

Privacy Impact Assessment

Electronic Disqualified Recipient System (eDRS)

■ Date: April 1, 2023



Privacy Impact Assessment for the Electronic Disqualified Recipient System (eDRS)

April 1, 2023

Contact Point

Alexander Soto Roman

**USDA/FNS/Program Accountability and Administration Division
United States Department of Agriculture
703-605-3218**

Reviewing Official

Michael Bjorkman

FNS Privacy Officer

**United States Department of Agriculture
(703) 305-1627**

Shawn Montgomery

OIT – Information Security Office

**United States Department of Agriculture
(703) 605-0484**

Abstract

Electronic Disqualified Recipient System (eDRS). eDRS is a centralized national database, utilizing data submitted by all 50 States, the District of Columbia, Guam, and the U.S. Virgin Islands. eDRS allows States a quick and efficient way to determine if a person has been disqualified from receiving SNAP benefits elsewhere. USDA's Food and Nutrition Service (FNS) is providing this PIA due to the Privacy Threshold Assessment determination that eDRS collects PII and is subject to PIA.

Overview

Electronic Disqualified Recipient System (eDRS); Food and Nutrition Service (FNS) owned database. See above – System used to determine if a recipient has been disqualified from participating in the Supplemental Nutrition Assistance Program (SNAP). eDRS supports our statutory requirements to maintain program integrity.

Contains information on individuals who have been disqualified from participation in SNAP, the length of their disqualifications, and how many times they have been disqualified. State agencies use the system for eligibility determination, to determine the length of a penalty, and enter information into the system on individuals disqualified in their State. State agencies that administer SNAP are granted access to eDRS through a direct online connection or through web services.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

eDRS maintains the following information.

- Personally identifying information about disqualified individuals: Name, social security number (or other identification number), date of birth, gender
- Disqualification details: Disqualification number, disqualification decision date, disqualification start date, length of disqualification period
- Agency imposing the disqualification: Locality code and the title, location, and contact information

1.2 What are the sources of the information in the system?

State agencies submit information about the disqualifications imposed by their State on individuals who have been found to have committed an intentional program violation.

1.3 Why is the information being collected, used, disseminated, or maintained?

States use this information to determine if a participant has been disqualified from a different state and if they are eligible to receive benefits. The information is also used to ensure the appropriate disqualification period is imposed for new disqualifications.

1.4 How is the information collected?

State agencies submit information related to disqualifications they impose.

1.5 How will the information be checked for accuracy?

State agencies submit records to eDRS and are responsible for ensuring the accuracy of the data they submit. Information in eDRS must be backed up by official documentation about each disqualification and must be verified before the information can be used for an adverse action on a SNAP case. Some simple validation functionality is built into eDRS to enhance likelihood of data integrity (e.g. inability to enter all 1-digit for social security number).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Section 6 of the Food and Nutrition Act of 2008, as amended, (7 U.S.C. 2015)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Risk is mitigated by controlling access to the system. Online Users must have e-Authentication Level 2 prior to accessing the system and complete an FNS-674. All online and web services users are assigned specific roles which are identified on the FNS-674 before they are able to access the system. Web Services: State provided authentication credentials for use of a state portal with a system to system connection to eDRS application web services. User access to the state designed and implemented system is authorized by the respective state's Level 2 eAuth credentialed official(s) who must complete a FNS-674.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

State agencies match against eDRS to ensure applicants and new household members are not currently disqualified from receiving SNAP benefits due to an intentional program violation (IPV). State agencies also use eDRS to ensure the proper disqualification period is imposed for new IPV's received in their State.

