Information Security Manager Position Description

Delaware Health Information Network (DHIN)

Organization Background

The Delaware Health Information Network (DHIN) is the nation's first statewide health information exchange. Established by statute as a not-for-profit public instrumentality, DHIN's primary mission is to facilitate the design and implementation of an integrated, statewide health data system to support the information needs of consumers, health plans, policymakers, providers, purchasers and researchers to improve the quality and efficiency of health care services in Delaware. Participation in DHIN by the health care community of Delaware is nearly universal, with expansion beyond state borders also having begun. DHIN is recognized as a national leader in the area of health information exchange.

Position Overview

The Information Security Manager is part of the DHIN leadership team, reporting to the Chief Technology Officer (CTO). The Information Security Manager works collaboratively with the CEO and other DHIN leaders to develop strategy and translate strategy into tactical and operational reality. Collaboration and cooperation to make the entire DHIN team successful are the paramount requirements of members of the DHIN leadership team.

Specifically, the Information Security Manager supports DHIN by participating in the leadership, implementation and maintenance of an effective and comprehensive compliance and security program that protects DHIN's health information data and operations. The Manager serves as a project lead and subject matter expert for DHIN in security operational initiatives, and is responsible for facilitating, executing, monitoring, and documenting policies, procedures, processes, and overall compliance operations. The Manager also assists in developing and executing communication and training modules and initiatives. The Manager performs monitoring activities and assists the DHIN management team in analyzing outcomes and communicating findings as appropriate. Additional responsibilities include leading and/or participating in the investigation of privacy, security and other ethics concerns, workplace safety, and compliance with federal, state and HITRUST rules and regulations.

The Information Security Manager exercises responsibilities and skills at SFIA (**Skills Framework for the Information Age)** level 5:

> Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines.

Autonomy	Works under broad direction. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or project/supervisory objectives. Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities.
Influence	Influences organization, customers, suppliers, partners and peers on the contribution of

	own specialism. Builds appropriate and effective business relationships. Makes decisions which impact the success of assigned work, i.e. results, deadlines and budget. Has significant influence over the allocation and management of resources appropriate to given assignments.
Complexity	Performs an extensive range and variety of complex technical and/or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/organizational requirements.
Business skills	Advises on the available standards, methods, tools and applications relevant to own specialism and can make appropriate choices from alternatives. Analyses, designs, plans, executes, and evaluates work to time, cost and quality targets. Assesses and evaluates risk. Communicates effectively, both formally and informally. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Takes all requirements into account when making proposals. Takes initiative to keep skills up to date. Mentors colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for continuous operational improvement. Demonstrates creativity, innovation and ethical thinking in applying solutions for the benefit of the customer/stakeholder.

Independent judgment and initiative are important and valued, but must never result in operational silos or sub-optimization within the organization. Frequent communication with other DHIN leaders is essential to ensure that the leadership team is united in expectations and execution.

The ideal candidate will be prepared to step outside of traditional job boundaries to meet the needs of the moment in support of the DHIN mission, and therefore must be flexible and adaptable to changing circumstances. A strong work ethic and ability to work well within a team are essential. The ideal candidate must have strong computer skills and excellent verbal and written communication skills, be exceedingly well organized, attentive to detail, flexible, proactive, resourceful, and efficient, and must remain poised and composed under pressure and maintain utmost confidentiality and professionalism in handling protected health information and information which is proprietary and confidential to DHIN's vendors and technology partners. DHIN seeks candidates who are committed to lifelong learning and growth.

The position is primarily located at the DHIN headquarters in Dover, DE. However, following a period of orientation, a great degree of flexibility in work hours and location are possible. Many of DHIN staff work from home one or more days each week.

Scope of Work:

Principle Duties and Responsibilities

- Collaborate with the DHIN Privacy Officer and Security officer to develop, and maintain documentation, tools and methodologies for the privacy and security programs.
- Be familiar with all DHIN policies and update those policies when needed as privacy and security requirements change.

