COSMOS
Navigate the Compliance Universe

Compliance Today - October 2022

Nick Weil
(nweil@epsilonlifesciences.com) is a Senior Associateat 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 1

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

Part 2 of this article series details personal data inventory, defines terms like "asset" and "data map" in detail, and provides actionable steps for undertaking these efforts in the healthcare context. But before we get to the how-to guide, the first part of our piece will examine the *why* behind the exercise.

We know from our experience working with HIPAA-covered providers, plans, and their business associates that they are not in the habit of doing data inventories. This is unusual among data-rich and rule-heavy industries, and healthcare is well behind other sectors in this regard. For those who need convincing or tips for obtaining buy-in from decision-makers, the first part of this piece will examine the commonsense reasons, best practice standards, legal requirements, and practical usefulness driving a data inventory exercise.

Part 1: Why do a data inventory

A medieval metaphor

Imagine you are charged with guarding a feudal castle. What would your first task be? Assuming your fort already had a gate and a moat, what next? Lacking unlimited money, time, and workforce, a castellan should prioritize action where need is greatest.

But how do you know where you are needed? By getting the lay of the land, of course. You might inspect the wall, walk the perimeter, and watch where folks come in and go out the castle. Everybody rushes to secure the front door, but what about the old stone wall at the back? The drain and the well? The river door by the dock? Where does the trash get out? Could someone come in that way? Could they dig through the moat? Climb the west wall? A map would be an indispensable tool for the job, but to be certain it is accurate, you might need to make your own, or update an existing one with current observations.

Visual inspection by itself would miss the human factors at work: error, carelessness, fraud, etc. Talking to the people who use the place would be essential as well. The soldiers at the gate are obvious subjects, but so are the cook, blacksmith, builder, priest, and king—even the farmer selling his crops—anyone who could help you build the inventory of who comes in and what goes out.

Once you have a complete picture, you can plan well. An urgent need might demand an immediate fix before the plan is finished ("There's a hole in this wall!"), but you couldn't deploy your limited resources efficiently until you were confident in your priorities, until the map was clear and the inventory current. Would you trust the captain who said he'd secured the fortress without knowing every entryway? Could you be confident in the guard

who did not know the castle's ways and means?

An industry standard

This protracted metaphor illustrates the logic behind a personal data inventory. A grasp of the relevant ecosystem is necessary before assessing risk.

But don't just take our word for it. Here is an industry standard to consider: the National Institute of Standards and Technology's Privacy Framework (NIST-P) of 2020 (Table 1). The function that begins the NIST-P framework is IDENTIFY, and the first category under it is *Inventory and Mapping*, described as "Data processing by systems, products, or services is understood and informs the management of privacy risk."[1]

Function	Categories
IDENTIFY-P (ID-P)	Inventory and Mapping (ID.IM-P) Business Environment (ID.BE-P) Risk Assessment (ID.RA-P) Data Processing Ecosystem Risk Management (ID.DE-P)
GOVERN-P (GV-P)	Governance Policies, Processes, and Procedures (GV.PO-P) Risk Management Strategy (GV.RM-P) Awareness and Training (GV.AT-P) Monitoring and Review (GV.MT-P)
CONTROL-P (CT-P)	Data Processing Policies, Processes, and Procedures (CT.PO-P) Data Processing Management (CT.DM-P) Disassociated Processing (CT.DP-P)
COMMUNICATE-P (CM-P)	Communication Policies, Processes, and Procedures (CM.PO-P) Data Processing Awareness (CM.AW-P)
PROTECT-P (PR-P)	Data Protection Policies, Processes, and Procedures (PR.PO-P) Identity Management, Authentication, and Access Control (PR.AC-P) Data Security (PR.DS-P) Maintenance (PR.MA-P) Protective Technology (PR.PT-P)

Table 1: NIST Privacy Framework

This category standard drills further into subcategory specifications: asking whether the organization has inventoried its data elements, data subjects, owners, users, recipients, and purposes.

