Privacy Impact Assessment for

FEHB Data Hub (HUB)

August 31, 2020

Contact Point
Dennis Hardy, Program Manager
Program Development and Support
Healthcare and Insurance

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The purpose of the FEHB Data Hub is to assist the Office of Personnel Management's (OPM) Healthcare & Insurance office in managing Federal Employees Health Benefits (FEHB) Program enrollment changes. Under the FEHB Program, OPM contracts with health insurance companies to offer health benefit plans. The Privacy Impact Assessment (PIA) is being conducted because the FEHB Data Hub collects, maintains, uses, and disseminates personally identifiable information about individuals who receive health insurance through the FEHB Program.

Overview

The Federal Employees Health Benefits (FEHB) Program is administered by the Office of Personnel Management's (OPM) Healthcare & Insurance (HI) office. It is the largest employer-sponsored group health insurance program in the world, covering over 8 million Federal employees, retirees, former employees, former spouses, and other eligible individuals plus their eligible family members. The FEHB Program offers over 200 fee-for-service and Health Maintenance Organization (HMO) health plan choices and FEHB carriers. An individual who chooses to participate in an FEHB plan can compare the costs, benefits, and features of different plans to make the best choice for themselves and their families.

The FEHB Data Hub is a service through which FEHB Program information is collected and exchanged. The Hub's principal function is to share the information that passes through the Hub with the various health insurance carriers that users select and, in some instances, from the carriers to other entities. The information is shared primarily to identify enrollees in the plan, indicate the enrollee and/or the family's eligibility for payment of a claim for health benefits services or supplies, and coordinate payment of claims with other carriers with whom the enrollee might also make a claim for payment of benefits. Specifically, the Hub receives electronic program enrollment

transactions from participating Hub agencies and posts enrollment data to a server for a secure, controlled distribution to FEHB Program carriers. The transactions include initial enrollments, changes to existing enrollments, cancellations, and terminations.

Information is also shared via the Hub in order to assist reconciling membership files from the FEHB carriers with enrollment files from the agencies. To do this, the Hub receives enrollment information from the FEHB carriers on a quarterly basis and pushes that information to the National Finance Center (NFC). The NFC houses the Centralized Enrollment Reconciliation Clearinghouse System (CLER), a system used to assist with maintaining the integrity of the carriers' membership files. Agencies also submit enrollment data, on a quarterly basis, to NFC for processing in CLER. NFC is then responsible for running a match between the enrollment data provided by the agencies and the enrollment data provided by the carriers. CLER then identifies any discrepancies between the data. , Once the data is processed, agencies review the data and take appropriate corrective action with the carriers. Carriers are responsible for processing corrective actions requested by the responsible agency either by receipt of Form SF-2809, Health Benefits Election Form, and Form SF-2810, Change in Health Benefits Enrollment Form, or by other notification. In some cases, the corrective action is made in CLER with the action being sent to the carrier through the Hub. CLER also has a reporting feature, which allows reports to be tailored to meet the needs of the requestor to assist in the reconciliation process.

The Hub also provides the carriers with an annual "crosswalk" of agency Payroll Office Numbers (PONs) to Employer Identification Numbers (EINs). This crosswalk assists the FEHB carriers with Internal Revenue Service (IRS) reporting requirements under the Employer Shared Responsibility (ESR) portion of the Affordable Care Act (ACA).

Also, as part of the ESR reporting requirements, each month a file of employees serviced by certain payroll Shared Service Centers (SSCs) is received by the Hub, which is then posted for pickup by the carriers to assist

with Internal Revenue Service reporting requirements. The information is required to confirm whether taxpayers have health insurance.

The Hub also serves to share information with OPM's Retirement Services (RS) in order to document those transactions that involve an enrollee's family members. This assists RS in accurately documenting an annuitant's family members, who may be eligible to receive benefits based on their relationship to the annuitant.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The FEHB Program is governed by 5 U.S.C. chapter 89, 5 C.F.R. parts 890 and 892, and the Employer Shared Responsibility (ESR) portion of the Affordable Care Act (ACA).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The records contained in the Data Hub are covered by the OPM/GOVT 1 General Personnel Records SORN and the OPM/Central 1 Health and Insurance SORN.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

FEHB Data Hub is in the process of receiving an independent security assessment and ATO outside of the scope of the existing ATO which is part of the Macon General Support System (GSS).

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

We are working to identify and/or develop an appropriate records schedule for the records in the Hub.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information is collected from enrollees through the Health Benefits Election Form (SF Form 2809), OMB Control number is 3206-0160. Information is also collected from agencies via the SF 2810, which is not subject to the PRA.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The Hub contains information about individuals who are enrolled in the FEHB Program and their eligible family members. The information includes: name, Social Security number, date of birth, address, phone number, email address, sex, marital status, relevant payroll office number, enrollment code for their chosen carrier, effective date of their coverage, Medicare status, and whether they have other insurance outside of the FEHB Program.

