



Privacy Impact Assessment for
FSAFEDS

February 25, 2022

Contact Point

Edward M. DeHarde

Assistant Director

Federal Employee Insurance Operations

Healthcare and Insurance

Reviewing Official

Kellie Cosgrove Riley

Chief Privacy Officer



Abstract

FSAFEDS is the federal flexible spending account program for individuals employed by the federal government. Through this program, eligible federal employees can set aside pre-tax funds to use later to pay for eligible medical, dental, and daycare expenses. FSAFEDS is administered through a platform managed by the FSAFEDS Contractor. The FSAFEDS Contractor provides participating federal agencies and employees with education, enrollment, administration, payment, and invoicing services. This Privacy Impact Assessment is being conducted because FSAFEDS collects, maintains, and disseminates personally identifiable information in conjunction with services provided to the federal participating agencies and employees.

Overview

The Federal Flexible Spending Account Program (FSAFEDS) is sponsored by the Office of Personnel Management and administered by a Contractor. FSAFEDS was established in 2003 and continues to offer federal employees an option to establish pre-tax accounts to cover out-of-pocket health care and dependent care expenses. There are three types of FSA accounts offered: general-purpose health care, limited expense health care, and dependent care.

- The general-purpose health care FSA (HCFSA) is a pre-tax benefit account used to pay for eligible medical, dental, and vision care expenses that are not covered by an individual's health care plan or elsewhere.
- The limited expense health care FSA (LEX HCFSA) is a partner FSA for individuals with a HSA-qualified high-deductible health plan with a Health Savings Account (HSA) through their carrier. It is a pre-tax benefit account used for eligible out-of-pocket dental and vision care expenses.



- The dependent care FSA (DCFSA) is a pre-tax benefit account used to pay for eligible dependent care services, such as preschool, summer day camp, before or after school programs, and child or adult daycare.

Eligible employees may enroll online annually during the Federal Benefits Open Season, within 60 days of entering federal service, or in connection with a qualifying life event at other times. Employees will go to www.FSAFEDS.com and set up an account providing the required demographic information and will then be directed to enter elections in the accounts they wish to establish. Once enrolled, participants may access their account information 24/7 online through the secure online account to obtain information about elections, claims adjudication, and balances.

Participant enrollment data is sent to BENEFEDS, a third-party Contractor for OPM, who then sends the data to the payroll providers to have the pre-tax per pay period deductions taken from payroll. Through this process, participants are validated as being active federal employees. The payroll providers send funding (dollars from payroll deductions) to the FSAFEDS Contractor to be loaded to participant accounts.

Participants may submit claims for reimbursement manually through mail/fax, online through the secure online account, mobile app, or take advantage of Paperless Reimbursement. By electing Paperless Reimbursement, participants allow their FEHB and FEDVIP carriers to send claims information to FSAFEDS for automatic processing. Participants can elect to have all claim reimbursements provided by the carriers processed automatically or choose which of those claims to be processed.

FSAFEDS offer various ways of receiving reimbursements, including check or direct deposit. Reimbursements are released daily to the option selected by the participant during enrollment. They can also update this option by logging into their account and updating the selection.



Participants are notified of critical timelines through the annual communication plan, such as Open Season and claim submission deadlines, via the website and email. These emails are sent through a third-party tool.

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?

OPM, and the FSAFEDS Contractor through OPM, is authorized to collect the information for FSAFEDS in accordance with the Federal Flexible Benefits Plan, a "cafeteria plan" under Section 125 of the Internal Revenue Code of 1986, as amended, and applicable regulations.

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

The applicable SORN is OPM CENTRAL-1 Civil Service Retirement and Insurance Records. Healthcare and Insurance (HI) are in the process of regrouping the records currently contained in OPM CENTRAL-1 and publishing the corresponding system of record notices. When a new system of records notice is published that applies to the information described in this PIA, this PIA will be amended to reflect this.

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

Yes. This system security plan was completed as part of the FSAFEDS ATO renewal issued on June 29, 2023.

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

The OPM Health and Insurance (HI) office is currently working to develop a records retention schedule.



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.

The PRA does not apply to the collection of information in this system.