Importantly, inventory is the first step that NIST expects of an organization that processes personal information. Note, too, that the inventory step comes before risk assessment, policies and procedures, and governance and risk management. Identifying the universe of data, actions, and actors is the industry-recognized first step in an effective privacy program.

The legal case

Healthcare companies lacking a data inventory are atypical among those organizations with sensitive data and active regulatory bodies. Financial services, technology, retail, manufacturing, and many others have been conducting and maintaining data inventories and maps for nearly a decade. This is due, in part, to the fact that they are more likely to be subject to the European Union's General Data Protection Regulation (GDPR) and its record of processing activities requirement. Similarly, recent state privacy laws, like the California Consumer Privacy Act (CCPA), heavily imply a data inventory requirement to meet its rules for public notice of the categories of data processing by the organization.

Another recent article in *Compliance Today* demonstrated that these and other new data privacy laws are more applicable to HIPAA organizations than is commonly realized.[2] This presents two reasons to conduct personal information inventory: to simply meet these requirements if your organization is subject to them, but also to establish what personal data you have to determine which regulations apply.

More to the point, many covered entities and business associates have missed that an inventory of electronic protected health information (ePHI) assets is a de facto expectation under the HIPAA Security Rule, too. The rule requires organizations to assess ePHI risk in their environments; control access to systems that contain ePHI; and secure the places that store, process, and transmit ePHI. How can covered entities and business associates functionally accomplish any of these without a comprehensive grasp of all the places where ePHI exists in the organization?

The U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) has confirmed this in guidance, stating that a thorough risk analysis includes "taking inventory of all systems and applications that are used to access and house data."[3] It even dedicated its "Summer 2020 OCR Cybersecurity Newsletter" to recommending how covered entities and business associates should inventory their IT assets.[4]

Recent trends in health information compliance also confirm the need for data inventories. The Information Blocking Rule—which prohibits organizations from blocking the access, exchange, or use of health information—requires a covered actor to know what information it has. Similar privacy laws across states like Virginia, Colorado, Utah, and California grant residents the right to know, access, edit, and delete personal data.

Inventory benefits

Before we move on to the "how," it must be noted there are many advantages to conducting a data inventory and having a data map. First, as we described, it greatly improves the privacy risk management process. Imagine the gain in clearly visualizing every place that maintains protected health information (PHI), all activities that process it, and each vendor who receives it. It's something you could (and perhaps should) build your HIPAA program around.

But regulatory compliance is not the only function that benefits from a data inventory: cybersecurity, health information management, medical records, legal, data governance, marketing, operations, and research and development—the list is practically endless. Anybody who needs data to do their job would benefit from knowing what and where all the data is. Information is risky but also valuable, which is why the modern economy is founded on it.

Let's highlight two departments that commonly work alongside privacy staff and might use a data inventory: legal and security. Legal is often charged with three tasks that are made exponentially easier with a data inventory: contract management, litigation discovery, and record retention. The data vendors, elements, and locations cataloged support each function. With a data inventory in hand, your organization's lawyers can ensure the correct agreements are in place with the right vendors (e.g., business associate agreements). They can find

necessary data quickly and efficiently when defending the organization from litigation or investigation; they will find it easier to ensure business records are maintained in compliance with law and policy.

Finally, as was clear from our castle analogy, security professionals tasked with maintaining the integrity, availability, and confidentiality of information assets would find immense value in an accurate personal data registry. A data inventory allows security to survey every system, application, and database storing PHI for critical controls like encryption protocols, backup status, and threat protection. Identifying business assets is fundamental to an effective information security program.

Indeed, the Center for Internet Security recommends as much in its Critical Security Controls framework.[5] This, plus the NIST-P, makes two different industry standards that recommend a data inventory. A recent amendment to the Health Information Technology for Economic and Clinical Health Act requires HHS to give credit to an organization experiencing a HIPAA breach if they can demonstrate they had "recognized security practices" 12 months before the breach.[6] This includes lowering HIPAA fines, early and favorable resolution of a HIPAA audit, and mitigation of remedies under an HHS resolution agreement. That's a benefit that will impress compliance, legal, and security stakeholders.