Privacy Officer Job Description, Role and Responsibility

Presentation by:

Brent Saunders

Karen Owen Dunlop

PRICEWATERHOUSECOOPERS

SIDLEY & AUSTIN
HIPAA requires health care organizations that transmit or maintain “protected health information” to designate a “Privacy Official”
Chief Privacy Officer

“CPO”

- A high-level Management or Officer Position
- The focal point for privacy compliance-related activities
Privacy Official Duties: Big Picture

- Implementing corporate policies and procedures
- Conducting educational programs
- Auditing and administering privacy program reviews
Privacy Official Access

- Board
- Chief Compliance Officer
- General Counsel
- Chief Operating Officer
Role Reflects Entity

- Size
- Structure
- Composition
- Lines of service
- Current and potential exposure to Protected Health Information – “PHI”
Role of the CPO

⇒ GENERAL:

- Leadership for privacy program
- Compliance related to privacy, security, confidentiality
- Liaison to regulatory and accrediting bodies

Continued...
GENERAL:

- Collaborate on cyber privacy and security policies and procedures
- Monitor systems development and operations for security and privacy compliance
- Counsel relating to business partner contracts
Role of the CPO

⇒ SPECIFIC

- Develop Corporate Privacy Policies & Procedures

- Handling (acquisition and management) of PHI; Corporation’s Notice of Information practices

- Use and disclosure of PHI

Continued...
⇒ Specific:

- Individual requests for Restriction of Use and Disclosure of PHI
- Access/Inspection/Copying of PHI
- Amendment/correction of PHI
- Accounting of Disclosures
- Record-keeping Procedures
- Administrative Procedures
Access/Disclosure Verification Procedures

- Individual requesting access who is the subject of the protected health information
- Emergency circumstances, including next-of-kin
- Power-of-attorney/legal authority

Continued...
Access/Disclosure
Verification Procedures

♦ Public health oversight bodies

♦ Coroners and Medical Examiners for law enforcement

♦ Government health data systems for specific classes of information

Continued...
Access/Disclosure Verification Procedures

- Disclosure required by other laws
- Financial institution non-routine transaction requests
- Judicial and administrative proceedings
- Research-related requests
Resolve allegations of non-compliance with the corporate privacy policies or notice of information practices
♦ Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee
Provide strategic guidance to corporate officers regarding information resources and technology.
-Assist the Security Officer with the development and implementation of an information infrastructure.
♦ Provide leadership in the planning, design and evaluation of privacy and security related projects
♦ Develop and implement a corporate-wide Privacy Training Program -- in conjunction with the Security Officer Oversight, Cyber Security Awareness & Training Program
♦ Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures

- Employees
- Business partners
Development and application of corrective action procedures:

♦ Mitigate effects of a use or disclosure of PHI by members of the entity’s workforce or business partners.
Establish an internal privacy audit program
Coordinate external audit processes of business Partners
Coordinate the development of privacy risk assessment policies and procedures
Periodically revise the privacy program in light of changes in laws, regulatory or company policy.
♦ Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
Thank You for your Participation

Brent Saunders
PriceWaterhouseCoopers
Phone: 202-822-4089
e-mail: brenton.saunders@us.pwcglobal.com

Karen Owen Dunlop
Sidley & Austin
Phone: 312-853-2223
e-mail: kdunlop@sidley.com