Navigate the Compliance Universe

Compliance Today - November 2022

Nick Weil (nweil@epsilonlifesciences.com) is a Senior Associate at Epsilon Life Sciences in Chicago, IL.

Mayesha Awal (mawal@epsilonlifesciences.com) is an Analyst at Epsilon Life Sciences in Chicago, IL.

Why covered entities need (and how to do) a personal data inventory, Part 2

By Nick Weil CHC, CHPC, and Mayesha Awal OneTrust Privacy Fellow

This article details a personal data inventory, defines terms like 'asset' and 'data map' in detail, and provides actionable steps for undertaking these efforts in the healthcare context. Part 1 of this two-part article—published in the October 2022 issue of *Compliance Today*—examined the *why* behind the exercise.[1] In Part 2, *how* to do a data inventory is outlined.

How to do a data inventory

In Part 1, we established how necessary and helpful a personal data inventory is for covered entities and business associates. Not only do several laws and regulations require them, but they also provide enormous compliance, privacy, security, and strategic benefits. But we should be clear upfront: a data inventory is not a casual exercise. Not only does it involve dozens of responsive individuals across the company, but it is also time and resource intensive. For example, when conducting data inventories for organizations, we often plan for over a hundred hours to be spent on the project. There is a commitment involved in this undertaking. But as we saw in the prior article, it is well worth the effort.

Terms and concepts

There are a couple of definitions to note before we jump into the process of data inventory:

- **Assets** are any repositories of information. This can be a system, application, database, device, or even a file cabinet.
- **Data inventory** is a register of activities and assets that process personal information.
- **Data map** is the visualized flow of personal information between different assets and activities, from the beginning of the data life cycle (e.g., collection) to its end (e.g., destruction).
- **Personal information** is any data that can be used to distinguish or trace an individual's identity, either alone or combined with other data linked or linkable to a specific individual. Protected health information (PHI) is a subset of personal information most familiar to HIPAA organizations, but keep in mind, personal information means identifiable data about *any* natural person: employees, contractors, or family members.
- **Processing** is any action on data, including use, storage, transmission, anonymization, archiving,

exchange, or destruction.

- **Processing activities** are business functions utilizing personal information at a given company. This might be marketing, patient care, billing, or operations.

A data inventory is best considered a matrix of assets and processing activities. Business functions and the systems that support them exist in a many-to-many relationship: one asset might support multiple activities, each of which has any number of assets backing them. A good example is your electronic health record (EHR). This critical asset probably supports many processing activities at your healthcare organization (treatment, medical records, billing, etc.). At the same time, each processing activity might have multiple assets supporting EHR, shared folders or drives, or email. Think of the output of an inventory as an Excel spreadsheet: the columns list where and the rows show how data is processed at your company.