Section 2.0. Characterization of the Information

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

The system may collect the following information from Federal employees who choose to enroll in FSAFEDS. Below are the potential data fields being collected for processing:

Agency, Sub Agency, Hire Date, First Name, Last Name, Middle Initial (not required), Date of Birth, Social Security number, Mailing Address, Zip code, Email, Phone Number, IP address, Bank Account Number, Bank Routing Number, Employment status and date (if provided), Employment termination date (if provided), FSA Election information (Healthcare and Dependent Care annual elections), Medical/Dental/Vision plan enrollment, payroll deductions applied to the accounts, Service Date, Service Type, Service description, Amount, Claim Number (from the carrier), CPT code (Current Procedural Terminology numbers sent by carriers), Service provider name, Service provider address, Patient Information – name and relationship, number (from carrier files), Letter of medical necessity, HIPAA authorization (name of individuals authorized to speak on the participants' behalf), HSA election (for HSA compatibility to determine if they have an HSA or not).

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

Federal employees, Federal Employees Health Benefits (FEHB) carriers, the Federal Employees Dental and Vision Insurance Program (FEDVIP) carriers, and BENEFEDS (payroll liaison) all provide information to the system. The



FEHB and FEDVIP carriers submit claim information on behalf of FSAFEDS participants who select this option for claims processing. BENEFEDS is a separate third-party Contractor that coordinates payroll files for employee payroll deductions.

Information will be collected via various methods: secure online accounts, secure file transfer capabilities, paper, telephone through customer service representatives, system to system, fax, and claim submission.

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

Commercial data is not utilized for this program.

2.4. Discuss how accuracy of the data is ensured.

The data used for administering the program is provided directly from federal employees who choose to participate in the program. The FSAFEDS Contractor partners with BENEFEDS to facilitate payroll deductions and, through that process, the participant's employing agency is validated. The FSAFEDS Contractor has also incorporated "red flag rules" within the application to identify relevant patterns, practices, and specific forms of activity that require validation with the participant, such as email address or banking information. These rules are set up so that participants are notified when changes have been made to their account to validate the activity. Participant validation helps protect against potentially fraudulent activities.

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

Privacy Risk: There is a risk that FSAFEDS may obtain more information than necessary to meet the business needs of the system.

Mitigation: This risk is mitigated by requesting only the data necessary to fulfill the plan's features. In addition, the system does not contain free-text fields that would allow for extraneous information to be entered.



Privacy Risk: There is a risk that information in FSAFEDS may not be accurate, leading to erroneous decisions that could adversely affect participants.

Mitigation: This risk is mitigated by confirming participant-provided data through a validation process that BENEFEDS conducts with payroll providers. Essentially, BENEFEDS is notified if a participant does not “exist” on their records. Once notified, BENEFEDS notifies the Contractor of the error and directs the participant to contact FSAFEDS. An example could be the wrong agency being selected during enrollment.

Section 3.0. Uses of the Information

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

The information obtained from federal employees who choose to participate in the program is used to establish their FSAFEDS accounts, to verify their eligibility, to exchange information with BENEFEDS to facilitate payroll deductions, to pay verified claims from participant accounts, and to obtain claims data from FEHB and FEDVIP plans for reimbursement of claims. The FEHB and FEVIP carriers provide claim information to FSAFEDS on behalf of participants who select this option for claims processing. This automation removes the need for participants to provide claims manually. In addition, the data is used to administer the program, which includes enrollment and claims administration.

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 FSAFEDS Contractor has incorporated “red flag rules” within the application to identify relevant patterns, practices, and specific forms of activity that signal possible identity theft. Red flag rules enable the FSAFEDS



Contractor to alert participants to changes on their account, such as updates to banking information, to validate that the participant made the change.

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

No

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

Privacy Risk: There is a risk that unauthorized persons may access the information in FSAFEDS or that authorized persons may access the information for any unauthorized purpose.

Mitigation: This risk is mitigated by restricting access to those contractor employees (including subcontractors) who need it to conduct the necessary actions to administer the program. Access to information is restricted to those with a need to know through role-based security and only with the approval of upper management.

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.

A Privacy Policy is available on the FSAFEDS website and can be viewed by the user at any time. In addition, this PIA and the SORN referenced in Section 1.2 also provide notice to individuals Terms and Conditions agreed to upon enrollment cover the program's rules, such as irrevocability of enrollment unless a qualifying event is experienced, deadlines for claim submission, etc. In addition, it confirms the individual understands deductions will be taken from payroll, that information will be shared with BENEFEDES and FEHB and FEDVIP carriers, and approval to contact via email/text/phone as needed.



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

By establishing an FSAFEDS account, individuals are consenting to the use of their information. Consent is granted during the registration of the account through affirmative acceptance of the Terms of Service. If individuals decline to provide certain information, they will be unable to participate in FSAFEDS.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive appropriate notice concerning what information will be collected about them and how that information will be used.

Mitigation: This risk is mitigated by participants providing data during enrollment, and use is outlined in the terms and conditions they attest to before starting the process.

