COSMOS
Navigate the Compliance Universe

Compliance Today - March 2023

Lisa Venn (lvenn@metrohealth.org, linkedin.com/in/lisa-venn-59154141/) is Privacy Counsel at The MetroHealth System, Cleveland, OH.

Building a privacy liaison program to combat ever-increasing risks

by Lisa Venn JD, MA

It is the privacy officer's trifecta of despair: an increasingly complex environment, ever-evolving risks, and a dearth of available privacy talent. As privacy counsel for a large healthcare system, I was part of a three-person privacy team grappling with multifaceted issues inherent in our ever-changing business environment.

I dreamed of an influx of seasoned privacy professionals fluent in all privacy-related issues—research, behavioral health, correctional medicine, health information exchange, patient access, and telemedicine, to name a few. In a perfect world, these eager experts would easily navigate our organization of 8,000 employees, four hospitals, and more than 20 health centers.

Sobered by a few rounds of colleague commiseration, I finally accepted the truth. The privacy cavalry is not coming. This coveted dream team would have to be developed from within the organization.

In this article, I share four steps to developing a privacy liaison program (PLP). These steps enabled us to identify the high-risk privacy areas in our organization from which we recruited liaison candidates. We developed a curriculum and trained and mentored liaisons based on how adults are motivated to learn. Finally, we integrated the PLP into our organization as liaisons share their privacy expertise and mentor the incoming PLP class.

By following these steps, our three-person privacy team was enhanced by 28 additional privacy experts capable of identifying and addressing issues within their departments.

Step 1: Identify the organization's high-risk areas

To build a successful PLP, we needed to understand the problem we aimed to solve. To this end, we identified the organization's high-risk privacy issues by analyzing internal and external data.

First, we reviewed in-house investigation data and identified departments or areas that repeatedly ran afoul of privacy requirements or had unresolved process gaps. From this information, we ranked issues by type, severity, volume, and source. We also reviewed the number and types of guidance requests the privacy team received. From this information, we identified training opportunities and potential liaison candidates.

Second, we leveraged enforcement data from oversight agencies, such as the U.S. Department of Health & Human Services Office for Civil Rights (OCR), and publications from professional organizations and industry watchdogs. For example, based on OCR's heightened enforcement of patients' right to access protected health information (PHI), we selected our release of information process for enhanced scrutiny. Also making the high-risk list are clinical areas that involve PHI that is specially protected by state and other federal laws, such as certain infectious diseases and behavioral health treatment.