DATA PROTECTION
BEST PRACTICES FOR NONPROFITS

NONPROFIT RESILIENCY NETWORK

NYLPI
JUSTICE THROUGH COMMUNITY POWER

Lawyers Alliance FOR NEW YORK
Connecting Lawyers, Nonprofits, and Communities

DATA PROTECTION BEST PRACTICES FOR NONPROFITS

People seeking assistance from nonprofit organizations often entrust the nonprofits with their most sensitive personal information. Safeguarding that information is essential to keep clients safe, to build trust, and to satisfy the organizations' own legal and ethical obligations. Developing strong data practices to protect sensitive client data is especially important in anticipation of enhanced oversight and investigation by the new federal administration. As with many of the challenges brought in this new landscape, New York Lawyers for the Public Interest and Lawyers Alliance for New York are working quickly to meet the needs of the nonprofit sector, we issue this Data Protection Best Practices Guide to help meet the concerns nonprofits are raising. Our unique positions allow us to be nimble and responsive to the needs and growing concerns of the nonprofit sector. We have developed this guide to outline and establish best practices.

This guide identifies six key data protection best practices:

1. Know what information you possess and where and how you keep it;
2. Avoid collecting unnecessary information, and delete extraneous data;
3. Implement internal data privacy policies and procedures;
4. Develop a plan to respond to government subpoenas and educate staff;
5. Review third-party data sharing arrangements to understand obligations and impose appropriate restrictions; and
6. Implement technical and organizational measures to protect your organization's data.

We explain each recommendation in the following guide.

This information is current as of May 2025, and should not be considered comprehensive, particularly given that legislative and administrative policies and priorities are evolving, and will continue to evolve, in real time. This is not a substitute for, and should not be relied upon as, legal or professional advice; we recommend that you consult professional advisors for guidance on your individual circumstances. Nothing contained herein creates an attorney-client relationship with New York Lawyers for the Public Interest or Lawyers Alliance for New York.

If you have any questions about this guide, please contact NYLPI via https://bit.ly/ClearinghouseIntake or Lawyers Alliance via (212) 219-1800 x224 or ResourceCall@lawyersalliance.org. For information about our organizations, visit www.nylpi.org and www.lawyersalliance.org.

DEVELOP DATA MAPS/INVENTORIES

▶ IMPLEMENTATION CONSIDERATIONS

Organizations should create an **inventory of all data** collected and processed in connection with the provision of their services and internal operations, particularly with respect to clients' personally identifiable information.

A data map/inventory should:

1. Identify the categories of data collected (e.g., names, addresses, contact information, immigration status, case history);
2. Classify data based on sensitivity and criticality, and identify any relevant legal, regulatory or contractual requirements. Understand any legal protections for certain types of data, including Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), attorney-client privilege, therapist privilege, etc. It's a critical step to preparing for demands to access the data (and each has specific requirements to preserve privilege and protections);
3. Map the sources from which such data is collected and for what purpose it is being used;

(Continues on next page)

DEVELOP DATA MAPS/INVENTORIES

▶ IMPLEMENTATION CONSIDERATIONS

(Continued from previous page)

4. Track where the data is stored, who has access to such data (e.g., internal staff, volunteers, vendors) and for how long the data is being retained; and
5. List the third parties to whom such data is disclosed or otherwise accessed by, and what agreements govern such disclosure or access.

Data maps should be **reviewed and updated regularly** for completeness and accuracy.

WHY IS THIS IMPORTANT?

It is important to understand what data your organization is collecting, how it is being used and shared, and how long it is intended to be stored in order to identify what data it has access to and to develop data governance policies and procedures tailored to the nature and sensitivity of such data.

EMPLOY DATA MINIMIZATION

INCLUDING BY DELETING DATA WHEN IT IS NO LONGER NEEDED TO ACHIEVE THE PURPOSE FOR WHICH IT WAS ORIGINALLY COLLECTED

▶ IMPLEMENTATION CONSIDERATIONS

Organizations should minimize the amount of data collected to only what is **necessary and proportionate** to perform a particular function, and should **consider deleting** or, if no longer needed in an identifiable form, **anonymizing, aggregating or de-identifying data** once the purpose for which such data was originally collected has been fulfilled, unless otherwise required to be maintained by applicable law.

