USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	OPM FEHB Centralized Enrollment Clearinghouse System (CLER)
Program Office	Office of the Chief Financial Officer (OCFO)
Mission Area	DAITO / OCFO-NFC
CSAM Number	1044
Date Submitted for Review	07/28/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nija Enclarde	318-955-1393
Information System Security Manager	Tracy Haskins	202-720-8245
System/Program Managers	Trudy Sandefer	504-426-7663

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 Centralized Enrollment Clearinghouse System (CLER), 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 CLER 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 NFC of the USDA has designed, developed, and implemented, the Federal Employees Health Benefits (FEHB) Centralized Enrollment Clearinghouse System (CLER) for the Office of Personnel Management (OPM). The system receives electronic data from federal government payroll offices by pay period and health insurance carriers on a quarterly basis for approximately 4 million health benefit enrollees (i.e., approximately 8 million records). The payroll offices electronically submit enrollment data on a pay period basis to NFC directly via a secure connection. Carriers submit their enrollment data quarterly to the OPM Macon Hub which submits the data to NFC via a secure connection. Upon receipt of the enrollment data, it is processed into the mainframe which stores, maintains, processes, edits, matches, combines, and compares the enrollment data from the payroll offices to that from the carriers using edit tables. After the data is input to the mainframe, the Web server can access the data in response to queries from the payroll offices, carriers, OPM, and NFC for inquiries, contact information updates, or reconciliation discrepancy correction, and report generation. Using the Web server, a payroll office may inquire on its data. Based on the payroll office analysis, a discrepancy with the carrier data may be encountered. The payroll office may submit forms requesting corrective action from the carrier by electronically using the CLER Web server. The corrective action request file will be forwarded from the Web server through the NFC mainframe, where it is processed and transmitted via a secure connection, to the carrier through the OPM Macon Hub. The carrier responds to the corrective action request directly through the Web server. The carrier response and update are maintained on the database and is available for inquiry by the payroll offices.

CLER also provides oversight reports to monitor carrier responses. CLER satisfies all system access and reporting requirements identified by OPM. CLER was designed and developed with great potential for future improvements and expansion beyond basic reconciliation in the event OPM should desire such enhancements. Payroll office and carrier information covering their operational/subject matter and technical contacts is maintained in the CLER System. The payroll offices and carriers are responsible

for keeping the information current for those contacts that have responsibility for coordinating and answering questions. The CLER Web server is used to update these contacts.

Generally, payroll offices have access to their own employee data; carriers have access to enrollment data for participants in their plans; OPM representatives have unrestricted inquiry access as appropriate; and NFC has access as needed to accomplish its assigned duties. OPM performs an oversight role on the CLER program. In this role, OPM has inquiry and report capabilities for all carriers and payroll office participants. The system provides statistical information related to the number of discrepancies, occurrence rates, corrective actions, enrollment changes, etc. This information provides OPM with data needed to effectively manage and oversee the FEHB reconciliation process.

NFC also has a responsibility to maintain the system, update tables and edits as appropriate, and to maintain system security. NFC takes a proactive approach to resolve any discrepancies between the payroll data and the carrier data identified during the - operation of CLER by working with the payroll offices, carriers, and individual enrollers as needed. The user organizations include all Payroll Offices/appropriate Human Resources Offices for the Government, all FEHB carriers servicing Government employees, and OPM.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

What legal authorities and/or agreements permit the collection of information by the project or system?

The legal authority comes from Executive Orders 9397, as amended by 13478, 9830, and 12107.

Has Authorization and Accreditation (A&A) been completed for the system?

Yes.

What System of Records Notice(s) (SORN(s)) apply to the information?

OCFO/NFC–1 Systems for Personnel, Payroll, and Time & Attendance

Is the collection of information covered by the Paperwork Reduction Act?

Yes.

Section 2: Characterization of the Information

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

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

Identifying Numbers:

- Social Security number
- Employee Identification number
- Health Plan Beneficiary number

Biographical Information:

- Name (Including Nicknames)

The system contains FEHB enrollment data such as an enrollee's name, social security number, carrier, enrollment code (enrollee's plan and option), agency ID (the agency where the enrollee is employed), payroll office ID (organization that is responsible for coordinating the enrollee's FEHB coverage and premium collections) and withholding/premium amount. Payroll offices electronically submit FEHB enrollment data by pay period directly to NFC via file transmissions. Carriers submit their FEHB enrollment data quarterly to the OPM data hub located in Macon, Georgia, which in turn submits the data to NFC. Upon receipt, the FEHB enrollment data is processed into NFC's DB2 mainframe. The mainframe database stores, maintains, processes, edits, matches, combines, and compares the FEHB enrollment data from the payroll offices to the data from the carriers using edit tables. This data is sent to the CLER Web server where the agencies, carriers, OPM,

What are the sources of the information in the system/program?

