Privacy Impact Assessment

Direct Premium Remittance System (DPRS)

- Version: 3.0
- Date: September 2020
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Direct Premium Remittance System (DPRS)

September 2020

Contact Point
Debby Tatum
Information System Owner
504-426-7664

Reviewing Official
Tracy Haskins
Information Systems Security Program Manager
202-720-8245

National Finance Center
United States Department of Agriculture

Abstract

The National Finance Center (NFC) is a Shared Service Center (SSC) under the OPM Human Resources Line of Business (HRLOB). To carry out its wide-ranging responsibilities, the U. S. Department of Agriculture (USDA), and its employees and managers have access to diverse and complex automated information systems, which include system, file servers, local and wide area networks running various platforms, and telecommunications systems to include communication equipment.

The USDA relies on its information technology systems, including the *Direct Premium Remittance System (DPRS)*, to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large.

The NFC Government Employees Services Division (GESD), which falls under the United States Department of Agriculture (USDA), is responsible for development, deployment, maintenance, and testing of the NFC DPRS major application (MA).

This Privacy Impact Assessment (PIA) is being conducted to fulfill the requirements of Section 208 of Public Law 107-347 (the E-Government Act of 2002).

Overview

The Direct Premium Remittance System (DPRS) serves as a centralized system for the billing and collection of health insurance premiums from eligible non-Federal enrollees who choose to participate in the Federal Employees Health Benefits (FEHB) Program under the Temporary Continuation of Coverage (TCC) and Spouse Equity regulations, National Defense Authorization Act of 1993, Direct Pay Annuitants and Dependents - Direct Pay of Premium by Annuitants Act of 1990 and American Recovery and Reinvestment Act of 2010 (ARRA). DPRS processes the reporting of information between the enrollees and the insurance carriers and the Office of Personnel Management (OPM). Through reimbursable agreements, DPRS processes the health insurance records for specific types of enrollees (annuitants and survivors) for OPM.

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?

DPRS collects, uses, and maintains health benefits account information, including Personally Identifiable Information (PII), needed to process the health benefits accounts of eligible individuals for USDA and other Federal agencies.

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

Banking institutions, individuals and agencies can provide data for use in the system.

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

The purpose of the data is to record, process, and report Health Insurance Information and Certain Enrollee account information with respect to Insurance billing and collections, and enrollee account status information pertaining to and including health insurance carrier information for USDA and other Federal agencies.

1.4 How is the information collected?

Information is collected via data entry and front end interfaces from banking institutions, individuals, customers and agencies. Agencies submit data via connect direct and secure FTP over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

1.5 How will the information be checked for accuracy?

DPRS application code as processed actions via either by enrollee request or systematic process actions occur via billing, collections and delinquency. These are maintained on the mainframe and applied to data entered and data transferred there. As Federal Employee Health Benefits (FEHB) Election form (2809) documents and Change in Health Benefits (2810) documents for Insurance Carrier Reporting are processed on a daily basis updated data replaces existing data elements on the DPRS database. Error-checking routines are built into applications including edits of data received, record counts and database status checking.

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

5 U.S.C. Sec. 552a governs the collection, use and safeguarding of data collected on individuals.

The SORN is OPM-GOVT-1

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

NFC complies with the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), to ensure that data is protected from unauthorized access, malicious or inadvertent modification, disclosure, and disruption.

NFC also works diligently to secure Personally Identifiable Information (PII) by requiring adequate training of employees and contractors that have access to the data. NFC provides the degree of protection (administrative, technical, and physical safeguards) for the data collected as prescribed by the Privacy Act of 1974, 5 U.S.C. Section 552a. NFC ensures all data included in data file transmissions are provided, received, and stored in a secure manner. NFC protects, labels, and handles the data in accordance with 5 U.S.C. Section 552, Privacy act of 1974, as amended and applicable to agency regulations. All employees and contractors adhere to security requirements for handling and storing of Federal data as directed by the Electronic Government Act Title III, also known as the Federal Information Security Management Act (FISMA).

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.

The purpose and routine uses of the data include recording, processing, and reporting the health benefit data for USDA and other Federal agencies.

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

DPRS has data validation routines built into the interface that checks for required fields, data types, and data ranges. Additionally, the business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency. Individuals and agencies may run predefined and custom reports against the data and have the ability to access data elements depending on access privileges requested by authorized agency personnel.

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

All information is provided by the individual, customer, or agency and does not use commercial or publicly available data.

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.

DPRS uses mainframe role base access and UserID/password to protect access to data. Agency Employees only have access to their agency records. Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret is used to manage end user security. Top Secret maintains strong role based security controls. Access is granted based upon security access requests from authorized agency security officers.

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?

The retention periods of data contained in this system are covered by NARA General Records Schedules; Civilian Personnel Records have various retention periods for specific types of data. These retention periods are adhered to per customer agency requirements and memorandum of understanding.

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

This system complies with the guidance contained in the NARA General Records Schedule 20, Electronic Records.

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

The purpose of retaining the information is to provide historical data to respond to any issues including but not limited to payroll and benefit corrections, Equal Employment Opportunity (EEO) issues or law suits, and disciplinary actions. Retaining these records are in accordance with GRS I, which has a fairly limited retention period, to mitigate privacy risks associated with maintaining these records.

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?

Authorized agency users of DPRS have access to their specific agency's information. This includes up to 170 agencies whose payroll is processed by NFC. The agency security officers handle submission of all security access requests for agency users as authorized by agency managers. Access is based on the principle of least privilege, which refers to granting the minimum required system/application resources to a user that enables them to perform their organizational functional duties

4.2 How is the information transmitted or disclosed?

Information is collected via data entry and front end interfaces from individuals, customers and agencies. Agencies submit data via connect direct and secure FTP over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

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.

