COSMOS
Navigate the Compliance Universe

Compliance Today - October 2019
The NIST Privacy Framework: An enterprise risk management tool

By Karen Greenhalgh, HCISPP, CHC, CHPC

Karen Greenhalgh (karen@cybertygr.com) is Managing Principal and Founder of Cyber Tygr in Virginia Beach, VA.

- linkedin.com/in/karen-greenhalgh

Protecting the privacy rights of individuals has become a primary goal of governments and organizations around the globe. In the U.S., Congress is considering an American version of the EU's General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is under scrutiny. The healthcare industry, still struggling with HIPAA and facing increasing privacy regulation, is recognizing that current cybersecurity and compliance programs are not structured to meet privacy needs. But how is the privacy of individuals to be effectively managed? By applying outcome-based methodology, the new National Institute of Standards and Technology (NIST) Privacy Framework treats privacy as a manageable risk.[1] This approach to privacy enables privacy compliance practitioners to state goals and achieve a measurable outcome for individuals' privacy.

An enterprise risk management tool

Scheduled for release in October 2019, the NIST Privacy Framework is the two-year culmination of intensive work by privacy experts from across the nation's public and private sectors, many from the healthcare industry. Representation by healthcare industry leaders in the creation of the Privacy Framework assures the framework will address the full scope of privacy risk. As an enterprise risk management tool, the Privacy Framework will help organizations answer the fundamental question: How are we considering the direct privacy impacts to individuals, and the secondary impact to the organization, as we develop our systems, products, and services?

Privacy vs security: Laws and regulations

Information security laws and regulations typically require risk analyses or other specific actions to assess effectiveness and allow flexibility in how controls are implemented. In contrast, privacy laws and regulatory policies typically prescribe precise obligations an organization must follow. This fixed approach to privacy produces assessments focused on compliance as rule enforcement, with less attention to measuring effectiveness of achieving a positive outcome for privacy. For example, assessments are conducted to determine whether the HIPAA-required Notice of Privacy Practices (NPP) exists, without an assessment to evaluate whether people are likely to read that notice and receive some privacy-protective benefit.

Comparing HIPAA's Security and Privacy Rules provides an example of the difficulties created by obligation-based privacy regulations.

Security Rule

- Section 164.306: Security standards: General rules. "(b) Flexibility of approach. (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

standards and implementation specifications as specified in the sub-part."[2]

- Entities are also required to perform outcome-based activities, including risk analyses, technical assessments, and non-technical assessments.

Privacy Rule

- Federal Register, page 82471: "This rule establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed settings."[3]
- Section 164.520 details the Privacy Rule's NPP for Protected Health Information (PHI), and is an example of obligation-based rigidity. This five-page section has the word "must" 26 times referring to covered entities, with no "flexibility of approach."[4]

Privacy regulations vs. security regulations

The result of enforcing privacy regulations without clear goals to measure progress is perfectly illustrated by the Office for Civil Rights (OCR) and the Department of Health and Human Services (HHS). In December 2018, the OCR/HHS issued a Request for Information on Modifying HIPAA Rules to Improve Coordinated Care.[5]

Of the 54 multi-part questions, 11 pertain to NPP because "OCR has received anecdotal evidence that individuals are not fully aware of their HIPAA rights" (which is the understood intent of the notification section of the Privacy Rule). The five-page NPP section of the Privacy Rule issues detailed rules for writing and distribution of the NPP to patients. Compliance practitioners are required to assure the myriad details in those five pages are executed. However, there is no requirement to assess comprehension by patients—the actual intent of the regulation.

Consider the outcome-based approach from using the Privacy Framework. The working draft at the time of this writing includes two subcategories: CM.AW-P1 would apply to the writing and distribution of the NPP, and CM.AW-P2 provides a measurable outcome-based action, rather than a check-the-box action:

- CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
- CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risk are established and in place.

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.