Section 5.0. Data Retention by the Project

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

Data is required by the contract to be retained for at least six years from the contract award. HI is working to develop and obtain approval for a records retention schedule with NARA for the records in this system. This schedule will incorporate the records retention requirements of the contract between OPM and the FSAFEDS Contractor. Until this record schedule is finalized, records will be treated as permanent. Once the schedule is established, the methods for disposing of records that are no longer eligible for retention will be established.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information will be retained for longer than is necessary to meet the business needs and Federal requirements for



which it was originally collected or that it will not be retained for a sufficient period of time to meet the requirements of the Federal Records Act.

Mitigation: This risk is currently not mitigated but HI is working with the Agency Records Officer to establish a NARA-approved records schedule. Until that is in place, the records will be retained as permanent.

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.

Yes. Various service providers (subcontractors) are leveraged in the ongoing administration of the FSAFEDS program. These service providers assist in different roles to support the FSAFEDS administration. For example, they provide: staff augmentation for call center and claim processing support, FISMA approved data center to house FSAFEDS participant data, banking support for reimbursements via EFT and check, call recording, and email and text support as communication options

In addition, information is shared with BENEFEDS and FEHB and FEDVIP carriers. As stated above, BENEFEDS provides coordination with the payroll providers for payroll deductions. Participant information is shared with the applicable FEHB and FEDVIP carriers to enable them to provide claims information on behalf of participants who elected this option for claims processing.

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

The external sharing with contractors and subcontractors is done only for the purpose of administering the FSAFEDS program, pursuant to routine use "k" in the OPM/Central 1 SORN.



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

The FSAFEDS Contractor may utilize Service Providers or Business Associates, such as call center and claims processing support. If used, an executed business associate agreement is obtained. The agreement states that the subcontractors are subject to the same regulatory restrictions, conditions, and requirements applicable to the FSAFEDS Contractor and sets forth the appropriate collection, use, and disclosure of information related to plan administration.

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

The FSAFEDS Contractor maintains records based on enrolled plan participant activity or upon written HIPAA authorization to another entity at the direction of the plan participant.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information, once shared appropriately, will be further disseminated or used in a manner that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by the FSAFEDS contractor in agreements with subcontractors that outline the appropriate use and dissemination of the records.

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

Mitigation: This risk is mitigated through role-based access controls to restrict access to those who have a need to know and who are aware of the appropriate use and dissemination of the information.



Section 7.0. Redress

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

An individual participant can access their information directly via the call center, web portal, or mobile application.

In addition, individuals may request access to their information covered by the Privacy Act by following the procedures set out in the SORN referenced in Section 1.2. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and Social Security number. Individuals requesting access must also follow OPM's Privacy Act regulations to verify identity and access to records (5 CFR part 297).

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

Participants can correct information through their secure online account or by contacting FSAFEDS customer service.

In addition, individuals wishing to request amendment of their records covered by the Privacy Act may follow the procedures set out in the SORN referenced in Section 1.2. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and Social Security number. Individuals requesting access must also follow OPM's Privacy Act regulations to verify identity and access to records (5 CFR part 297).

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

Federal employees who choose to participate provide the information used to set up their accounts and administer the program and are provided with relevant information at that time. BENEFEDS notifies participants whose employment cannot be confirmed at the agency provided. Participants are directed to contact FSAFEDS to update their agency information. This is done



in order to correct any account errors and ensure payroll deductions are received so the benefit is available.

In addition, this PIA and the SORN referenced in Section 1.2 also provide notice to individuals.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information about them that is contained in FSAFEDS or be afforded adequate opportunity to correct that information.

Mitigation: This risk is mitigated by participants updating their information online or via the FSAFEDS Mobile Application. They may also reach the FSAFEDS contact center to update on their behalf, except banking information that participants must update directly.

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?

The FSAFEDS Contractor is contractually required to participate in audits conducted by the Office of Inspector General as requested.

Auditing is a shared responsibility between the data center provider and the FSAFEDS Contractor. Logs are reviewed monthly by the FSAFEDS Contractor's IT Operations team.

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

The FSAFEDS Contractor's employees undergo annual training in both privacy and security.



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

The FSAFEDS Contractor employs role-based security based on the principle of least privilege for access to sensitive information.

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?

Any changes to the contract, included new organizations or information sharing needs, are coordinated with the Program Office, Contracting Office, and the FSAFEDS Contractor for approval and updated via a contract modification, if applicable.

Responsible Officials

Edward M. DeHarde
Assistant Director
Federal Employee Insurance Operations
Healthcare and Insurance

Approval Signature

Signed copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer