ROCHESTER RHIO

Regional Health Information Organization

Job Title: Chief Privacy and Security Officer
Reports To: Chief Executive Officer
Job Type: Full-Time, Exempt
Location: Rochester, NY
Remote/Hybrid Work Options Available.
Email resumes to: careers@grrhio.org

As the trusted data steward for secure health information exchange, Rochester RHIO is one of the most respected, trusted and successful health information exchanges in the United States. Rochester RHIO serves 14 counties in the greater Finger Lakes Region and 1.5 million residents. At Rochester RHIO, we love connecting with talented people who get excited about making a difference in patient care with health data.

Rochester RHIO requires all employees to comply with the company's COVID-19 vaccination policy upon hire. Please include 2-3 job references with your resume.

Job Summary: The Chief Privacy and Security Officer (CPSO) holds a key role in the organization, with responsibility for compliance with all security and privacy policies related to health information and data, and with extensive executive level responsibility.

Required Skills & Abilities: This position requires a dedicated professional, with extensive experience in the policy and security landscape of health information technology. The CPSO must be highly skilled in verbal and written communications, and comfortable in discussions with community, government and healthcare leadership, as well as with consumers.

Key Responsibilities include, but are not limited to:

Information Security

- Maintain an extensive working knowledge of the organization's physical and virtual infrastructure and the services which this infrastructure provides.
- Work with managers from all departments to maintain the architectural development of this infrastructure in a secure manner that aligns with the current governance and IT security frameworks applicable to the organization.

- Select and schedule all third-party risk and vulnerability assessments, including penetration testing, environment scanning, and the use of any other third-party resources available for maintaining the organization's information security program.
- Assess the results of third-party scanning and testing tools and work with managers from all departments to mitigate any risks discovered in the testing processes.
- Manage security compliance assessments and the development of secure relationships with all contractors, vendors, and data sources.
- Responsible for all matters related to information security, including but not limited to: physical and logical security, encryption standards for data-at-rest and data-in-transit, policies and procedures, information security monitoring and audits, etc.
- Provide regular briefings on the organization's information security program and maintain records of these briefings for auditing purposes.
- Ensure that the organization's workforce receives training and education on current information security issues, policies, procedures and best practices.
- Work with other information security professionals directly involved with the organization to ensure interoperability and a secure health information exchange.
- Develop policies and procedures that create growth in the organization's information security program and adhere to the current governance and IT security frameworks.
- Maintain a vision of the organization's current threat and risk landscape and how to mitigate and/or manage current threats and risks. The CPSO will address the threat and risk landscape with RHIO leadership, managers, contractors, vendors, or data sources as needed.
- Lead the maintenance of the organization's security certifications in order to maintain the organization's good standing with funding sources, the Board, and the community.

Privacy

- Serves as an internal health information privacy officer.
- Advises the organization about patient privacy issues.
- Assists outside legal counsel in dealing with various regulatory initiatives, including issues related to applicable privacy requirements (e.g., compliance with HIPAA requirements).
- Develops, implements, and oversees privacy and security policies and procedures for employees.

- Initiates and conducts activities to create information privacy, security awareness, and education for employees, participants and consumers.
- Prepares and conducts internal HIPAA training.
- Facilitates business associate agreements, health information privacy, and security policies and procedures for sub-contractors and business associates with access to health information.
- Reviews service specifications, health information retention plans, release of information, and website content for compliance with health information privacy and security regulations.
- Participates in the Secondary Use Committee evaluation of requests for health information for clinical research.

Education/Experience

- Thorough understanding of Information Privacy and Security concepts and relevant regulatory requirements, and experience in Security and HIPAA compliance in networked solution.
- Bachelor's degree (B.A. /B.S.); and five to ten years related experience and/or training; or equivalent combination of education and experience; CHPE and CISSP certification preferred.

More About the Company: Health information exchange services allow a medical care team to share records across institutions and practices, making patient information available wherever and whenever needed to provide the best care. Patients benefit from fewer repeated tests, easier second opinions, and a reduced risk of mistakes caused by poor handwriting or incomplete records, and more informed care during office visits and emergencies. Rochester RHIO is a Qualified Entity of the Statewide Health Information Network of New York (SHIN-NY), and was founded in 2006. You can learn more at https://rochesterrhio.org.

Rochester RHIO is an equal opportunity employer, and we celebrate diversity at our organization.