CLER receives electronic FEHB enrollment data from health insurance carriers by pay period and federal payroll offices on a quarterly basis. Also, agencies and carriers have primary contact in each of their organizations and must maintain the contact information in CLER.

How is the information collected?

Payroll offices electronically submit FEHB enrollment data by pay period directly to NFC via file transmissions. Carriers submit their FEHB enrollment data quarterly to the OPM data hub located in Macon, Georgia, which in turn submits the data to NFC. Only authorized users with an established "need-to-know" may access the FEHB enrollment data.

Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

All information is provided by the health insurance carriers and federal agencies and does not use commercial or publicly available data.

How will the information be checked for accuracy? How often will it be checked?

CLER application code provides reconciliation routines at the application level. These are maintained on the mainframe and applied to data entered and data transferred there. Extensive error-checking routines are built into applications including edits of data received, record counts and database status checking.

Does the system/program use third-party websites?

Not applicable

What is the purpose of the use of third-party websites?

Not applicable.

What PII will be made available to the agency though the use of third-party websites?

Not applicable.

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Mitigation: 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 federal data as directed by the Electronic Government Act Title III, also known as the Federal Information Security Management Act (FISMA).

Section 3: Uses of the Information

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

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The mission of CLER is to provide a web based centralized, automated system that timely and accurately reconciles payroll office and health insurance carrier Federal Employees Health Benefits enrollment records. CLER provides an efficient and cost-effective way for both health insurance carriers and federal government payroll offices to conduct their quarterly reconciliation of FEHB enrollment data records.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

CLER 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. Health insurance carriers and agencies may run predefined and custom reports against the data and can access data elements depending on access privileges requested by authorized personnel.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: Ensure that information is handled in accordance with its intended use.

Mitigation: CLER uses role-based access and UserID/password to protect access to data. Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret and DB2 access are used to manage end user security. CLER maintains strong role-based security controls. The purpose and routine uses of the data include recording, processing, and reporting the FEHB enrollment data for USDA and other federal agencies.

Section 4: Notice

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

How does the project/program/system provide notice to individuals prior to collection?

CLER is only used by federal payroll offices and health insurance carriers to conduct quarterly reconciliation of FEHB enrollment data records. No notice is provided.

What options are available for individuals to consent, decline, or opt out of the project?

None.

Privacy Impact Analysis: Related to notice.

Privacy Risk: Individuals are unaware of the collection of information.

Mitigation: Agencies are responsible for notifying employees of information collected. 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.

Section 5: Data Retention

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

What information is retained and for how long?

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.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Mitigation: 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 lawsuits, and disciplinary actions. Retaining these records are in accordance with GRS I, which has a limited retention period, to mitigate privacy risks associated with maintaining these records.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

CLER does not share information with any internal organizations.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: CLER does not share information with any internal organizations.

Mitigation: The System 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 determined by the agency and based upon the application need and level to access the data.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Information collected by CLER is owned by each health insurance carrier and agency. NFC maintains and secures the information on behalf of our customers. CLER receives electronic FEHB enrollment data from health insurance carriers on a quarterly basis and federal payroll offices by pay period. The CLER database stores, maintains, processes, edits, and combines the data from the carriers and compares it to the data from the payroll offices. FEHB enrollment information is available on the CLER Web server where the agencies, carriers, OPM, and NFC access the information for inquiries, discrepancy corrections, and report generation. Authorized users can access CLER after security access is requested by the users' computer system security officer and clearance is provided by the NFC Information Systems Security Office (ISSO).

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: External organizations have only the information required to perform their business function.

Mitigation: 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 7: Redress

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

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

Individuals do not have access to their information. Only authorized users (federal agencies, health insurance carriers, OPM, and NFC) have access to CLER. NFC grants authority to use/access CLER at the request of OPM and the user's computer system security officer. Individuals who wish to have information about their own FEHB enrollment should contact their health insurance carrier and/or agency personnel office.

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.

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

Not Applicable.

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

Not Applicable.

Privacy Impact Analysis: Related to redress.

Privacy Risk: Redress is not available to individuals.

Mitigation: Individuals do not have access to the information in CLER. Only agency payroll office personnel have access to correct FEHB enrollment data. NFC access control procedures and role-based security of the application mitigate the risk of improper access.

Section 8: Auditing and Accountability

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

How is the information in the system/project/program secured?

CLER provides auditing at the application, database and network/operating system levels. The application is controlled by security attributes which only allow authorized users to access the system. The hosting environment also provides technical safeguards, such as database encryption, to prevent misuse of data.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

The agencies determine user access. NFC follows Directive 58, Information Security Program (Revision 2); and Directive 91, Role Based Security Access Policy.

How does the program review and approve information sharing requirements?

USDA requires annual system security assessments which include a review of information sharing requirements to fulfill mission and business objectives.

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

Employees and contractors must complete annual security training and be properly trained in the system.