2.2 What types of tools are used to analyze data and what type of data may be produced?

This system uses no analysis tools.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to the system is controlled by FNS through the authorization process, which grants access only to those with a valid need to know. The other two controls that are utilized are physical and procedural safeguards.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Records in eDRS are maintained until the record no longer serves its intended regulatory purpose and is no longer needed to fulfill any legal retention requirement. State agencies delete records on individuals they have disqualified from eDRS:

1. When the recipient is deceased;
2. When the recipient reaches their 80th birthday, if the State has chosen to implement this option;
3. In cases where the determination of intentional program violation is reversed by a court of appropriate jurisdiction;
4. If a State determines that supporting documentation for a disqualification record that it has entered is inadequate or nonexistent;
5. If a State agency is unable to demonstrate to the satisfaction of FNS that the information in question is correct.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. N1-462-09-8

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Risk: Risk of PII info accessed by unauthorized users.

Mitigation: All PII data is encrypted at rest and in transit. Access to the data is tightly controlled through the use of eAuthentication.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information is only accessible to USDA/FNS employees based on their permission level (eDRS user role), which is indicated on their FNS-674.

4.2 How is the information transmitted or disclosed?

Information is not transmitted internally. Information is disclosed to employees based on their permission level which is indicated on their FNS-674.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy risk is mitigated by only allowing role-based access for all users.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

FNS owns and maintains eDRS, but State agencies are both the source and the recipients of the information in eDRS. The system's purpose is to allow State agencies to share information about disqualifications in their States and to allow other

State agencies to access the national database to perform their program administration and program integrity duties.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes. Sharing of this information is covered under SORN FNS-5 which states:

Records contained in this system may be disclosed, as part of a computer matching program or otherwise, to State agency personnel responsible for investigating or prosecuting violations of SNAP regulations, and to Federal, State, and local officials responsible for administration of SNAP. Records contained in this system also may be disclosed to the General Accounting Office for program audit purposes.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared with State agencies responsible for administering the SNAP via the online eDRS system or Web Services interfaces.

All transmissions i.e. online or Web Services are encrypted for security purposes. After online or web services interface transmission, the state agencies are responsible for the safeguarding of the data.

Online Users and the Web Services State Administrator must have e-Authentication Level 2 prior to accessing the system and complete an FNS-674. User permissions and access levels are granted based on the specific user role identified on the FNS-674. Information is not disclosed to the general public.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is shared with State agencies responsible for administering SNAP. Online users must have e-Authentication Level 2 prior to accessing the system and complete a FNS-674. Online users are assigned specific roles which are identified on the FNS-674 before they are able to access the system.

Web Services: state provided authentication credentials for use of a state portal with a system to system connection to eDRS application web services. User access to the

state designed and implemented system is authorized by the respective state's Level 2 eAuth credentialed official(s) who must complete an FNS-674.

Information is not disclosed to the general public.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

USDA/FNS-5, Information on Persons Disqualified from the Supplemental Nutrition Assistance Program. <https://www.ocio.usda.gov/sites/default/files/docs/2012/FNS-5.txt>

6.2 Was notice provided to the individual prior to collection of information?

Yes, SNAP benefit participants are informed when they apply for SNAP benefits.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes, however; in order to participate in the program, information is required by regulation.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. In order to participate in the program information for particular uses is required by regulation.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

State agencies have implemented procedures and developed forms to meet the Privacy Act requirement to provide individualized notice to applicants for and recipients of financial assistance or payments under federal benefit programs that any information provided by applicants and recipients may be subject to verification through matching programs. Methods for notification include, but are not limited to, a statement on the initial application for SNAP benefits (hard copy and electronic); an explanation in the benefit program handbook provided at the time of application; a banner on the State agency website for SNAP applicants and

SNAP renewal; and, a statement in letters to applicants and recipients of SNAP assistance. Privacy Impact Assessment – Electronic Disqualified Recipient System Page 11 When information obtained from a matching program indicates that an applicant is not eligible for SNAP benefits and such information has been independently verified, the State agency will provide the applicant with a written notice that provides the affected individual an opportunity to contest any such information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

An individual may obtain information about a record in the system which pertains to the individual by submitting a written request to the systems manager listed above. The envelope and the letter should be marked "Privacy Act Request." A request for information pertaining to an individual should contain the name, date of birth and SSN or Green card Number of the individual, and any other information that will assist in locating the record.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals desiring to contest or amend information maintained in the system should direct their request to the state agencies, the reasons for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. The State agency submitting such record(s) is responsible for providing prompt verification of the accuracy of the record. If a State determines that supporting documentation for a disqualification record that it has entered is inadequate or nonexistent, or they are unable to demonstrate to FNS that the information in question is correct, they must delete the record from eDRS.