- Conduct Privacy and Security Risk Assessment Management including third party, internal and HITRUST assessments.
- Participate in external Privacy and Security advisory groups.
- Manage the Information Security internal advisory work group.
- Manage monitoring activities related to or required by HITRUST.
- Manage DHIN's relationship with HITRUST and DHIN's HITRUST assessor.
- Manage and execute the Employee Education and Awareness program for Privacy and Security.
- Manage the Security Program Plan and assist with its documentation.
- Lead continuous improvement security control projects – internal, third party and HITRUST associated corrective action plans (CAPs).
- Assist in the analysis and reporting of Privacy and Security disclosures, vendor assessments, employee compliance, and other security assessment requests.
- Serve as liaison to State and Federal Agencies for communications related to Fraud, Waste and Abuse (FWA), disclosure, breach notifications etc.
- Manage the Privacy and Security escalation investigation, tracking and reporting.
- Manage the Policy and Procedure documentation annual review process.
- Serve as a subject matter expert resource for Information Security functions at DHIN.
- Make recommendations for privacy and security improvements to DHIN's vendors.

Supervision Received

- The position reports to the Chief Technology Officer (CTO).

Supervision Exercised

This position does not have formal supervision of other personnel. However, the following supervisory duties apply:

- Leads matrixed teams and provides coaching and education to staff.
- Provides staff with feedback on their privacy and security compliance.

Job Impact

- Work performed in this position impacts thousands of users of DHIN systems across the entire state of Delaware and into bordering states.
- Budget impact of this position is moderate.
- Timeline of work assigned is both periodic for projects and continuous for programs operational in nature.

Key Competencies

The following are the minimal knowledge, skills, and abilities which the Information Security Manager must possess:

1. Knowledge and strong understanding of relevant legal and regulatory requirements, such as Health Insurance Portability and Accountability Act (HIPAA), Service Organization Control (SOC) standards, NIST, HITRUST.
2. Knowledge and experience in information security management frameworks, policy and procedure development, information security assessments and audits.
3. Knowledge of risk analysis methodologies.
4. Knowledge of IT compliance and control frameworks.
5. Knowledge of technology as it relates to privacy and security controls.
6. Profound understanding of the needs of stakeholders and the impact on end users

7. Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and non-technical audiences.
8. Demonstrated ability to establish and maintain effective relationships and partnerships with key stakeholders.
9. Demonstrated ability to facilitate meetings and mediate among stakeholder groups and individuals to resolve conflicts and disagreements.
10. Strong project management skills.
11. Strong analytical skills, techniques, and technical writing skills.
12. Proficiency in the use of technology to support work activities, e.g. expertise in Microsoft Project, Microsoft 365 software, proven ability to develop charts and graphs to summarize information for reporting.
13. Poise and ability to act calmly and competently in high-pressure, high-stress situations.
14. Ability to prioritize and organize work effectively and under pressure and with light supervision.
15. Comfortable establishing and managing plans, which include pooling multiple resources and preparing for the unknown.
16. Self-starter who pays extreme attention to detail and strives for excellence.
17. Ability to lead and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals.
18. High level of personal integrity, as well as the ability to professionally handle confidential matters, and show an appropriate level of judgment and maturity.

Qualifications

The successful candidate will possess the following experience and credentials:

- Advanced degree in computer science or information technology is preferred. Baccalaureate degree will be considered. Equivalent training and work experience relevant to the duties of the position will be considered.
- Minimum of five years of experience in information security, quality control, risk management, regulatory compliance, corporate compliance, healthcare compliance, privacy compliance or workplace safety compliance roles. Employment history must demonstrate increasing levels of responsibility.
- Certifications such as CTPRP, CISA, CISSP, CIPP, CRISC, and CISM are a plus. If not currently held, a willingness to attain one of these is expected.
- Experience in health IT and knowledge of HL7 is a plus, but is not required.
- All DHIN employees are expected to be certified in ITIL Foundations, or commit to becoming certified within the first year of employment. This is a condition of employment.

Interested parties should send resume and cover letter to careers@dhin.org or visit www.dhin.org.