Version 1.0

Date: 10/5/2019

Privacy Officer Position Description

1. 0 Purpose

To provide our members a template that can be modified and used to hire and select an employee for your company to serve as a Chief Privacy Officer. If you are an organization governed by HIPAA (See our HIPAA fact sheet), you are required to have a Chief Privacy Officer. The HIPAA Security Rule mandates that every practice or health care organization that creates, stores or transmits ePHI (Electronic Personal Health Information) must designate a privacy compliance officer regardless of their size. The General Data Protection Regulation (GDPR) also requires a Data Protection Officer, with similar responsibilities. This position description aligns with HIPAA requirements, however, can be used for non-HIPAA regulated companies.

A Privacy Officer plays an important role in an organization, namely that of the face of privacy internally and externally. While a small business may not have a full-time privacy officer, there should be an employee responsible for the duties of the privacy officer. Generally, the Privacy Officer is responsible for the organization's Privacy Program including but not limited to daily operations of the program, development, implementation, and maintenance of policies and procedures, monitoring program compliance, investigation and tracking of incidents and breaches and compliance with applicable federal and state laws. The following list of duties may not apply to all businesses, but are provided as a checklist to cover all possible activities. Select all that applies to your specific business situation.

2.0 Duties

PROGRAM DEVELOPMENT AND OVERSIGHT

- Establish and lead a privacy program for our company consistent with applicable laws.
- Establish an internal privacy audit program.
- Undertake a comprehensive review of the company's data and privacy activities and ensure that they are consistent with industry best practices and our legal requirements.
- Develop and manage an organizational policy development process that includes procedures to ensure our products and services are consistent with our legal obligations.
- Establish a process for receiving, documenting, tracking, investigating and acting upon on all complaints concerning the organization's privacy policies and procedures.
- Establish with management a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity. (HIPAA)
- Provide leadership in the planning, design and evaluation of privacy and security related projects and activities.
- Periodically revise the privacy program to address changes in laws, regulations or company policy.
- Provide privacy guidance to assist in the identification, implementation and maintenance of our organization's information policies and procedures. Ensure new projects have a privacy review before implementation.

Version 1.0

Date: 10/5/19

Privacy Officer Position Description

COMPLIANCE and COORDINATION

- Coordinate with general counsel, external affairs and business units to ensure both existing and new services comply with privacy and data security obligations.
- Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
- Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
- Coordinate and liase with regulatory and accrediting bodies as necessary. Work with management to develop relationships with regulators and other government officials responsible for privacy and data security issues.
- Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
- Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.
- Work with organizational senior management to establish an organization-wide Privacy Oversight Committee.
- Serve in a leadership role for Privacy Oversight Committee activities.
- Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations
- Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
- Work cooperatively with applicable organizational units in overseeing consumer information access rights (GDPR).
- Serve as the information privacy liaison for users of technology systems.

DATA GOVERNANCE

- Assure that the use of technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information
- Monitor systems development and operations for security and privacy compliance
- Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected.

Privacy Officer Position Description

- Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions
- Review all system-related information security plans to ensure alignment between security and privacy practices
- Work with all company personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements
- Account for and administer individual requests for release or disclosure of personal and/or protected information.

OPERATIONS

- Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Assist business units with development of tools and methodologies to ensure on-going compliance.
- Provide strategic guidance to corporate officers regarding information resources and technology.
- Assist the Security Officer with the development and implementation of an information infrastructure
- Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements
- Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed
- Act as, or work with, counsel relating to business partner contracts
- Mitigate effects of a use or disclosure of personal information by employees or business partners
- Develop and apply corrective action procedures
- Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel
- Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations
- Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties
- Conduct on-going privacy training and awareness activities

Version 1.0 Date: 10/5/19

Privacy Officer Position Description

Privacy Officer Candidate Skills Required:

- Experience as a Privacy Officer or knowledge of privacy protection laws and data breach laws.
- Solid knowledge of national data protection laws and history of privacy laws.
- Knowledge of data processing operations in the company's sector is preferable.
- Familiarity with computer security systems.
- Ability to handle confidential information.
- Ethical, with the ability to remain impartial and report all noncompliance.
- Organizational skills with attention to detail.
- Demonstrated leadership skills achieving stated objectives involving a diverse set of stakeholders and managing varied projects.
- Demonstrated negotiation skills to interface successfully.
- Demonstrated client relationship skills to continuously coordinate with other company personnel while maintaining independence.
- Demonstrated communication skills to speak with a wide-ranging audience, from the board of directors, managers, IT staff and/or lawyers.
- Demonstrated self-starter with ability to gain required knowledge in dynamic environments.
- Demonstrated record of engaging with emerging laws and technologies.
- Experience in legal and technical training and in awareness raising.
- Experience in dealing successfully with different business cultures and industries.
- Professionally licensed as a lawyer, an information security or privacy professional.