Help Wanted: Privacy Officer

Save to myBoK

Sample Position Description

Position Title: (Chief) Privacy Officer[1]

Immediate Supervisor: Chief Executive Officer, Senior Executive, or Health Information Management (HIM) Department Head[2]

General Purpose: The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, patient health information in compliance with federal and state laws and the healthcare organization's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee,[3] and legal counsel.
- Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.
- Serves in a leadership role for the Privacy Oversight Committee's activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works 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.
- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates,and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Establishes with management and operations 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.
- Works cooperatively with the HIM Director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking 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.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.

- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
- Serves as a member of, or liaison to, the organization's IRB or Privacy Committee,[4] should one exist. Also serves as the information privacy liaison for users of clinical and administrative systems.
- Reviews all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Serves as information privacy consultant to the organization for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications:

- Certification as an RHIA or RHIT with education and experience relative to the size and scope of the organization.
- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of HIM, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

This description is intended to serve as a scalable framework for organizations in development of a position description for the privacy officer.

Notes

1. The title for this position will vary from organization to organization, and may not be the primary title of the individual serving in the position. "Chief" would most likely refer to very large integrated delivery systems. The term "privacy officer" is specifically mention in the HIPAA Privacy Regulation.
2. Again, the supervisor for this position will vary depending on the institution and its size. Since many of the functions are already inherent in the Health Information or Medical Records Department or function, many organizations may elect to keep this function in that department.
3. The "Privacy Oversight Committee" described here is a recommendation of AHIMA, and should not be considered the same as the "Privacy Committee" described in the HIPAA privacy regulation. A privacy oversight committee could include representation from the organization's senior administration, in addition to departments and individuals who can lend an organization-wide perspective to privacy implementation and compliance.
4. Not all organizations will have an Institutional Review Board (IRB) or Privacy Committee for oversight of research activities. However, should such bodies be present or require establishment under HIPAA or other federal or state requirements, the privacy officer will need to work with this group(s) to ensure authorizations and awareness are established where needed or required.

The Official Position of AHIMA

Position

The American Health Information Management Association (AHIMA) recognizes the increased complexity of protecting patients' privacy while managing access to, and release of, information about patients and other healthcare consumers. Credentialed health information management (HIM) professionals-because of their academic preparation, work experience, commitment to patient advocacy, and professional code of ethics-are uniquely qualified to assume positions as designated privacy officials as required by the Health Insurance Portability and Accountability Act (HIPAA).

Background

Healthcare is a service industry that relies on information for every facet of its delivery. Health information has value to the patient it describes, the provider it serves, and the organization it supports, in addition to society as it directs the health of the population. It must be protected as a valuable asset, and in its primary form as the medical record of a unique individual, it must be safeguarded.

Privacy concerns grow as technology increases access to health information. Mental health, substance abuse, sexually transmitted disease, and now genetic information create a heightened awareness of the need for privacy. Documented cases of the use of health information to make decisions about hiring, firing, loan approval, and to develop consumer marketing have sensitized the public to the risks of sharing information with their healthcare provider.

For years, states have written laws and regulations to protect their citizens' privacy by limiting release of information based on the requestor, the type of information, and the use of that information. Due to the complexity of the issue, the number of concerned parties, and the variety of health information, no two states have the same laws.

Over the last 10 years, the federal government has tried to address the patchwork nature of state laws by developing comprehensive federal legislation, but has failed to complete that task. In an effort to ensure all citizens have a standard minimum protection, the Department of Health and Human Services has promulgated regulation under the authority of HIPAA to provide a universal floor of protection. However, the industry is already concerned with meeting this new minimal level.

To ensure the necessary leadership for compliance, the Standards for Privacy of Individually Identifiable Health Information released in December 2000, require that each health plan, healthcare clearinghouse, and certain healthcare providers must designate a privacy official who is responsible for the development and implementation of their policies and procedures relative to privacy.

HIM professionals have effectively managed the release of information in healthcare organizations for decades. Establishing policy, training staff, developing consents, releasing information, and documenting information use are key elements of the HIM role. Coursework that prepares HIM professionals to fulfill this role has long been included in the curriculum of all accredited HIM academic programs, and is included in the certification examination for both registered health information administrators and technicians. Since its formation in 1928, AHIMA has supported its members in their efforts to protect patient privacy.

Support for the position

To maintain the privacy, confidentiality, and security of health information, AHIMA members assume a leadership role in compliance with state and federal laws, develop appropriate organizational initiatives, and exercise ethical decision making. HIM professionals are uniquely qualified to assume the role of privacy officials, because we:

- Interpret state and federal laws that apply to the use of health information, into policy
- Understand the decision-making processes throughout healthcare that rely on information
- Direct the flow of information within healthcare organizations and throughout healthcare
- Apply HIM principles to information in all its forms
- Understand the content of health information in its clinical, research, and business contexts

- Apply the technologies used to collect, access, store, and transmit information in all its forms
- Establish and recognize best practices in the management of privacy of health information
- Collaborate with other healthcare professionals to ensure appropriate security measures are in place
- Historically managed the release of information function
- Advocate for the patient, relative to health information confidentiality
- Live by a Professional Code of Ethics specific to maintenance of patient privacy

---

Article citation:
"Help Wanted: Privacy Officer." *Journal of AHIMA* 72, no.6 (2001): 37-39.
