risks to the organization

QUALIFICATIONS:

The following qualifications are the minimum necessary to adequately perform this job. However, any equivalent combination of experience, education and training which provides the necessary knowledge, skills and abilities would be acceptable, subject to any legal and/or regulatory requirements.

Education and Formal Training

- Bachelors degree from an accredited university or college. Masters degree preferred
- An individual with a combination of the following: medical records/health information management background, information systems/technology background; compliance, legal or performance improvement background

Work Experience

- A least 5 years of relevant medical records, clinical or healthcare administration experience
- Experience in a supervisory capacity and the ability to direct and develop others

Knowledge, Skill and Abilities Required

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies
- A high level of integrity and trust
- Substantial computer skills required (Microsoft Office at a minimum)

- Able to communicate clearly, make oral presentations to senior management, and prepare concise detailed written reports
- Demonstrated organization, facilitation, communication, and presentation skills.
- Project management skills
- Self motivation and initiative

Physical Requirements

- Sit, read, write, speak, use computer keyboard
- Able to travel to hospitals as needed
- Flexibility with work schedule to meet headquarters and hospital needs