Responsibilities of the Privacy Official

Purpose

[ORGANIZATION] is committed to ensuring the privacy and security of patient health information. In order to manage the facilitation and implementation of activities related to the privacy and security of protected health information, [ORGANIZATION] will appoint and maintain an internal Privacy Officer position.

The Privacy Officer (PO) will serve as the focal point for privacy compliance-related activities and responsibilities, as listed below. In general, the PO is charged with implementing company policies and procedures, conducting educational programs, and administering reviews relating to the company's privacy program.

The PO must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel.

Responsibilities

1. Provides leadership to the company's committees, work groups, and task forces charged with creating and implementing an enterprise-wide privacy program.
    - Develops company privacy policies and procedures consistent with applicable laws, rules, and regulations.
    - Ensures that processes are implemented to maintain compliance with Federal and State laws related to privacy, security, confidentiality, and protection of information resources and health care information. This includes coordination with the [Security Officer] in evaluating and monitoring operations and systems development for security and privacy requirements.
    - Develops, implements, and administers company-wide consent and authorization procedures for access to, use, and disclosure of protected health information.
    - Develops, implements, and administers a company-wide procedure to allow individuals to exercise their rights to protected health information under applicable State and Federal Laws.
    - Develops and implements company-wide privacy training programs and, in conjunction with the [Security Officer], a security awareness and training program.
    - Coordinates with the [Corporate Compliance Officer] and Human Resources to develop appropriate sanctions for employees or business partners that fail to comply with the company's privacy policies and procedures.
    - Coordinates with [Quality Improvement Program] to measure effectiveness, performance and quality of the company's privacy program.

2. Coordinates with the [Corporate Compliance Officer] regarding corporate complaints and information relating company's privacy program and regarding investigation of all allegations of non-compliance with the company's privacy policies.
3. Coordinates with the [CCO], [Security Officer], and other applicable departments regarding the mitigation of the effects of any unauthorized or otherwise inappropriate released of health information.
4. On a periodic basis reports the status of the privacy program to the [Executive Compliance Committee].
5. Serves as resource to the company's designated liaisons to regulatory and accrediting bodies for matters relating to privacy and security.

Regulatory Authority

45 C.F.R. §164.530

(a)(1) Standard: personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.

(2) Implementation specification: personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

Analysis, Background, and Implications

In 45 C.F.R. §164.530(a), covered entities are required to designate an individual as the entity's privacy official, responsible for the implementation and development of the entity's privacy policies and procedures. The Department of Health and Human Services (DHHS) basically left the implementation details to the discretion of the covered entity. While DHHS recognizes that there may be some advantages to establishing formal qualifications, it concluded the disadvantages outweigh the advantages. Since the job of privacy official will differ substantially among organizations of varying size and function, a single set of federally specified qualifications would sacrifice flexibility and scalability in implementation. Implementation is expected to vary widely depending on the size and nature of the covered entity, with small offices assigning this as an additional duty to an existing staff person, and large organizations creating a full-time privacy official.

This designation must be documented. The designation of a privacy official within affiliated entities will depend on how the covered entity chooses to designate the component entities under 45 C.F.R. §164.504(b) – health care components. If a subsidiary is defined as a covered entity under this regulation, then a separate privacy official is required for that subsidiary covered entity. If several subsidiaries are designated as a single covered entity, pursuant to 45 C.F.R.

§164.504(b), then together they need have only a single privacy official. Further, DHHS does not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of the rule are met for each such covered entity. If several covered entities share a notice of privacy practices provided on the same premises, pursuant to 45 C.F.R. §164.520(d), that notice need designate only one privacy official for the information collected under that notice.

Furthermore, these requirements for a privacy official are consistent with the approach recommended by the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, ("Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment," p. 29)

DHHS estimates the designation of a privacy official as one of the largest cost items for covered entities in complying with the Privacy rule, at an initial year cost of $723 million and a ten-year cost $5.9 billion. Industry salary projections for Privacy Officers are estimated at an average range of $70,000 – 170,000 for a large organization that designates a full-time position. The cost calculated by DHHS is only for the ongoing, operational functions of a privacy official (e.g., clarifying procedures for staff) that are in addition to other requirements of compliance that will certainly involve the privacy officials responsibilities and duties.

