Blue Light IT
Cyber Resilience Experts

NPI Inventory Worksheet

NPI Inventory Worksheet

Here's a straightforward **NPI Inventory Worksheet** tailored for small CPA firms. This worksheet helps track and categorize Non-public Personal Information (NPI) for better compliance with the FTC Safeguards Rule.

Disclaimer

This NPI Inventory Worksheet is provided as a general guideline to assist small businesses in understanding and managing their sensitive data. It is not intended to serve as legal, regulatory, or cybersecurity advice.
Each business has unique data management needs and should customize this worksheet accordingly. Blue Light IT (BLIT) assumes no responsibility for the completeness, accuracy, or suitability of this worksheet for your specific circumstances.
By using this Worksheet, you acknowledge that it is your sole responsibility to adapt and implement it in alignment with your business processes, risks, and applicable regulations. For personalized assistance or to ensure compliance, consult a qualified cybersecurity or legal professional.

NPI Inventory Worksheet

Firm Name: [Insert Your Firm Name]
Date Created: [Insert Date]
Last Updated: [Insert Date]

Purpose

This worksheet identifies and documents all locations where Non-Public Personal Information (NPI) is collected, stored, processed, or shared. It supports compliance with the FTC Safeguards Rule by helping firms understand and secure their sensitive data.

1. NPI Categories

List the types of NPI handled by your firm. Check all that apply:

- ☐ Client names
- ☐ Social Security numbers
- ☐ Tax Identification Numbers
- ☐ Financial account numbers
- ☐ Tax return data
- ☐ Other (specify): [_____]

2. NPI Data Locations

Use the table below to document where NPI is collected, stored, and processed.

Data Source	Data Format	Location/Storage	Accessed By	Retention Period	Notes
Client Intake Forms	Paper/Digital	Locked file cabinets/CRM	Admin staff, tax preparers	7 years (or firm policy)	Update retention policy
Tax Software	Digital	[Software Name/Cloud]	Tax preparers, admins	As per software policy	Ensure encryption enabled

Data Source	Data Format	Location/Storage	Accessed By	Retention Period	Notes
Email Correspondence	Digital	Email server/cloud archive	All authorized staff	2 years (or firm policy)	Secure email configuration
Backup Storage	Digital (encrypted)	External hard drive/Cloud	IT personnel	Rotated weekly	Verify regular backups
Third-Party Providers	Digital	[Name of Provider]	Providers' authorized users	As per contract	Annual vendor review

3. NPI Sharing and Access

Identify parties with whom NPI is shared and specify the purpose.

Third Party/Provider	Purpose of Sharing	Security Measures in Place	Access Limitations
Payroll Service	Payroll processing	Encrypted file transmission	Only specific employees
Cloud Storage Provider	Secure document storage	Data encryption, 2FA	Contractual limitations
Tax Preparation Software	E-filing and record keeping	Vendor security certifications	Licensed users only

4. NPI Protection Measures

For each data location, outline specific security measures implemented:

Location	Protection Measures
Physical files	Locked cabinets, office access control
Digital systems	Password protection, encryption, two-factor authentication

Location	Protection Measures
Cloud storage	End-to-end encryption, access logging
Email	Secure email gateway, phishing filters
Backups	Encrypted backups stored offsite

5. Periodic Review

- **Review Frequency:** [e.g., Quarterly, Annually]
- **Reviewer Name and Title:** [Insert Name and Title]
- **Last Review Date:** [Insert Date]
- **Next Review Date:** [Insert Date]

This worksheet is a living document and should be updated regularly to reflect changes in operations, personnel, or technology.