Job Title: Chief Information Security Officer

Healthix is part of a nationwide effort to improve our health care system through better access to information.

Healthix is the largest Regional Health Information Organization, or RHIO, in New York State. Our team collaborates closely with premier academic medical centers, and with the New York City (NYC) and New York State (NYS) Departments of Health (DOH) to provide technology and consulting services that connect health care providers and patients. We maintain data of 10,000,000 patients that is continuously updated by over 150 Participant organizations and accessible by over 13,000 Authorized Users. With the patient’s consent, we help Providers and health plans securely access patient data to support more effective treatment and care management, consistent with regulations and policies established by NYS DOH.

We improve how health care is delivered with the end result of better care for the patient and greater efficiency for everyone.

Position Description:

Reporting to the Senior Vice President and Chief Information Officer, the Chief Information Security Officer plays an integral part in defining the fundamental principles for the protection of Healthix’s information resources and the proper controls needed to ensure compliance with internal and external regulations, while supporting the business needs and upholding the Healthix’s reputation with its participants.

The Chief information Security Officer will be accountable to oversee all the Information Security policies in place and determine the security controls that are appropriate to the level of risk associated with IT systems leveraged to support Healthix employees and customer services. This role will provide strategic leadership and provide an Information Security program to manage and improve information security while mitigating risk.

This role serves as an expert advisor to senior management in the development, implementation and maintenance of information systems to ensure best practice control objectives are achieved in protecting information assets.

This role guides the senior leadership team by making pragmatic recommendations for priority investments and projects that will mitigate overall risks by strengthening defenses and reducing vulnerabilities for Healthix’s information assets.

Responsibilities include but are not limited to:

- Develop, manage and improve a comprehensive information security risk-based program to ensure the integrity, confidentiality and availability of information assets.

- Develop an IT security architecture roadmap that will identify security controls, and identify and assess technologies that will enforce the organization’s security priorities.

- Develop, maintain, and promote information security policies, standards and guidelines. Ensure that controls comply with contractual obligations, corporate policies, and legal and regulatory requirements.

- Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users.

- Define and facilitate the information security risk assessment process, including the reporting and oversight of treatment efforts to address findings with collaboration of the Sr. Director of Compliance and Compliance Coordinators.

- Create, communicate and implement a process to manage vendor risk, including assessment and remediation efforts to address such risks that may result from partners, consultants and other service providers.

- Provide strategic risk guidance and consultation for corporate IT projects, including the evaluation and recommendation of technical standards and controls.

- Establish and implement a process for incident management to effectively identify, respond, contain and communicate a suspected or confirmed incident with collaboration of the Sr. Director of Compliance and Compliance Coordinators.

- Identify, assess, and prioritize IT risks to corporate data and systems, including external threats, cyber-crimes, internal threats and third-party risks. Advise relevant stakeholders on the appropriate courses of action to mitigate or eliminate risk.

- Coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of a security event. Provide direction, support and in-house consulting in these areas.

- Effectively manage an information security budget, and monitor for variances.

- Provide regular reporting on the current status of the information security program to the senior leadership team and the board of directors as part of a strategic enterprise risk management program.

- Facilitate a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the security.

The qualified candidate for this position will possess:

EDUCATION:

- Bachelor degree in Information Security, Computer Science, Management of Information Systems, or related field required. Masters preferred.

EXPERIENCE:

- Minimum of 8 years of experience in a combination of risk management, information security and information technology fields. At least 4 years of experience in a senior leadership role. Employment history must demonstrate increasing levels of responsibility.

REQUIRED SKILLS AND ABILITIES:

- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and nontechnical audiences.

- Proven track record and experience in developing information security policies and procedures, as well as successfully executing programs that meet the objectives of excellence in a dynamic environment.

- Poise and ability to act calmly and competently in high-pressure, high-stress situations.

- Knowledge and demonstrated experience of relevant legal and regulatory requirements, such as SOX, PCI DSS, HITECH, HIPAA Privacy & Security and other CMS regulations and guidelines as they are updated by the Federal Government.

- Knowledge of common information security management frameworks, such as NIST.

- Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.

- Knowledge of various health care related code sets such as CPT-4, ICD-9/10, LOINC, SNOMED, etc.

- Exhibit excellent analytical skills, the ability to manage multiple, inter-disciplinary projects as well as the ability to work well in a demanding, dynamic environment and meet overall objectives.

- Project management skills: financial/budget management, scheduling and resource management.

- High level of personal integrity, as well as the ability to professionally handle confidential matters, and show an appropriate level of judgment and maturity.

- High degree of initiative, dependability and ability to work with little supervision.

Healthix is an Equal Opportunity Employer