Privacy Impact Assessment for

Federal Long Term Care Insurance Program (FLTCIP) System

January 14, 2022

Contact Point
Edward M. DeHarde
Deputy Associate Director
Federal Employees Insurance Operations
Healthcare & Insurance

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The Federal Long Term Care Insurance Program (FLTCIP) System is hosted by an Office of Personnel Management (OPM) Contractor. FLTCIP provides long-term care insurance to eligible Federal employees, annuitants, active and retired members of the uniformed services, and their qualified relatives on an enrollee-pay-all basis. This Privacy Impact Assessment is being conducted because the FLTCIP System collects, uses, disseminates, and maintains information about Federal employees, annuitants, certain members of and retirees from the uniformed services, and their qualified family members.

Overview

The Office of Personnel Management (OPM) Healthcare and Insurance office (HI) administers the Federal Long Term Care Insurance Program (FLTCIP), along with other insurance and benefits programs. FLTCIP provides long-term care insurance to eligible Federal employees, annuitants, active and retired members of the uniformed services, and their qualified relatives on an enrollee-pay-all basis. All enrollees must apply for FLTCIP coverage individually.

The FLTCIP System, including enrollment and claims administration functions, is operated by an OPM Contractor. The Contractor operates a website (www.LTCFEDS.com) where individuals can access educational information about FLTCIP. The website includes an enrollee portal, which allows users to apply online and manage their existing accounts.

The FLTCIP System is used for administering enrollment, underwriting, customer service and claims for the FLTCIP. It also interacts with the online enrollee portal and collects and maintains enrollee information, payroll/annuity provider information, eligibility status, and health information received during the application and claims processes. The FLTCIP backend database is hosted on a computer platform and stores

records specifically related to the users' online accounts and collects the information from online applications.

The Contractor maintains controls on the system in accordance with industry standards and practices. These controls comply with all applicable laws and guidance. All Contractor employees receive annual Security and Privacy Awareness Training. This Contractor-provided training addresses the requirements of the Privacy Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, allowable uses and disclosures of information, and reasonable safeguards.

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 FLTCIP Contractor pursuant to the contract with OPM, are authorized to collect the information in the FLTCIP System based upon the authority provided under 89 U.S.C. Chapter 90, Long-Term Care Insurance, and 5 CFR Part 875, Federal Long Term Care Insurance Program.

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

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

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

Yes. A system security plan was completed in connection with the Authority to Operate.

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

No. HI is currently working with the Agency Records Officer to develop and obtain approval for a records retention schedule for the records in the FLTCIP System.

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 information in the system is not currently subject to the PRA process. The Office of Privacy and Information Management will review relevant forms with HI to determine whether PRA applies.

Section 2.0. Characterization of the Information

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

During either the on-line or paper application process, applicants provide their name, gender, address, phone number, email address, Social Security number, date of birth, agency, employment status, billing information, and Social Security number of the employee if applicant is a qualified relative. If the applicant selects automatic bank debit for premium payments, they will provide a bank account number and bank routing number.

During the application process, certain applicants will provide medical information by answering questions needed to determine applicant eligibility. During the claims process, enrollees provide information about their care needs, doctors, and care providers, medical insurance information, other long term care insurance, and durable power of attorney/authorized contact information. Once approved, the FLTCIP enrollee is assigned an FLTCIP unique ID number.

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

Eligible Federal and United States Postal Service (USPS) employees and annuitants, active and retired uniformed service members, and certain qualified relatives provide the information that is contained in the FLTCIP System via a paper or online application process or by providing the information over the telephone to an FLTCIP customer service representative who then enters the information into the system. Information from a paper application is entered into the FLTCIP System by the New Business team members.

Information in the system may also be obtained from an individual's health care providers if the appropriate authorization is obtained from the applicant. FLTCIP underwriting applications have a Medical Release section that an applicant must sign in order to have the application processed. The release authorizes the FLTCIP Contractor and its subcontractors to receive health information in order to provide contracted services, including underwriting, claims, and customer service.

Premium and employment status is received from payroll providers. The FLTCIP Contractor works with the Enterprise Human Resources Integration (EHRI) system to obtain information such as hire date, agency code and payroll office indicator which assists with eligibility research and verification.

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

FLTCIP receives United States Postal Service (USPS) address updates from a vendor certified by the USPS, which verifies residential addresses of enrollees. Decedent information is obtained from the Social Security Death Master File (SSDMF).

The Contractor verifies certain demographic information such as provider tax identification numbers and also verifies date of death to assist with eligibility and claims operations.

During the FLTCIP underwriting process, an applicant's medical records are retrieved by a subcontractor and provided to the Contractor to determine if the applicant medically qualifies to have coverage under the program. The applicant signs a medical release form during the application process.

During a FLTCIP new claim benefit eligibility request and ongoing recertification process throughout the life of the claim for an FLTCIP enrollee, an enrollee's medical records may be retrieved by a subcontractor and provided to the FLTCIP Contractor to determine eligibility. The enrollee signs a medical release form during the benefit eligibility process.

A separate subcontractor conducts benefit eligibility on-site assessments, which are provided to the Contractor to determine eligibility.

2.4. Discuss how accuracy of the data is ensured.

The majority of medical records are obtained through a subcontractor retrieval vendor who obtains records directly from the provider or the provider's designated record keeper. The Contractor provides the subcontractor with SSN, Name, and DOB along with the standard FLTCIP authorization to obtain medical records. Prior to a request being sent by the subcontractor to a provider, the subcontractor will verify by phone that the provider matches the provider information provided by the applicant and that the provider has records for the applicant/claimant as well as being a licensed legitimate provider that operates under HIPAA. The vendor requests medical records from the provider's office or record keeper using the identifying information along with the authorization to obtain medical records.

Providers may also require a specific authorization to release records. In these cases, the vendor would obtain the authorization from the

applicant/claimant directly on the provider's form. When the records are received by the vendor, they validate the SSN, Name, and DOB to ensure they match an outstanding request. In addition, medical records sent by the vendor or the applicant directly are validated by the Contractor's Underwriter/Care Coordinator by comparing key identifying information that is normally a combination of SSN, Name, and DOB.

The Contractor incorporates Quality Control (QC) checks throughout its business processes to ensure the accuracy of the information received. Applicants are provided an opportunity to review information and certify it is accurate prior to submission.

The Contractor validates each name and address against the United States Postal Service (USPS) database to make sure the Contractor has the latest name and address. The Contractor validates enrollee information including claim number to verify that the enrollee is an annuitant receiving payment. The Contractor uses the payroll providers to verify Social Security number, eligibility, and employment status.

The FLTCIP System has QC checks built in to automatically check accuracy of information or search for anomalies. For outgoing mail containing personally identifiable information, the Contractor conducts manual QC checks that include address verification.

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

Privacy Risk: There is a risk that information that is not necessary for a business purpose will be collected and maintained in the FLTCIP System.

Mitigation: This risk is mitigated because the system is designed to collect only the information that is necessary to accomplish enrollment and claims and premium views in the benefit information offered by OPM through the portal. In addition, effective procedures have been established to avoid the unnecessary collection of information about individuals.

Privacy Risk: There is a risk that the information in the FLTCIP System may not be accurate, leading to erroneous decisions that could adversely affect an individual.

Mitigation: This risk is mitigated by the Quality Control procedures incorporated in the FLTCIP System, as discussed above in Section 2.4. In addition, enrollees in the program have opportunities to view and correct inaccurate information, as discussed below in Section 7.

Section 3.0. Uses of the Information

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

All information that is gathered during the application and enrollment process in FLTCIP, or in the course of customer service interactions, is used for managing enrollment and claims administration.

Social Security numbers (SSN) are collected from enrollees. Enrollees who wish to have their premiums deducted from their government payroll or pension must provide an SSN in order to identify enrollees in agency payroll and retirement systems. Additionally, all enrollees who file and are approved for claims must provide an SSN for tax purposes. All enrollees also have an FLTCIP unique ID assigned which is used to identify the accounts in place of an SSN, such as on direct bills and explanation of benefits statements.

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 Contractor uses several electronic searches, queries, and analyses, including scheduled control and ad hoc queries, analyses, batch modules that do reconciliations of enrollments and premiums, history search tools, marketing segmentation queries, system reports, and system data scans. The Contractor also uses aggregate information to improve the enrollee

website experience. These are not used, however, to discover predictive patterns or anomalies.

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

Besides HI and the FLTCIP Contractor, there are no other OPM programs or offices with assigned roles and responsibilities within the FLTCIP System.

The FLTCIP Contractor provides summary reports to OPM program management in HI on a regular basis and upon request. They also provide demographic data to the OPM Office of the Actuaries within HI. OPM actuaries receive a quarterly report from the FLTCIP Contractor with general demographic information about current claims, such as a breakdown of claims by age and gender.

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

Privacy Risk: There is a risk that the information in the FLTCIP System will be accessed by an authorized user for an unauthorized purpose and used in a manner that is inconsistent with the purpose for which it is being collected and maintained in the FLTCIP System. For example, authorized FLTCIP Contractor employees could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: This risk is mitigated through the use of Role Based Access Controls (RBAC) by the FLTCIP Contractor, comprised of employee provisioning, permissions management, and access controls. Access to the FLTCIP System by Contractor employees is limited to only the information needed to perform their assigned duties. In addition, FLTCIP Contractor employees are trained about appropriate uses of the data.

Privacy Risk: There is a risk that the PII in the FLTCIP System will be inappropriately exposed in the system, leading to unauthorized use.

Mitigation: The FLTCIP Contractor has undergone a review of its systems by OPM to ensure the confidentiality, integrity, and availability within the system. The FLTCIP Contractor conducts quarterly reviews of employee access to ensure all employee access to the FLTCIP System is in alignment with NIST controls.

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.

Notice is provided to individuals prior to the collection of information. FLTCIP provides statements about the collection of information via a Privacy Notice, and a HIPAA Privacy Notice found on the FLTCIP website. In addition, notices about the collection and use of information prior to application and enrollment in FLTCIP are provided on the FLTCIP website; through this PIA; and, more generally, via the SORN identified in Section 1.2.

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

The FLTCIP registration process is voluntary. Individuals can refuse to provide requested information by electing not to enroll in the program. However, individuals are informed that if they do not provide the requested information, their application for coverage or request for benefits cannot be processed.

During the FLTCIP registration process, individuals are provided with the opportunity to opt out of receiving marketing material and the Contractor stores this indicator so individuals will not be sent marketing material.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is 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 the Privacy Notices found on the FLTCIP website. In addition, notices prior to application/enrollment in FLTCIP are provided on the FLTCIP website; through publication of this PIA; and the SORN referenced in Section 1.2. Additionally, individuals are notified by their agencies, which are responsible for counseling employees regarding their rights and benefits. This risk should be further mitigated by the inclusion of an appropriate Privacy Act statement at the point of information collection and HI will work with the Contractor to put that in place.

Section 5.0. Data Retention by the Project

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

HI is working to develop and obtain approval for a records retention schedule with NARA for the records contained in this system. This schedule will incorporate the records retention requirements of the contract between OPM and the FLTCIP 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.

Individual application and enrollment information will be retained in the FLTCIP System for as long as the enrollee is eligible for coverage in order to collect and administer premiums, process claims, and adjust coverage as needed upon request from the enrollee or upon automatic adjustments to accommodate inflation.

Pursuant to the contract between OPM and the FLTCIP Contractor, the Contractor is required to retain and make available all records throughout the life of the contract and to continue to retain all records that support the annual statement of operations for a period of 5 years after the end of the year to which the records relate. Individual enrollee claims records will be maintained for 10 years after the end of the year to which the claim records

relate. The threshold described above does not apply to records related to open audits being conducted by OPM's Office of the Inspector General, provided the Contractor was notified of the audit within the records retention timeframes. Specific records identified in the scope of these open audits are maintained until the audits are resolved by OPM.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in the system 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 not currently mitigated but HI is working with the Agency Records Officer to establish a NARA-approved records schedule. Until a records schedule has been established, the Contractor will not delete any of the records in the system. Once the schedule is in place, HI will work with the contractor to implement the schedule.

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 FLTCIP Contractor shares individual enrollee data with various subcontractors where necessary to fulfill the underlying FLTCIP contract requirements. As an example, the FLTCIP Contractor shares information with a subcontractor that conducts on-site assessments for new and existing claims to determine eligibility. The agreements with subcontractors limit the use of the information and require compliance with Federal law and policy to safeguard enrollee information. In addition, the Contractor uses commercial print vendors for enrollee mailings to provide bulk mailing capacity; uses an external vendor to perform address scrubs (i.e., obtaining an address

preferred by the U.S Postal Service); and uses subcontractors to obtain medical records used by the Contractor for underwriting and to conduct benefit eligibility on-site assessments (as described in Section 2.3).

FLTCIP premium information is stored in the FLTCIP System however FLTCIP premium functions are administered as part of the BENEFEDS contract and covered under the respective BENEFEDS Privacy Impact Assessment.

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

Consistent with the purpose articulated in the OPM Central-1 SORN, the Contractor discloses the records in this system in order to obtain information and verification on which to base eligibility for application, complete enrollment, determine benefit eligibility, and perform claims administration and premium deduction. The disclosure is made in accordance with an appropriate routine use in the applicable SORN, including routine use (k).

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

Yes. Use and disclosure of FLTCIP information is subject to the terms in signed contracts which limit re-dissemination for a purpose other than meeting the requirements of the contract. For example, the Contractor and subcontractors are specifically not permitted to use or collect enrollee data for marketing purposes.

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

The project tracks all disclosures of PII and PHI through the Contractor's compliance department. The tracking mechanism includes the following information: enrollee's name; enrollee's FLTCIP unique ID; date request received; date information was sent; name of individual/entity to whom the information was disclosed; if disclosed to a third party, the authority allowing the disclosure; and the address to which the information was sent or securely emailed. A copy of the information disclosed is saved to the enrollee's file for reference.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information from the FLTCIP System may be inappropriately disclosed outside of the Contractor's facility.