With respect to data deletion, nonprofit organizations should pay close attention to any legal or contractual requirements to retain specific types of data, even if no longer needed for the originally collected purpose. For example, nonprofit organizations should closely review any record-keeping obligations under their grant agreements to ensure compliance and avoid liability for breach of contractual obligations.

WHY IS THIS IMPORTANT?

The best way to ensure client confidentiality and privacy and to limit third party access (whether authorized or otherwise) to such information is by minimizing the information collected and stored. Deleting or anonymizing client information as soon as it is not needed will protect access to sensitive client data and minimize the risk of data breaches.

IMPLEMENT DATA PROTECTION POLICIES AND PROCEDURES

▶ IMPLEMENTATION CONSIDERATIONS

Drafting and implementing data protection policies and procedures (e.g., **data classification and handling policies, data usage policies, data sharing standards, incident response plans, data retention/deletion schedules**) are paramount to ensuring enterprise-wide compliance with data protection best practices. Such policies and procedures should be **tailored based on an organization's data map/ inventory, and take into account the organization's specific data protection compliance obligations** (e.g., legal and contractual obligations and restrictions on data collection and use) and the risks specific to the types of data collected (e.g., heightened protections may be required with respect to highly sensitive data).

Organizations should closely monitor staff compliance with data protection policies and procedures, and regularly audit, review and refine such policies and procedures in light of changing legal requirements and an organization's specific risk assessments.

WHY IS THIS IMPORTANT?

Not only will implementing such policies and procedures assist an organization with its legal and contractual compliance obligations, but documentation of such policies serves to provide a framework to enable an organization to maintain data confidentiality, integrity and availability, and prevent unauthorized data access, use or disclosure.

DEVELOP A PLAN TO RESPOND TO GOVERNMENT SUBPOENAS,
AND EDUCATE AND TRAIN STAFF ACCORDINGLY

▶ IMPLEMENTATION CONSIDERATIONS

Upon receipt of a government subpoena or investigatory demand for access to confidential client data, a nonprofit organization should first **notify necessary parties** (i.e., any general counsel, president, leadership, etc.) **of such receipt and issue a "hold"** over any relevant documents or other information that may be responsive to the request (i.e., by directing staff not to destroy potentially responsive material in their possession).

Based on a factual assessment of the request in consultation with legal counsel, organizations can consider responding to the request by:

1. Contacting the party who issued the subpoena in an attempt to informally resolve the issue and determine what information the party is seeking;
2. Serving written objections to a document subpoena;
3. Moving to quash (or modify) the subpoena or moving for a protective order;
4. Contacting an adverse party (that is, a party to the litigation whose interests are adverse to those of the party that issued the subpoena) in an attempt to have the adverse party exercise its rights against the party who issued the subpoena; or

(Continues on next page)

DEVELOP A PLAN TO RESPOND TO GOVERNMENT SUBPOENAS,
AND EDUCATE AND TRAIN STAFF ACCORDINGLY

▶ IMPLEMENTATION CONSIDERATIONS

(Continued from previous page)

5. Complying narrowly with legally required portions of the subpoena and providing the requested testimony or documents.

If the organization receives a federal grand jury subpoena, special considerations will apply. Counsel will want to negotiate the scope and timing of any response directly with the government (and there are unlikely to be any third parties involved due to grand jury secrecy requirements). If an appropriate scope cannot be negotiated, or the organization has some other basis to object, the organization can move to quash the subpoena, but note that deference is typically provided to the grand jury's demands in a criminal investigation.

Determining how to respond to (and thus whether to comply with) the subpoena is a strategic step, and may require weighing multiple considerations, each of which should be **carefully considered with legal counsel on a case-by-case basis.**

WHY IS THIS IMPORTANT?