The agency security officer handles requests for information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is granted to agency users based application functional need, and restricted to their agency data.

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?

Authorized agency users of DPRW have access to their specific agency's information. This includes up to 170 agencies whose payroll is processed by NFC, and several agencies whose payroll we do not process (Department of Defense, Department of Treasury, OPM, Postal Service, General Services Administration, and National Business Center). In addition, DPRW is accessed by non-federal, Tribal Benefit Offices based on their specific personnel office

ID. Information collected by DPRS is owned by each agency/tribal benefit office. The agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of our customers. Access is determined by agencies' functional managers and submitted by the agency or tribal security officers. NFC will grant authority to use/access DPRW to authorized users at the request of the agencies' security officer. In order to process health benefits accounts for eligible individuals, NFC shares health benefits account information collected in DPRW/DPRS with FEHB insurance carriers via OPM's Macon Data Hub.

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.

Please see Section 5.1 above. NFC follows the OPM GOVT-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference.

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

Information is collected directly from individuals, customers, and agencies. Agencies submit data and file transfers via connect direct and secure FTP over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

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

Only authorized individuals can access information under the "need-to-know" policies. The proper controls are in place to protect the data and prevent unauthorized access.

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

Yes.

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

Yes. Individuals have the opportunity to decline to provide the information and informed that the data is required to complete routine business functions. Below is the Privacy Act notice wording.

Privacy Act Notice

We are authorized to request this information under 5 U.S.C. Chapter 84. Executive Order 9397 authorizes us to ask for your Social Security number, which will be used to identify your account. We will use the information you provide to process the transaction you request on the NFC Web site.

You are not required by law to provide this information, but if you do not provide it, it may not be possible to process the actions you request on this Web site.

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

Yes. Individuals are provided a consent statement, prior to logging into the application, via a warning banner which states:

**********WARNING**********

1. You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only.

2. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

3. By using this information system, you understand and consent to the following:

1) You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.

2) Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

3) Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding

communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

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

From a regulatory and management controls perspective, a copy of the redacted PIA is available on USDA's Office of the Chief Information Officer web site. Individuals are notified several ways such as; by their agency, during online registration, during application use, etc. From the standpoint of an individual using the application, they are made aware of the collection of data and potential uses and must consent to both prior to accessing the system.

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?

At the agency's discretion and according to the agency's security policies, individuals may be assigned a unique user id and password that allows them access to their own data in the system.

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

Information in the system must be corrected by authorized users from the agency's payroll/personnel human resources department at the request of the individual or at agency direction.

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

Each agency using the system would provide this information to its employees.

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

Each agency using the system would provide this information to its employees.

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

It is the responsibility of the agency to ensure that personnel with access to correct data on individuals have the proper clearances, position sensitivity designations, and appropriate system access to tile data. NFC access control procedures, role based security of the application, and agency reporting of individual access and utilization aid agency officials to mitigate the risks of agency individuals with improper access.

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?

The agencies determine user access. NFC follows Directive 58, Information Systems Security Program Revision 3, and Directive 2, Access Management.

8.2 Will Department contractors have access to the system?

Yes, if authorized by agency functional manager and submitted by the agency security officer.

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

Authorized agency users and contractors must complete annual security awareness and rules of behavior training and be properly trained on the system.

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

Yes.

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

DPRS provides auditing at the application, database and network/operating system levels.

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?

A Risk Assessment was performed on DPRS and security controls have been documented in the System Security Plan. These controls are tested annually under SSAE-18 and A·123 programs and an independent assessment is performed every three years or when changes are made to the system.

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?

The Direct Premium Remittance System (DPRS) serves as a centralized system for the billing and collection of health insurance premiums from eligible non-Federal enrollees who choose to participate in the Federal Employees Health Benefits (FEHB) Program under the Temporary Continuation of Coverage (TCC) and Spouse Equity regulations, National Defense Authorization Act of 1993, Direct Pay Annuitants and Dependants - Direct Pay of Premium by Annuitants Act of 1990 and American Recovery and Reinvestment Act of 2010 (ARRA). DPRS processes the reporting of information between the enrollees and the insurance carriers and the Office of Personnel Management (OPM). Through reimbursable agreements, DPRS processes the health insurance records for specific types of enrollees (annuitants and survivors) for OPM.

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

No. DPRS is an established mainframe application with a web component that allows only batch updates to the DPRS database on the mainframe The DPRS system has undergone a detailed security vulnerability assessment and has been Certified and Accredited.

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.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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?

Not applicable.

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

Not applicable.

If so, is it done automatically?

Not applicable.

If so, is it done on a recurring basis?

Not applicable.

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

Not applicable.

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?

Not applicable.

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)?

No.

10.10 Does the system use web measurement and customization technology?

Not applicable.

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?

Not applicable.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Not applicable.

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.

Not applicable.

Agency Responsible Officials

DEBORAH TATUM
Digitally signed by DEBORAH TATUM
Date: 2020.09.03 15:44:37 -05'00'

Debby Tatum
Information System Owner
Government Employees Services Division (GESD)
USDA National Finance Center

Agency Approval Signature

TRACY HASKINS-JOHNSON
Digitally signed by TRACY HASKINS-JOHNSON
Date: 2020.09.22 08:47:38 -04'00'

Tracy Haskins
Information Systems Security Manager
United States Department of Agriculture OCIO-DAITO