2.2. What are the sources of the information and how is the information collected for the project?

Most of the information in the Hub is submitted by participating agencies, who receive the information either directly from individual enrollees via the SF 2809 or indirectly through self-service systems that individuals use to enroll or change their enrollment options. These self-service systems include Employee Express, Employee Benefit Insurance System, myPay, PostalEase, Employee Self-Service, and Employee Personal Page and allow Federal employees and annuitants to view and make changes to their payroll and associated personnel records in one convenient location. The Hub also receives enrollment information from the FEHB carriers on a quarterly basis and pushes that information to the National Finance Center (NFC); and a weekly list of recent retirees from OPM's Retirement Services office (RS).

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The Data Hub uses information from commercial carriers who participate in the FEHB Program. The information from the carriers is used to identify enrollees and verify their enrollment. Information from the carriers is used to provide information to the National Finance Center to reconcile enrollment.

2.4. Discuss how accuracy of the data is ensured.

In most cases, the data is provided by the enrollee. The Hub verifies that there is a valid FEHB enrollment code, that certain fields have information in them and other basic validation checks. Unless there is an obvious error, the agencies do not verify this data. However, some accuracy is gained by the process of using social security numbers, which are collected and used to validate enrollees since they are the primary and common identifier used by agencies, FEHB Carriers, and the IRS.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information collected through the system is not accurate.

Mitigation: This risk is mitigated by exception processing located at the carriers, OPM staff and our enrollment reconciliation system. The Hub will not accept information that does not pass certain edit accuracy and HIPAA compliance formatting. However, the risk is not fully mitigated since the agencies do not verify this data. Information sent or gathered into the system will be assumed to be correct from the source and will not be subject to analysis or modification if incorrect.

Privacy Risk: There is a risk that the Data HUB will collect more information than is necessary to meet the business needs of the system.

Mitigation: This risk is mitigated by limiting the information collected, used, and disseminated by the Hub to that information that is on the SF 2809 and SF 2810. The Hub collects, uses, and disseminates only the information that is needed by the entities that interact with the Hub.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The HUB is a clearinghouse to move FEHB enrollment information between agencies, carriers, and the National Finance Center. The principal use of the HUB is to share information with the health insurance carrier that was selected by an enrollee. The HUB routes an enrollee's data via the plan code and sends it to a translator to make it Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant. The system is designed to coordinate with carriers and communicate information regarding an enrollee and FEHB plan details. The HUB reports family member information (via a data file) for Self Plus One and Family transactions to OPM/Retirement Services (RS) for RS-identified claims/SSNs.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The system does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

OPM Macon (the computer system and personnel at the OPM Computer Center in Macon, Georgia) is the administrator of the system and the only office with direct access to the system. The Healthcare and Insurance Office (HI) does not have direct access to the information that passes through the Hub but OPM Macon will provide the information to (HI) as needed. In

addition, Retirement Services (RS) provides information to and receives information from the Hub but does not have direct access into the system.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized persons may access information in the system for an unauthorized use.

Mitigation: This risk is mitigated through the use of defined user roles and access, which permit authorized users to access only information for which they have a need to know. Only those with a function related to managing the Hub will be granted access, and only authorized users may access or modify the data.

Privacy Risk: There is a risk that authorized users may access information that they are not authorized to see, use information for an unauthorized purpose, or inappropriately disclose this information, either intentionally or unintentionally.

Mitigation: This risk is mitigated by following a strict IT access provisioning policy, and through the use of role-based access controls, which limit the information authorized users can access or be sent only what they need to know for the agency's mission.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals who participate in the FEHB Program do not interact directly with the Hub and, therefore, do not receive direct notice from the Hub or specifically about the Hub. Individuals do receive notice about why the information they provide in the enrollment process is being collected and how it will be used via Privacy Act statements provided on the Health Benefits Election Form (SF Form 2809) provided to employees by their

employing agency. In addition, this PIA as well as the SORNs referenced in Section 1.2 also provide notice to individuals.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Participation in the FEHB Program is voluntary. The relevant Privacy Act statements that individuals receive when they enroll in the FEHB Program note that providing information is voluntary but that failure to provide it may result in a delay in processing their enrollment and failure to furnish an SSN or Medicare Beneficiary Identifier may impact the processing of the promptness of claims payments, proper coordination with Medicare, and/or proper insurance status reporting to the IRS. Once individuals enroll in FEHB, however, they do not have the opportunity to consent or decline to have their information included in the Hub.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice concerning how their information will be used and that it will be included in the Hub.