A subpoena cannot command an organization to produce documents that are not in its "possession, custody or control." Therefore, following the data protection tips listed in this guide can help ensure that your organization does not retain excess, sensitive information, which in turn helps protect your clients and organization from having to produce such data in response to a subpoena.

REVIEW DATA SHARING ARRANGEMENTS

TO UNDERSTAND OBLIGATIONS / IMPOSE APPROPRIATE RESTRICTIONS

▶ IMPLEMENTATION CONSIDERATIONS

Organizations frequently share confidential data with, or receive confidential data from, third party organizations, lessening the organization's ability to maintain control over data hygiene and use. Many nonprofits store files offsite and data in the cloud maintained by vendors for a variety of purposes, including case management, document storage, data analysis, contact management, and communications.

When entering into contracts with third-parties to whom you provide confidential client data, an organization should consider:

1. **Conducting due diligence** into third-party vendors to understand their data privacy and security posture and the measures utilized to protect confidential data;
2. Ensuring all vendor contracts **impose proper protections for cybersecurity and confidentiality**, including by entering into NDAs with all third-parties to whom confidential client data is provided or who otherwise access confidential client data; and
3. Imposing obligations on third-party vendors to **notify you in the event of a data breach** as well as to coordinate with you, where legally allowed, when client data is subpoenaed or otherwise subject to a governmental order or other request.

(Continues on next page)

REVIEW DATA SHARING ARRANGEMENTS

TO UNDERSTAND OBLIGATIONS / IMPOSE APPROPRIATE RESTRICTIONS

▶ IMPLEMENTATION CONSIDERATIONS

(Continued from previous page)

Typical provisions in data related contracts may include:

1. **Allocation of data ownership** between the parties (both for existing and newly created or derived data);
2. **Standard confidentiality provisions** imposing restrictions on the data recipient's use, disclosure and retention of data;
3. **Where personally identifiable information is implicated:**
    a. Customary representations and warranties, including compliance with applicable data privacy laws, the terms of applicable privacy policies or notices and/or the relevant terms of any applicable contracts related to data processing;
    b. Allocation of responsibility for responding to and honoring consumer privacy rights requests;
    c. Data breach, data misuse or other security incident notification obligations and allocation of responsibility to inform regulators and affected persons of such incident; and
    d. Audit rights permitting the data provider to ensure compliance by the data recipient with the foregoing obligations;

(Continues on next page)

REVIEW DATA SHARING ARRANGEMENTS

TO UNDERSTAND OBLIGATIONS / IMPOSE APPROPRIATE RESTRICTIONS

▶ IMPLEMENTATION CONSIDERATIONS

(Continued from previous page)

4. **Guardrails around responding to government subpoenas or other governmental orders or demands for data access,** including sole discretion of the data provider to contest such requests or demands, and limitations regarding the data to be provided by the data recipient in response to such requests;
5. **Obligations that the data recipient implement technical and organizational measures** (e.g., access controls, encryption requirements, de-identification/anonymization standards) to protect and safeguard data;
6. **Indemnification provisions** in the event of gross negligence or other breach of data use restrictions by the data recipient; and
7. **Requirements that the data recipient delete all data** upon termination of the relevant services or the agreement unless retention is required by law (in which case any applicable confidentiality requirements should survive such termination with respect to any data retained by the data recipient).

WHY IS THIS IMPORTANT?

Client data is often stored, accessed, or processed by, and is even often collected or received from, third-party vendors, which can include sensitive client information. Conducting due diligence and imposing confidentiality obligations on third-party vendors protects client data and can limit government agencies from accessing sensitive client information through such vendors.

IMPLEMENT TECHNICAL AND ORGANIZATIONAL MEASURES TO PROTECT DATA

▶ IMPLEMENTATION CONSIDERATIONS

Organizations must **assess and ensure implementation of reasonable security procedures and practices** appropriate to the nature of the data processed in order to protect such data from unauthorized access or disclosure.

