Systems Security Officer (SSO)
Job Description

The position of Systems Security Officer (SSO) is required by HIPAA Security Standards, Section 164.308(a)(2).

The Systems Security Officer is responsible for the overall direction of security functions associated with information technology, systems, networks, communications and computing services within [redacted]. The SSO works with management, departments and committees to ensure data security, integrity, and protection of [redacted] systems from external and internal threats and to ensure [redacted] maintains an effective security compliance program.

Functions & Responsibilities:
General:

- Manages the development and implementation of global security policy, standards, guidelines and procedures to ensure ongoing maintenance of security.
- Works with others to develop and maintain a cost-effective and appropriate security posture for the organization.
- Ensures organization compliance with the security provisions of federal and state regulations, including HIPAA standards.
- Provides leadership for the company-wide security program and security compliance improvement activities, consistent with corporate strategic plans.
- Oversees schedules, status reports, budgets and other management communications regarding information security projects and activities.
- Facilitates and promotes a risk management approach to information security, and is responsible for seeing that significant risks are addressed.
- Provides the foundation for the security culture and awareness throughout the company.
- Identifies ways to enhance security capabilities and competencies of the organization.
- Reviews risk assessment and audit reports. Works with internal and external auditors to respond to needed requests, suggestions and security related findings, and determines appropriate action.
- Ensures IT staff is trained on security tools and compliance issues, as appropriate for their job description.

Security Incident Reporting:

- Receives allegations of security incidents and conducts complex investigations.
- Oversees incident response planning and investigation when a security violation has occurred; recommends and implements counter-measures as appropriate.
- Documents the security incident response, including written findings, recommendations, and follow up evaluation; prepares oral and written reports to various internal and external stakeholders at all levels.
- Reports on security issues and incidents to senior management, legal counsel, and the Security Governance Committee, as appropriate.
- Assists with disciplinary and legal matters associated with security breaches as necessary.

Skills and Qualifications:

- Bachelor's degree in computer science or related technology field.
- Ten+ years of relevant computer systems management experience, at least some of which has been in a healthcare setting.
- Solid understanding of Information Technology, Information Security, Risk Management and Business Continuity Planning.
- Maintains familiarity with industry-wide and corporate-wide standards, regulations, best practices and compliance issues related to information security.
- Understanding of information technology, including network architectures, data management, risk analysis, disaster recovery, audit tracking, intrusion prevention, and IT infrastructure and application security issues.
- Fluent with MS-Office desktop products.

- Keen problem-solving, analytical and investigative skills.
- Demonstrated project management, organization, leadership, team building and facilitation skills.
- Information Security Management Certification (CISM) or Information Systems Security Professional Certification (CISSP) desirable.
- Excellent interpersonal and communication skills to effectively communicate security-related concepts to all levels of personnel, including providing documentation and presentations to management staff.
- Conforms to ethical practices, professional practice standards, and demonstrates effective behaviors, objectivity and professionalism in difficult situations.
- Maintains confidentiality to protect individuals and the organization.

Additional Requirements:

- May be required to work outside of typical M-F 8am-5pm work schedule.
- May be on-call for security-related matters and work off-shift in emergency situations.

HIPAA Privacy Category 4: Employee job responsibilities require management and/or administration of processes involving member's Protected Health Information.

NOTE: There may be additions, deletions, and modifications to the qualifications and responsibilities of this job from time to time as may be required by business conditions, change in circumstances or particular situations. In addition, all employees must perform any and all other duties or responsibilities assigned to them by management.