Privacy Impact Assessment

OPM FEHB Centralized Enrollment Clearinghouse System (CLER)

- Version: 2.2
- Date: November 2018
- Prepared for: USDA OCIO

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

OPM FEHB Centralized Enrollment Clearinghouse System (CLER)

November 2018

Contact Points
Debby Tatum, Associate Director
Web Applications Directorate
504-426- 1102

Reviewing Official
Ivan Jackson, Associate Director
Information Technology Security
202-431-2971

USDA 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 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 has the ability to 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 is 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 relative 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 enrollees 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 1.0 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?

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, and NFC access the data for inquiries, discrepancy corrections, and report generation. Also, agencies and carriers maintain their contact information in CLER.

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

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 a primary contact in each of their organizations and must maintain the contact information in CLER.

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

The purpose of the data is to provide an efficient and cost-effective way for both health insurance carriers and federal government payroll offices to conduct a quarterly reconciliation of their FEHB enrollment records.

1.4 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.

1.5 How will the information be checked for accuracy?

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.

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

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

1.7 <u>Privacy Impact Analysis</u>: 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 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.

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

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 have the ability to access data elements depending on access privileges requested by authorized 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 health insurance carriers and federal agencies 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.

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 is 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 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?

CLER does not share information with any internal organizations.

4.2 How is the information transmitted or disclosed?

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.

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 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.

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?

Information collected by CLER is owned by each health insurance carrier and agency. NFC maintains and secures the information on behalf of our customers.

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.

NFC follows the USDA/OP-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?

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).

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 to payroll office employees regarding 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?

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

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

No. See 6.1.

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

No. See 6.1.

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.

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 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?

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.

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.

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

Not applicable.

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

Not applicable.

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

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 mitigates the risk of 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 Security Program (Revision 2); and Directive 91, Role Based Security Access Policy.

8.2 Will Department contractors have access to the system?

Yes, if authorized a valid role.

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

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

8.4 Has Assessment & Authorization 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?

CLER 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 CLER and security controls have been documented in the System Security Plan. These controls are tested annually under SSAE-16 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?

CLER is a web based centralized, automated system that timely and accurately reconciles payroll office and 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. The CLER database stores, maintains, processes, edits and combines the data from carriers and compares it to the data from payroll offices.

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

No. CLER is an established mainframe application with a web interface component on a Windows server, and a DB2 database on the NFC Mainframe. The NFC CLER MA inherits security protection implementations from the NFC Data Center and its supporting general support systems. Data security is achieved through resource allocation/access management implemented through Computer Associates' Top Secret (CA-TSS) software and other security software products. Data is routed into and out of the mainframe using the NFC Enterprise Infrastructure (EI) GSS. Data moving outside the LAN utilizes AT&T's secure network, Universal Telecommunications Network (UTN). Transmissions between CLER and OPM/Payroll Offices are conducted over secure VPN.

The CLER system has undergone a detailed security vulnerability assessment and has been Assessed and Authorized.

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?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

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: 2018.11.27 16:24:41 -06'00'

System Manager/Owner
Debby Tatum, Associate Director
Web Applications Directorate
Government Employees Services Division (GESD)
USDA National Finance Center

IVAN JACKSON

Digitally signed by IVAN JACKSON
Date: 2018.12.07 14:48:02 -06'00'

NFC Privacy Officer/ ISSPM/ CISO
Ivan R. Jackson, Associate Director
Information Technology Security
Information Technology Services Division (ITSD)
USDA National Finance Center

Agency Approval Signature

Adrianne F. Riviere, acting for Cristina Chiappe

Digitally signed by Adrianne F. Riviere, acting for Cristina Chiappe
Date: 2018.12.12 10:51:09 -06'00'

Authorizing Official Designated Representative
Cristina Chiappe, Director
Government Employees Services Division (GESD)
USDA National Finance Center