Such controls may include:

1. **Physical access controls** (e.g., requiring badges to access computers where sensitive data is stored);
2. **Technical access controls** (e.g., complex passwords, multi-factor authentication firewalls, encryption);
3. **Contractual controls** (e.g., execution of non-disclosure agreements or other data sharing agreements); or
4. **Organizational measures** (e.g., employee security and privacy awareness training to educate staff on how to identify and report data breaches or other security incidents).

(Continues on next page)

IMPLEMENT TECHNICAL AND ORGANIZATIONAL MEASURES TO PROTECT DATA

▶ IMPLEMENTATION CONSIDERATIONS

(Continued from previous page)

Organizations should also consider enhancing security by **embracing the principle of least privilege** – meaning access to data, particularly sensitive client data, should be limited to only what is necessary for a particular staff member to perform their job functions. Staff data access should be regularly audited and reviewed for compliance.

Assess the risk relevant to how you operate in practice, such as employee travel or accessing data outside the US; the right of Border Patrol to search any electronic device at entry, including the property of US citizens; the need to access data from remote locations; and the use of personal electronic devices.

WHY IS THIS IMPORTANT?

Implementing robust data security and access controls protects sensitive client data, and reduces the likelihood of unauthorized access. Such safeguards can help ensure nonprofits are complying with any applicable regulations and obligations imposed under grant agreements to protect confidential information. In addition, with recent technological advancements, particularly the advancement of artificial intelligence, threat actors are developing sophisticated tools to target nonprofit organizations to obtain sensitive client data such as social security numbers, birth dates, and other financial information. For example, threat actors have used phishing emails and AI-generated deepfakes to pose as the IRS or other government agencies, or to claim to be representatives of legitimate organizations, to gain access to sensitive client data. Employing appropriate data security measures and safeguards can help keep client data secure as well as protect your organization's reputation.

ADDITIONAL RESOURCES

Please see these additional resources for more tools related to data privacy and digital security:

- Just Futures Law: Digital Security Resources
- Ford Foundation: Cybersecurity Assessment Tool

DATED: May 6, 2025

NONPROFIT RESILIENCY NETWORK

ABOUT THE NONPROFIT RESILIENCY NETWORK

The Nonprofit Resiliency Network strengthens and protects the nonprofit sector by providing informational resources, relationship-building, practical training, and legal advice and representation to nonprofits and CBOs dealing with the changing landscape at a time when nonprofits are needed more than ever. It will foster collaboration, build capacity, and distribute essential resources and legal advice to build resilient nonprofits.

N Y L P I
JUSTICE THROUGH COMMUNITY POWER

ABOUT NEW YORK LAWYERS FOR THE PUBLIC INTEREST (NYLPI)

Founded nearly 50 years ago, NYLPI pursues equality and justice for all New Yorkers. Our work activates the power of New York communities as they lead the fight to make equal justice a reality. We strive to create equal access to healthcare, achieve equality of opportunity and self-determination for people with disabilities, ensure immigrant opportunity, strengthen local non-profits, and secure environmental justice for low-income communities of color. Guided by community priorities, NYLPI files lawsuits, organizes, seeks policy reform, informs and educates the public, creates pro bono partnerships, and builds the capacity of local nonprofits to serve our communities. Through workshops, trainings for nonprofit leaders, legal counseling, and our Nonprofit Toolkit publications, NYLPI's Pro Bono Clearinghouse is at the forefront of helping nonprofits maximize their performance and their impact.

Lawyers Alliance FOR NEW YORK
Connecting Lawyers, Nonprofits, and Communities

ABOUT LAWYERS ALLIANCE FOR NEW YORK

Lawyers Alliance for New York is the leading provider of business and transactional legal services for nonprofit organizations and social enterprises that are improving the quality of life in New York City neighborhoods.
Our network of pro bono lawyers from law firms and corporations and staff of experienced attorneys collaborate to deliver expert corporate, tax, real estate, employment, intellectual property, and other legal services to community organizations. By connecting lawyers, nonprofits, and communities, Lawyers Alliance for New York helps nonprofits to provide housing, stimulate economic opportunity, improve urban health and education, promote community arts, and operate and advocate for vital programs that benefit low-income New Yorkers of all ages.