A RESOURCE OF THE 2020 DATA EMPOWERMENT REPORT

Getting Started With a Data Inventory

You need to know what you have in order to protect it. An inventory of the data you store is a necessary first step in building useful policies or training your staff. Ask yourself three questions: What data do we have? Where is it stored? How is it transmitted?

What is a Data Inventory?

A data inventory is the foundation of data policy for your organization. To start, develop a simple table that lists the kinds of data in your organization, what sensitive information is included, and where that data should be stored. Then, a data inventory should be widely distributed, posted, and well known by your staff.

We've provided a template Excel document you can use to inventory the data in your own organization. Follow along below as we walk through the critical aspects of any inventory. Customizing the template is better to create something that works for your organization rather than feeling stuck in a specific format. The only requirement is to keep it simple enough for end-users to understand. Use non-technical language and limit the length. If you can't construct an entire inventory with ten rows or fewer, consider having a data inventory for each team.

Here's an example:

WHAT DATA?	WHAT'S INCLUDED?	WHERE IS IT STORED?
Client health records	SSN, private medical information, demographics, provided forms, test results	Only in our Electronic Medical Health Records system
Exported outcomes data	Internal client ID #s and various test and demographic data.	Approved staff may keep this data on encrypted laptops or on the secure network drive. Aggregated, non-identifiable information can be kept by anyone on any approved file storage tool.
Staff HR records	SSN, demographics, health information, employment records, accommodation needs.	In the secure HR cloud drive or on HR staff encrypted laptops. Some information will be in the email accounts of HR staff.
Identifiable donor information	Names, addresses, demographics.	In our cloud donor database. Any exported data that retain identifiable information can only be kept on the encrypted laptops of approved staff.
Case notes	Names, identifiers, detailed personal records.	This data may be temporarily stored as documents on the case workers' encrypted laptops. These files must be deleted after the information has been transferred to our Electronic Medical Records system.

Ways to transfer data safely

Where you *store* the data is only part of the problem. Your staff also needs to understand how to safely transfer that data. We can use the data inventory for this too. Just add additional columns explaining how this data can be transferred.

Safe transfer is not necessarily *ethical* transfer. So, in addition to the inventory, you'll need data-sharing guidelines for your departments. These guides will be nuanced, reflecting the individual work of each team. But they should cover sharing data with other staff, guardians, wellness practitioners, funders, and partner organizations.:

Here's an example of a safe transfer policy:

What Data	EMHR messaging & portal	Regular email internal people	Regular email external people	Encrypted Email	Anonymous Sharing Links	Authenticated Links	Phone	Voice	Text
Client health records	✓			✓		✓	✓		
Exported outcomes data		✓		✓	✓	✓	✓		
Staff HR records		✓				✓	✓		
Identifiable donor information		✓	✓			✓	✓		
Case notes	✓			✓			✓		

Data Retention

We shouldn't make the mistake of storing data indefinitely. The longer we have data, the greater the chance data will be lost or stolen. And the older the data becomes, the less accurate it is about our constituents, staff, and donors. The only data we need to keep "forever" for most nonprofits is aggregate outcomes data and information in our accounting system. Identifiable information – particularly sensitive identifiable information – should be deleted or anonymized as soon as possible.

You'll need to consider laws, ethics, and practicalities when deciding how long data should be stored (in that order). For each kind of data, ask yourself the following questions, then add a note in your data inventory how long the data should be kept for:

- Am I required by local, state, or federal law to keep this data? For how long?
- Am I required by a funder to keep this data? For how long?
- What is the potential impact to clients and our organization if this data is lost? Should I feel an urgency about deleting this data as soon as possible?
- How far back do I realistically need to go for this kind of data? What's the furthermost back I've gone in recent memory?
- When considering year-over-year reporting, how far back can I go and still reasonably compare detailed and identifiable data from today to data from the past?
- Are there alternatives to keeping this identifiable information? Can I anonymize it? Export aggregate statistics? What are my other options?

The duration should be kept in your data inventory. However, you'll still need a plan to delete the old data. Review our **Data Policies Your Nonprofit Needs** article (an additional resource of the Data Empowerment Report) for a sample data retention policy and other ideas to keep your staff and communities safe.