

For: FSA Employees and Contractors

PII Data Types

Approved by: Deputy Administrator, Management



1 Overview

A Background

PII refers to any information about an individual that is maintained by an agency that includes, but is not limited to, the following:

- financial transactions
- medical or criminal history
- information that can be used to distinguish or trace an individual’s identity, such as the following:
 - name (when connected to PII)
 - Social Security number (SSN)
 - date and place of birth
 - mother’s maiden name
 - biometric records, such as fingerprints
 - any other personal information that is or can be linked to a specific individual.

B Purpose

This notice provides examples of:

- the following categories of PII data types:
 - core

Note: This should **not** appear in the public domain; for example, SSN.

Disposal Date November 1, 2009	Distribution All FSA employees and contractors; State Offices relay to County Offices
----------------------------------------------	-----------------------------------------------------------------------------------------------------

1 Overview (Continued)

B Purpose (Continued)

- identity verification

Note: This could appear in the public domain; for example, phone book.

- data types that are:
 - protected by the Privacy Act
 - most commonly dealt with by FSA employees and contractors.

C Contact

If there are questions about this notice, contact John W. Underwood, FSA Privacy Act Officer/FSA PII Officer, at either of the following:

- e-mail at john.underwood@kcc.usda.gov
- telephone at 816-926-6992.

2 PII Data Types

A Overview

This paragraph serves as a quick reference guide for identifying core PII data types and identity verification PII data types. The PII data type lists must **not** be viewed as encompassing all PII data types.

B Core PII Data Types

Core PII data types are PII that have the greatest potential to be misused for identity theft and include the following:

- SSN, including the last 4 digits (or any other part) of SSN
- tax ID number or producer's/owner's ID number (when the tax ID number or producer's/owner's ID number is identical to SSN or any part of SSN)
- financial information, such as the following:
 - bank account number/information
 - financial transaction history
 - credit report/credit worthiness information
 - credit/debit card number
 - personal identification number

2 PII Data Types (Continued)

B Core PII Data Types (Continued)

- tax information
- biometric records, such as the following:
 - fingerprints
 - voiceprint
 - retina or iris scan
 - scan of hand or face geometry
- driver's license number
- LincPass information.

Note: SSN, tax ID, or producer's/owner's ID **does not** need to be connected to a specific individual for the number to be considered PII. Just SSN, tax ID, or producer's/owner's ID shown on its own is considered to be PII.

C Identity Verification PII Data Types

Identity verification PII data types are PII that can be used to confirm the accuracy/validity of the core PII data types. It is possible that identity verification PII may have been placed into the public domain by non-FSA sources. However, even if already in the public domain, FSA shall continue to properly protect (do **not** publicly disclose) the identity verification PII. Identity verification PII includes the following:

- date of birth
- place of birth
- mother's maiden name
- personal contact information, such as the following:
 - home address of FSA employees, contractors, and any producer that has **not** received an FSA program payment
 - the following information of FSA employees, contractors, and all producers:
 - home telephone number
 - personal cell phone number
 - home e-mail address.

3 Additional Information

A Privacy-Protected Data Types

FSA **shall** properly safeguard privacy-protected data types. In addition to core PII and identity verification PII data types, there are data types that FSA generally does **not** disclose to the public in response to a FOIA request. Privacy-protected data types that are most commonly processed by FSA include the following:

- information of FSA employees, contractors, and all producers; such as:
 - race, ethnicity, sex, national origin, and disability information
 - investigatory information
- personal insurance information (**not** relating to USDA/FSA programs)
- legal/lawsuit information (when the information has **not** been disclosed to a Court according to an established legal process)
- medical information, including FSA employee sick leave data
- FSA employee disciplinary information
- scores and comments appearing on FSA employee performance appraisals
- responses submitted on OGE-450's
- information that sheds light on a producer's operations or financial situation, such as the following:
 - actual crop production amounts
 - actual crop yields
 - cropland acres
 - farmland acres
 - specific crop acres
 - number of livestock information; for example, number of head
 - insurance information (relating to USDA/FSA programs)
 - loan/loan application information

Notice AS-2179

3 Additional Information (Continued)

A Privacy-Protected Data Types (Continued)

- irrigation data (crop is/is **not** being irrigated)
- references to terms of:
 - lease agreements/lease forms
 - farm loan agreements/farm loan forms
- share percentages between parties on FSA program applications/contracts
- name of financial institution where benefits are direct deposited
- information that reveals the following:
 - wealth or poverty of a producer
 - success or failure of a given farming operation
 - payment assignments that reveal payments directed to other person or entity to whom the producer owes money.

B Determining PII

For assistance with PII determinations, FSA employees and contractors are **encouraged** to seek advice and guidance from their respective FOIA/Privacy Act Service Center at **http://www.fsa.usda.gov/Internet/FSA_File/fsaservicecenter20087.pdf**.

C Reporting Loss or Suspected Compromise of PII

Employees or contractors having any reason to suspect that PII has been lost or compromised **shall report** concerns within 1 workday of becoming aware of the issue. Contact the 24-hour support Security Incidents Hotline at either of the following:

- 888-926-2373
- 877-PII-2YOU.