USDA Food and Nutrition Service
U.S. Department of Agriculture

Research Summary April 2023

How States Safeguard USDA's Supplemental Nutrition Assistance Program Participants' Personally Identifiable Information

Background

All applicants and participants in the Supplemental Nutrition Assistance Program (SNAP) are required to submit personally identifiable information (PII) in order to receive program benefits. This PII includes geographical details like home addresses and phone numbers, as well as immediately identifying information such as names and Social Security numbers (SSNs). This information is submitted during the application and recertification processes, and State agencies (SAs) have been largely successful in implementing policies and practices to safeguard SNAP PII.

The primary purpose of this study was to both better understand how SAs are currently protecting SNAP PII and to gather best practices for data security. There is a need for more focus on protecting PII due to the growing amount of data collected and stored by SAs, the extent of data matching and sharing between SAs and the federal government, and the increasingly sophisticated methods of breaching data safeguards. The study objectives were to (1) describe the policies and regulations that address safeguarding PII, (2) detail the methods that can be used to safeguard PII, (3) outline precautions that SAs currently take to protect PII, (4) examine the consistency of these safeguards among SAs, and (5) provide recommendations for improving how PII is protected by SAs.

Key Findings

- In the area of Personnel Policies and Procedures, a majority of SAs limit staff access to SNAP applicant/recipient PII and offer staff training on safely handling and storing PII, although the frequency and thoroughness of training was inconsistent.
- For Security Policies and Procedures, most SAs have implemented measures for protecting PII and have plans in place for responding to data security incidents. Most SAs (nearly 80 percent) have not experienced data breaches.
- For Safeguarding Practices used during program operations, few SAs reported masking SSNs during data entry, but most reported timeout functions on eligibility system screens.

Data Sources

The study included three principal data sources:

- A survey administered to all SNAP SAs, which covered familiarity with PII regulations, preventing data breaches, and compliance with mandatory security protocols. This survey was conducted between September 2021 and January 2022.
- Interviews with eight industry experts with extensive backgrounds in data security. These interviews focused on expert views on PII protection and industry benchmarks for data security.
- Interviews with programs and IT staff from five SAs that have demonstrated an exemplary record of handling PII. Staff from California, New Jersey, North Dakota, Oklahoma, and South Carolina were interviewed on best practices recommendations.

Methods

The information gathered was used to identify barriers to compliance, gaps in knowledge and implementation, and next steps for better maintaining data security as well as to compile best practices for protecting PII. The study sorted data safeguards into three categories:

- Personnel Policies and Procedures: SA protocols to ensure that only essential, appropriately trained staff who have met baseline security requirements have access to PII.
- Security Policies and Procedures: FNS requirements to ensure SAs have robust security plans; secure PII across hardware, software, and networks; and engage in assessing risk, vulnerabilities, and security testing.
- Safeguarding Practices: The processes and procedures for administering SNAP, including data masking and using secure data systems when processing PII data.

Findings

In the area of Personnel Policies and Procedures, a majority of SAs limit staff access to SNAP applicant/recipient PII and offer staff training on safely handling and storing PII, although the frequency and thoroughness of training was inconsistent. SAs reported they limit staff access by requiring them to get approval to either modify (93 percent) or access (84 percent) SNAP participant data. Annual trainings were reported by 96 percent of SAs, and 83 percent reported training staff when hired. Less frequently reported training topics included protecting specific PII used for issuing EBT cards (57 percent of SAs) and the use of data matching (59 percent of SAs).

For Security Policies and Procedures, most SAs have implemented measures for protecting PII and have plans in place for responding to data security incidents. Most SAs (nearly 80 percent) have not experienced data breaches. Ninety-one percent of SAs reported regular backups of stored data. Eighty-four percent reported securely disposing of data, identifying critical physical safeguards in storage facilities, or regular risk assessment of physical resources. In the event of a data breach, 98 percent of SAs confirmed developing a response policy, and 87 percent identified initial steps of incident response.

Nearly all SAs allowed remote access to systems containing PII, but their implementation of remote access varied. Seventy percent of SAs allowed employees to use equipment authorized by the agency to remotely access systems containing PII; however, only 28 percent of SAs permitted employees to use their personal devices to remotely access systems containing PII.

For Safeguarding Practices used during program operations, few SAs reported masking SSNs during data entry, but most reported timeout functions on eligibility system screens. Only nine percent of SAs reported that they have a statewide SNAP eligibility system that masks SSNs. Data masking is replacing a number or character with asterisks or a randomly generated pseudonym. Ninety-six percent of SAs reported using timeout functions on eligibility system screens with an average time limit of 20 minutes.

A significant majority of SAs reported satisfaction with their safeguarding practices. In total, 86 percent of SAs reported being 'very satisfied' or 'satisfied' with safeguards on personnel handling PII. Eighty four percent of SAs reported the same level of satisfaction in their office's program operations, and 82 percent reported similar satisfaction in office security policies.

This study included best practices for safeguarding PII throughout the data lifecycle (i.e. collection, storage, disposal). Such practices included:

- Implementing least privilege access to sensitive data and continually assessing the appropriateness of user access.
- Limiting access to PII to essential records for evaluating applicants and participants.
- Adhering to required protocols for PII encryption during storage, transmission, and dissemination. Access to transmission endpoints should be limited as much as possible.
- Disposing of PII in a manner which complies with established protocols for clearing, purging, and destroying acceptable data.
- Developing new incident response plans which outline how a breach is reported and when individuals are notified.

The capacity of SAs to implement these best practices were influenced by several factors. Such factors included:

- A workplace culture of security that considers data security a core agency value.
- Training opportunities in cybersecurity to cultivate workplace security awareness.
- Effective partnerships with technology vendors.
- Workplace use of security technology, particularly cloud computing.
- Strong support from State agency leadership.

For More Information:

Nisar, H., Okvere, D., et al. (2023). "How States Safeguard Supplemental Nutrition Assistance Program Participants' Personally Identifiable Information." Prepared by 2M Research. US Department of Agriculture, Food and Nutrition Service. Available online at www.fns.usda.gov/research-and-analysis.