Mitigation: This risk is mitigated by the fact that information maintained in the FLTCIP System is only shared in a manner consistent with the routine uses prescribed in the SORN identified in Section 1.2, and consistent with OPM's contract requirements or required by law. This risk is further mitigated through role-based access controls used by the FLTCIP Contractor to limit access of information to approved staff and training provided to Contractor staff.

Privacy Risk: There is a risk that information, once shared appropriately, will be further shared or used in a manner that is inconsistent with the original purpose for which it was collected.

Mitigation: This risk is mitigated through the use of written contracts and agreements that define the purposes for which the information is shared, prohibits additional uses, and defines limits for any further sharing with third parties or legal entities.

Privacy Risk: There is a risk that information will be lost or misused in transit or by the receiving entities with which the FLTCIP System shares information.

Mitigation: This risk is mitigated by transmitting information via secure connections pursuant to NIST standards. In addition, the FLTCIP Contractor has activated security safeguards to monitor the movement of PHI and PII within the company network as well as movement outside of the company network.

Section 7.0. Redress

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

Individuals may access their own records on the FLTCIP website by following a two-step identification and authorization process using a personal or system user identifier and a password or other personal information. More generally, individuals may request access to their Privacy Act covered information by following the procedures set out in the OPM CENTRAL-1 SORN. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and Social Security number or FLTCIP unique ID. In addition, individuals requesting access must also follow OPM's Privacy Act regulations on verification of 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?

FLTCIP applicants are provided an opportunity to review information and certify it is accurate prior to submission and receive a full copy of their application for coverage. Enrollees can review and correct their information throughout the year. Since medical records are received from health care providers, the applicant or enrollee must contact the respective provider to access and correct medical information.

In addition, individuals wishing to request amendment of their records covered by the Privacy Act may follow the procedures set out in the OPM CENTRAL-1 SORN. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and Social Security number. In addition, individuals requesting access must also follow OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

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

The FLTCIP website contains a Privacy Notice that describes how individuals can access and correct information in the system. Additionally, individuals are notified by their agencies, which are responsible for counseling employees regarding their rights and benefits, and through publication of this PIA and the OPM CENTRAL-1 SORN.

7.4. Privacy Impact Analysis: Related to Redress

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

Mitigation: This risk is mitigated as FLTCIP applicants are provided an opportunity to review information and certify it is accurate prior to submission and receive a full copy of their application for coverage. Enrollees can review and correct their information throughout the year by accessing the system. The Contractor offers several options for accessing and correcting account information, including access to customer service representatives by telephone, or by mail. Specific telephone numbers and email and postal addresses are listed on the FLTCIP website.

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 FLTCIP Contractor performs quarterly self-assessments of compliance with the NIST security control framework. Triennially, the Contractor has a third-party security firm conduct a FISMA (Federal Information Security Modernization Act) Assessment and prepare all forms needed for the OPM Authority to Operate (ATO).

A formal development process exists for the systems that support FLTCIP. The FLTCIP System is constantly reviewed for risk and during any changes, the Contractor's change control board considers risks to the system and to individual's data.

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

Annual training is provided to all existing FLTCIP Contractor employees as a condition of employment. All Contractor employees receive annual Security and Privacy Awareness Training. This training addresses the requirements of the Privacy Act and HIPAA Privacy and Security Rules, allowable uses and disclosures of information, and reasonable safeguards. Security training examines appropriate administrative, physical, and technical safeguards. The Contractor's human resources department coordinates the on-line training and maintains documentation of completion for each employee. This training is also administered at time of hire.

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 FLTCIP Contractor has separate business units handling system management, programming, and quality assurance. Users with access to the Contractor's transactional systems all have unique IDs. The Contractor ensures separation of duties of individuals as necessary to prevent collusion for malicious purposes, documents the separation of duties, and implements this separation through assigned system access authorization and controls for this separation via automated control programs. The Contractor requires documentable evidence of its separation of duties, and information system-specific permissions separate how users have access to the system.

The Contractor requires its management to review access authorization to applications and systems. These access requests must be documented and approved, and access is reviewed on a regular basis for appropriateness. Additionally, the Contractor's administration accounts are closely monitored.

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 information sharing agreements are drafted with input from various Contractor subject matter experts. The documents go through a review and approval process across multiple layers of personnel to ensure completeness and accuracy.

The OPM staff also reviews any information sharing agreements every three years for renewal or as necessary updates are required. Any new access to the system will be evaluated by the appropriate personnel. New uses of the information are business decisions determined by the FLTCIP Contractor's Executive Management Office, in coordination with OPM.

Responsible Officials

Edward M. DeHarde
Deputy Associate Director
Federal Employees Insurance Operations
Healthcare and Insurance

Approval Signature

Kellie Cosgrove Riley
Chief Privacy Officer