7.3 How are individuals notified of the procedures for correcting their information?

All data is provided by and maintained by the State agencies that administer SNAP. State agencies are responsible for entering and maintaining accurate information in eDRS. When information obtained from an eDRS match indicates that an applicant is not eligible for SNAP benefits and such information has been independently verified, regulations require the State agency to provide the applicant with a written notice that provides the affected individual an opportunity to contest any such information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal process is required by regulations and described above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional privacy risks are associated with redress. Regulations around privacy and disclosure of recipient information are no different regardless of whether the information is provided during initial application or recertification or to contest information from an eDRS match.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

All online users of the system must have an eAuth Level 2 and complete a FNS Form 674.

Web Services: state provided authentication credentials for use of a state portal with a system to system connection to eDRS application web services. User access to the state designed and implemented system is authorized by the respective state's Level 2 eAuth credentialed official(s) who must complete an FNS-674. The state provided authentication credential provides an audit trail for all state activity.

Access is limited to FNS staff and managers responsible for SNAP participant accuracy and applications.

eDRS access is strictly limited to those who have an approval and need to know.

8.2 Will Department contractors have access to the system?

Yes

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

FNS has annual security training requirements which all FNS employees and contractors supporting eDRS are required to take. FNS has developed and provided on request Train-the-Trainer security training to the states. It is also our understanding

that each state conducts their security training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The ATO is dated August 11, 2020 and expires August 11, 2023.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Online Users must have must have e-Authentication Level 2 prior to accessing the system and complete an FNS-674. Users are assigned specific roles which are identified on the FNS-674 before they are able to access the system. Information is not disclosed to the general public.

Web Services: state provided authentication credentials for use of a state portal with a system to system connection to eDRS application web services. User access to the state designed and implemented system is authorized by the respective state's Level 2 eAuth credentialed official(s) who must complete an FNS-674. The state provided authentication credential provides an audit trail for all state activity.

There are limits to the amount of data that can be retrieved in a single query. All communications are over secure channels.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Risk: Risk of PII info accessed by unauthorized users.

Mitigation: All PII data is encrypted at rest and in transit. Access to the data is tightly controlled through the use of eAuthentication.

Detailed Explanation: The risks are mitigated by users being required to have e-Authentication Level 2 prior to accessing the system and complete an FNS-674. Users are assigned specific roles which are identified on the FNS-674 before they are able to access the system.

Web Services: state provided authentication credentials for use of a state portal with a system to system connection to eDRS application web services. The level of user access to the state designed and implemented system is authorized by the respective state's Level 2 eAuth credentialed official(s) who must complete an FNS-674.

Information is not disclosed to the general public. There are limits to the amount of data that can be retrieved in a single query. All communications are over secure channels.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

.NET Framework v 4.7, Microsoft SQL Server 2016 Version 13.2, Microsoft Windows Server 2016 X 64

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes. ISSPM has reviewed the required policies mentioned above.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

There are no 3rd party websites or applications in use.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

There are no 3rd party websites or applications in use.

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

There are no 3rd party websites or applications in use.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

There are no 3rd party websites or applications in use.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

There are no 3rd party websites or applications in use.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

There are no 3rd party websites or applications in use.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

There are no 3rd party websites or applications in use.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

There are no 3rd party websites or applications in use.

10.10 Does the system use web measurement and customization technology?

No

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.



There are no 3rd party websites or applications in use.