STORE + TRACK YOUR DATA:
Data Confidentiality for Nonprofits

More emPower Tools
+ learn more about each topic
thecapacitycollective.org/resources

Purpose: This tool can help support non-profits in data protection planning. With expanding risks and regulations, data security is important to:

- Keep clients' personal information confidential.
- Maintain trust in relationships you have with clients, employees and donors.
- Make sure you are in legal compliance so your good work can continue!
- Develop mechanisms for data confidentiality that still are user friendly for non-profit employees

Framework for Protecting Information

Whose Information?

Clients: most importantly, we have an obligation to protect the private information of clients who are depending on our services

Employees: your employees likely are providing private information as part of their hiring process.

Donors: you may be collecting information from volunteers or donors.

What Information? PII[1]

The first step to protecting sensitive information that is collected and stored by the non-profit is knowing what information we are talking about! **Personally identifiable information, or PII**, can be defined in several different ways. However, in general:

- **Includes:** first and last name *AND* other identifying information that can be used to identify, contact, or locate an individual person, or to identify an individual in context (e.g., email addresses/password, SSNs and driver's license numbers, biometric data, medical or financial info)
- **Does not include:** city or state of residence, zip code, area code, gender, age, or aggregate data that cannot be broken down to identify a specific individual; publicly-available information

What's the Threat?

Unintentional privacy breaches from everyday activities are the most common risks to data privacy, although hackers certainly do exist. Some **common privacy breaches** occur when:

- **Storing and transferring** PII about employees, volunteers, donors, and clients
- Allowing community **partners or volunteers** to access PII without safeguards
- **Storing** PII on cloud servers or systems or allowing access to PII on laptops and smartphones without safeguards
- **Processing** payments or event registrations online, or using an unknown online platform to collect information

Legal Landscape

There is no single, comprehensive law regulating privacy and the collection, use, processing, disclosure and security of PII in the US. Instead, there are **many laws governing privacy and PII**:

- **Federal** rules that are specific to sector (e.g., COPPA, GLBA, HIPAA, TCPA, FCRA, FERPA)
- **State** laws (i.e. laws that say what you should do if there is a data breach)
- **Common law** principles (invasion of privacy, negligence, etc.)
- **Best-practices** in the industry (i.e., regulations that are not laws but are considered best practices)

See Microsoft's Guidelines for Cybersecurity and Privacy, nonprofitrisk.org, and councilofnonprofits.org for more information.

Best Practices in Data Privacy

Program level

Use a data confidentiality agreement: Everyone who may see or interact with clients' personal information and stories should sign a confidentiality agreement. This includes staff, volunteers, and external consultants.

Check security when working online: (1) any online payments or information with PII exchange should be done using a secure browser connection *(look for small lock in lower right or upper left corner of web browser!)* (2) erase the web browser cache and history regularly. Always erase these data after using any public computer.

Handle PII with transparency, fairness and lawfulness. Nonprofits should communicate clearly with donors, employees, and clients how personal data is being used.

Minimize collection and storage of PII so that you collect and keep only what you need. Get rid of all information you are not using and legally able to delete to limit the possibilities of a data breach.

- Shred physical documents, and delete electronic documents with PII
- Streamline storage: minimize places that PII is being stored
- Streamline/minimize access points to PII: minimize devices to access and platforms that contain PII

Ensure accuracy of PII and enable it to be erased or rectified. Should be able to edit, correct, or delete!

Personal Practice

Keep your computer secure.

- *Be careful of email attachments, web links, and pop-ups:* Do not click on a link/attachment you were not expecting.
- *Be careful downloading software:* do not download software from an unknown web page.
- *Do not connect personal or untrusted storage devices* or hardware into computers (like USBs).

Use separate personal and work computers, cell phones and accounts as much as possible.

- Limit work-related communication on personal devices.
- Don't do web surfing, gaming, downloading videos, etc., on work devices.
- Don't send work-related information to your personal email addresses.

Protect the PII on your computer.

- *Use strong passwords.* use random sequence of letters (upper case and lower case), numbers, and special characters.
- *Encrypt (code to protect) PII in storage and transit* do this as much as possible, especially when transferring or sending
- *Be aware you're your screen.* Don't leave your computer with PII unattended or easy to see.

Watch out when providing personal or organizational information. Never give out usernames or passwords; if you are ever suspicious about a request, ask your supervisor before providing information.

Steps to Putting Data Confidentiality into Practice

1. **Know your current practices**
   Take time to map out the following questions: (1) What data do we collect about people? (2) What do we do with it? (3) From where is it accessed? (4) Where do we store it? (5) Who is responsible for it?
   This information inventory should be regularly updated.
2. **Create an internal privacy policy:** many organizations get external legal advice to create this. Policy should include the practical safeguards and practices to ensure legal requirements are followed.
3. **Communicate policies and best practices to all staff:** this will likely include training in the on-boarding process for new staff as well as regular staff check-ins to ensure all staff have clarity around data confidentiality practices.
4. **Communicate to stakeholders how data is being used**: this includes consent forms upfront, and ongoing communication if data is used differently than originally stated
5. **Set up reporting procedures in case of breach:** mechanisms to (1) quickly identify violations of policy, (2) how staff should communicate a concern to management, (3) how management can respond effectively, and (4) how those affected by the breach will be informed of the breach (all breaches of PII require that it is reported to the individual)