Mitigation: This risk is mitigated by providing individuals with a Privacy Act statement when they complete the F 2809. That statement outlines why their information is being collected and how it will be used. This PIA and the relevant SORNs also provide individuals with notice about the collection and use of their information.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The OPM's Macon Data Hub (Hub) provides a service through which data for the FEHB Program is passed to participating health insurance carriers and sometimes from the carriers back to OPM. It receives electronic program

enrollment transactions from participating agencies and posts enrollment data for distribution to FEHB Program carriers. The records that pass through or are used by Hub are meant to be of an intermediary nature. They are created or used in the process of creating a subsequent record by the insurance carriers or other agency systems. The program will work to identify and/or develop an appropriate records schedule for the records in the Hub.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than it is needed to meet the business needs for which it was collected.

Mitigation: This risk will be mitigated by identifying and/or developing an appropriate records schedule for the records in the Hub.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The Hub provides data to health insurance carriers that participate in the FEHB Program. Transfers of electronic program enrollment transactions from participating agencies come into the system, and then enrollment data is posted for distribution to insurance carriers. The Hub also receives membership files from carriers on a quarterly basis and pushes data to the National Finance Center (NFC) so that NFC can reconcile enrollment and payment information.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Providing information to the carriers and to NFC is compatible with the purposes expressed in the OPM/GOVT 1 General Personnel Records SORN, which is in part to determine status, eligibility, and employees rights and

benefits and to provide personnel services; and with the purposes expressed in the OPM Central 1 Retirement and Insurance Records SORN which is in part to verify and compute FEHB enrollments. The external sharing described in Section 6.1 is permitted by published routine uses that permit the disclosures, including routine uses d and f in the OPM/GOVT 1 SORN and routine uses n and ww in the OPM/Central 1 SORN.

6.3. Does the project place limitations on re-dissemination?

There are no limitations on re-dissemination of the information that is provided to the carriers, the participating agencies, or the NFC. However, no onward dissemination of the information is necessary and all entities in the information flow are subject to requirements related to the handling of PII.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The system generates audit logs that record the push or pull of data files, to include the carrier who picked up the generated output files.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be shared outside of OPM for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by providing information only pursuant to published routine uses in the applicable SORN and through role-based access controls to limit access to the Hub to only OPM management and technical staff with a need to know, participating agency personnel who have a need to know and provide information to the Hub, and to appropriate personnel at the FEHB carriers.

Section 7.0. Redress

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

Individuals do not have direct access to the Hub in order to view their FEHB enrollment information. Some individuals may, however, be able to access their enrollment information directly through another system, such as Employee Express or other self-service systems employed by their agency. In addition, individuals may request access to their records by following the process set forth in the OPM/GOVT 1 and OPM/Central 1 SORNs.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals do not have direct access to the Hub in order to make changes to their information directly. Some individuals may, however, be able to make changes and corrections to their enrollment information through another system, such as Employee Express or other self-service system employed by their agency, that will then be sent to the Hub. In addition, individuals can contact their agency human resources offices and in some cases the carriers directly in order to request assistance with correcting inaccurate or erroneous information. Individuals may also request amendment of their records by following the procedures set forth in the OPM/GOVT 1 and OPM/Central 1 SORNs.

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals do not receive any notice directly from the Hub. However, they are provided notice through this PIA, the applicable SORNs, and from their individual agencies regarding how to correct any erroneous or inaccurate information.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information that is contained in the Hub nor be afforded adequate opportunity to correct erroneous information.

Mitigation: This risk is mitigated by providing individuals with the opportunity to access and correct their information (though not via direct access to the Hub), through self-service systems, ability to contact appropriate personnel at their agencies or at the carriers, and through formal Privacy Act requests.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Access to the FEHB Data-Hub system is granted to appropriate OPM management and technical staff, agency data providers, and FEHB Carriers by the System Administration and Database Administration groups.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

OPM staff complete required IT security and privacy awareness training on an annual basis. There are no other specialized role-based trainings required to access the system.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

OPM uses software which allows system administrators to provide for account and role management. The software is restricted to authorized system administrators.

Supervisors must submit a technical personnel access request via an IT service portal. Only system administrators can grant access. Carriers are

vetted and granted access to individual SFTP folders via OPM's Change Review Board

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The project team works with the appropriate offices within OPM to follow guidelines and procedures to review and approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations within OPM and outside.

Responsible Officials

Laurie Bodenheimer
Acting Director, Healthcare and Insurance

Approval Signature

Signed Copy on file with Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer