Privacy Impact Assessment for

Federal Long Term Care Insurance Program (FLTCIP) System

October 29, 2025

Contact Point
Delon G. F. Pinto, System Owner
Healthcare and Insurance
Life and Ancillary Benefits

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

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 interested persons must apply for FLTCIP coverage individually.

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

The FLTCIP System interacts with the online portal and collects and maintains insured individual's 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 FLTCIP Contractor maintains controls on the system in accordance with industry standards and practices. These controls comply with all applicable laws and guidance. All FLTCIP 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.

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 information in the FLTCIP System based upon the authority provided under 5 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 records contained in this system are covered by OPM Central-26, FEDVIP, FLTCIP, and FSAFEDS Records.

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. However, in alignment with the FLTCIP contract and HIPAA record retention requirements, the FLTCIP Contractor will retain and make available all records that support the annual statement of operations for a period of 6 years after the date of creation or the date they were last in effect. Insured individuals' claims records will be maintained for 10 years after the end of the year to which the claim records relate. The retention thresholds described above do not apply to records related to open audits being conducted by OPM's Office of the Inspector General, provided the

FLTCIP Contractor is notified of the audit within the records retention timeframes. Specific records identified in the scope of such audits must be maintained until the audits are resolved by OPM.

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 FLTCIP System team is collaborating with OPM's PRA manager to ensure any collections covered by the PRA provide appropriate notice.

Section 2.0. Characterization of the Information

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

During both the on-line and paper application processes, applicants provide their name, address, sex, date of birth, phone number, email address, Social Security number (SSN), employing agency and employment status if applicable, and billing information. If the applicant is a qualified relative of a federal employee or annuitant, the applicant must also provide the Federal employee or annuitant's, name, date of birth, and SSN.

Although applications for coverage are currently suspended, during periods of non-suspension, newly eligible Federal employees and their spouses may qualify for abbreviated underwriting if they apply within 60-days of becoming eligible. Federal employees and spouses who do not apply during the initial 60-day eligibility period and later enroll during an open enrollment period are subject to full underwriting and must complete a health assessment so that the FLTCIP Contractor can determine their insurability. Qualified relatives are always subject to full underwriting. As part of the underwriting process, the FLTCIP Contractor may collect records from an applicant's health care providers and ask the applicant to complete various health screenings.

At the time of application, individuals may optionally elect to name a non-household member to receive notice if, in the future, insurance coverage is

at risk of lapsing because the FLTCIP Contractor does not receive premium payments. Applicants who designate such an individual must provide that person's name, address, and telephone number. In addition, FLTCIP 3.0 coverage uniquely includes a premium stabilization feature that gives applicants the option to designate up to four beneficiaries to receive a refund of premium death benefit. For each such individual named, an SSN, address, e-mail, and phone number are collected.

During the enrollment process, individuals must also select their preferred billing option: direct bill; payroll or annuity/pension deduction; or automatic bank withdrawal. Applicants who select direct bill do not need to provide any additional information. However, applicants who select payroll or annuity/pension deduction must provide their CSRS/FERS account number or the name, SSN, and CSRS/FERS account number of the payor. Applicants who select automatic bank withdrawal must provide a checking or savings account number. Paper applicants are also asked to include a voided check or deposit slip, as applicable.

Once approved for long term care insurance coverage, each enrolled participant of the FLTCIP is assigned a FLTCIP unique ID number, which reduces the need to use an SSN as an identifier.

Later, when an insured individual initiates a claim, the individual must again provide sensitive information and explain why a claim is being filed. That explanation could include information about the insured individual's care needs and/or diagnosis of a cognitive impairment such as Alzheimer's disease or dementia. Insured individuals are also asked to submit information about all the clinicians they have seen in the last 12-months as well as any hospital or rehabilitation facility stays. When a claim is initiated, the insured individual must provide insurance information, including coverage under any medical or other long term care insurance policy for coordination of benefits purposes. Insured individuals who want to authorize someone to make decisions on their behalf must submit a copy of their durable financial power of attorney or guardianship papers. They are encouraged to do so before the need arises so that the benefit eligibility and claims processes are seamless.

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

Individuals enrolled in the FLTCIP could be Federal and United States Postal Service (USPS) employees and annuitants, active and retired uniformed service members, and certain qualified relatives of those individuals. Such persons may provide information directly into the system via an online portal or a customer service representative may act as an intermediary and enter into the system information transcribed from an e-mail, telephone conversation, facsimile, or letter.

In addition, both the full and abbreviated FLTCIP underwriting applications have a Medical Release section that an applicant must sign to have the application processed. The Medical Release authorizes the individual's health care providers to release, to the FLTCIP Contractor and its subcontractors, health information to provide contracted services, including underwriting, claims administration, and customer service.

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

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 FLTCIP Contractor receives USPS address updates from a vendor certified by the USPS, which verifies residential addresses of insured individuals. Decedent information is separately obtained from the Social Security Death Master File (SSDMF).

The FLTCIP Contractor also uses information from several other commercial sources in connection with administrative tasks such as benefit eligibility and claims payments. For example, the FLTCIP Contractor uses Accurint, a Lexis Nexis product, to verify SSNs for Informal Care providers as well as to verify tax ID numbers for formal providers. The FLTCIP Contractor also uses

Accurint death records to determine when a death has occurred so that premium billing and claims payments can be stopped. The FLTCIP Contractor uses TransUnion's TLOxp to assist in the investigation of cases of suspected fraud by identifying connections between people, accounts, and business through verification of details such as phone numbers, address history, and professional licensure, as applicable.

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

Subsequently, when a benefit eligibility request is made, and throughout the life of a claim, the insured individual's medical records may also be retrieved by a subcontractor and provided to the FLTCIP Contractor so that the insured individual's condition can be assessed to determine benefit eligibility and whether to approve the claim. An insured individual may be asked to sign another Medical Release during the benefit eligibility and/or claims review process. The FLTCIP Contractor cannot determine whether an insured individual is eligible for benefits without access to applicable medical records.

Additionally, the FLTCIP Contractor subcontracts with a company to perform virtual and on-site health assessments of insured individuals to aid in the determination of whether a claim should be approved. Whenever such an assessment is performed, the subcontractor produces a report containing medical information and submits it to the FLTCIP Contractor.

2.4. Discuss how accuracy of the data is ensured.

Most medical records are obtained through a subcontractor who obtains electronic and paper records directly from health care providers or the providers' designated record keepers. To facilitate retrieval of medical records, the FLTCIP Contractor provides the subcontractor with an individual's SSN, Name, and DOB along with a copy of the signed authorization to release medical records, which is then forwarded to the applicable health care providers. The subcontractor will verify by phone that

a health care provider matches the provider information submitted by the applicant/claimant and has records for the applicant/claimant, before forwarding the release to the health care provider's office or record keeper. However, over time, the FLTCIP Contractor has learned that some health care providers will not release medical records unless they receive authorization on a practice-specific form. In these cases, the subcontractor works with the applicant/insured individual to obtain and complete the specified form so that the medical records can be obtained.

Whenever medical records are received by the subcontractor, they check the SSN, Name, and DOB to ensure they match an outstanding request for records. Separately, whenever medical records are received by the FLTCIP Contractor from either the subcontractor or directly from the applicant/claimant, the FLTCIP Contractor confirms that they received the correct records by comparing key identifying information that is normally a combination of the individual's SSN, name, and DOB.

Applicants who collect information to submit to the FLTCIP Contractor or its subcontractor can review that information prior to submission. The FLTCIP Contractor also incorporates additional Quality Control (QC) checks throughout its business processes to ensure the accuracy of the information received. The FLTCIP System has QC checks built in to automatically check the accuracy of information and search for anomalies. For example, on a quarterly basis, the FLTCIP Contractor validates each insured individual's address against the USPS database and makes changes in its system as needed. If an insured individual's address appears to have changed, the FLTCIP Contractor sends a letter to the old and new addresses as confirmation. The FLTCIP Contractor also uses agency payroll providers to verify SSN, eligibility, and employment or annuity status.

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 provide premium and claims views to insured individuals. Effective procedures have been established to avoid unnecessary information collection.

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, insured individuals 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, and during customer service interactions, is used for managing enrollment and benefits administration.

SSNs are collected from insured individuals and used to verify identity. Insured individuals who wish to have their premiums deducted from their government pay or annuity/pension must provide an SSN so that the FLTCIP Contractor can confirm employment or retirement status with agency payroll offices and retirement systems, as applicable. All insured individuals also have a FLTCIP unique ID assigned upon enrollment, which is used to identify accounts in place of an SSN in account communications such as direct bills and explanation of benefits statements. All insured individuals who file a claim for benefits, and are approved, must complete Form W-9; it requires the individual's SSN because the FLTCIP Contractor must report the benefits paid during the year to the Internal Revenue Service for tax purposes.

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 FLTCIP 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 FLTCIP Contractor also uses aggregated 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 also upon request. The FLTCIP Contractor also provides demographic data to the OPM Office of the Actuaries within HI. OPM actuaries receive quarterly reports from the FLTCIP Contractor that include current claims experience, stratified by demographics such as age and sex.

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 perform illegitimate 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 FLTCIP 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, including HIPAA Privacy and Security trainings.

Privacy Risk: There is a risk that the PHI/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, which are also found on the FLTCIP website and available to the public prior to application and enrollment in FLTCIP; 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?

Enrollment in the FLTCIP is voluntary. Individuals can refuse to provide the requested information by electing not to apply to the program or by submitting an incomplete application. However, individuals are informed that if they do not provide all the requested information, their application for coverage or subsequent request for benefits eligibility determination/claims approval cannot be processed.

The FLTCIP contractor may do a limited marketing of its service to applicants, but during the FLTCIP application process, individuals are provided with the opportunity to opt-out of receiving marketing material and the FLTCIP Contractor stores this indicator so individuals will not be sent marketing material. Insured individuals can update their election at any time via the online portal.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is risk that individuals will not receive adequate 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, which are available to the public; 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.

Section 5.0. Data Retention by the Project

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

As noted in section 1.4, and in alignment with the FLTCIP contract and HIPAA requirements, the FLTCIP Contractor will retain and make available all records that support the annual statement of operations for a period of 6 years after the end of the year to which the records relate. Claim records from insured individuals will be maintained for 10 years after the end of the year to which the claim records relate. The retention thresholds described above do not apply to records related to open audits conducted by OPM's Office of the Inspector General, provided the FLTCIP Contractor is notified of the audit within the records retention timeframes. Specific records identified in the scope of such audits must be maintained until the audits are resolved by OPM.

Individual application and enrollment information will be retained in the FLTCIP System for as long as the individual is eligible for coverage to support the collection of premiums, processing of claims, and adjustment of coverage upon the request of an insured individual or in the event of automatic benefits adjustments due to inflation.

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 HIPAA or the Federal Records Act.

Mitigation: The FLTCIP Contractor is working on mitigating this risk by implementing the above-described record disposal 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 enrollee information with various subcontractors as necessary to fulfill the underlying FLTCIP contract requirements. As an example, the FLTCIP Contractor shares personally identifiable information with a subcontractor that conducts virtual and on-site health assessments to determine new and continuing eligibility for benefits. In addition, the FLTCIP Contractor uses commercial print vendors to send bulk mailings to insured individuals; 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 FLTCIP Contractor for underwriting and benefit eligibility/claims review processes (as described in Section 2.3). Agreements with subcontractors limit the use of enrollee information and require compliance with Federal laws and regulations that aim to safeguard sensitive information.

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-26 SORN, the FLTCIP Contractor discloses the records in the system to obtain information and verification on which to base eligibility for application, complete enrollment, collect premiums, determine benefit eligibility, and perform claims administration. The disclosure is made in accordance with an appropriate routine use in the applicable SORN, including routine use (g).

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 any purpose other than meeting the requirements of the contract.

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 FLTCIP Contractor's compliance department. The tracking mechanism includes the following information: insured individual's name; insured individual's FLTCIP unique ID; date request for disclosure is received; date information is sent; name of individual/business entity to whom the information is disclosed; the address to which the information is electronically sent or securely mailed; and, if disclosed to a third party, the authority allowing for the disclosure. A copy of the information disclosed is also saved to the insured individual'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.

Mitigation: This risk is mitigated by policies that require information maintained in the FLTCIP System only be 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 as otherwise 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, who are trained on appropriate access of the FLTCIP System and use of information contained therein.

Privacy Risk: There is a risk that information, once shared appropriately, will be further used or disclosed 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 permissible data use and disclosure and prohibit additional uses and disclosures for purposes unrelated to contract administration.

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 in the FLTCIP portal by following a multifactor authentication (MFA) process using a personal or system user identifier and a password or other personal information. Additionally, implementation of optional phishing-resistant MFA is offered to the user using OKTA as the MFA authentication service which allows an additional layer of security.

More generally, individuals may also request access to their Privacy Act covered information by following the procedures set out in the OPM CENTRAL-26 SORN. Individuals must furnish certain information for their records to be located and identified. 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. Insured individuals can review and correct their information at any time. However, since medical records are received from health care providers, an individual must contact the respective health care provider to request a correction of any information contained therein. After correction, the individual can resubmit the applicable medical record

to the FLTCIP Contractor or its subcontractor.

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-26 SORN. Individuals must furnish certain information for their records to be located and identified. 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-26 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 an adequate opportunity to correct that information.

Mitigation: This risk is mitigated as FLTCIP applicants are provided opportunity to review information and certify it is accurate prior to submission and receive a full copy of their application for coverage. Insured individuals can review and correct their information at any time by accessing the online portal. The FLTCIP Contractor offers several options for accessing and correcting account information, including access to customer service representatives by telephone, email, 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 monthly self-assessments of compliance

with the NIST security control framework and reports results to OPM monthly. Triennially, the FLTCIP 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 continuously reviewed for risk and during any changes, the FLTCIP Contractor's change control board considers risks to the system and to individuals' data.

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

Annual Security and Privacy Awareness Training is provided to all existing FLTCIP Contractor employees and must be completed as a condition of employment. This training addresses the requirements of the Privacy Act and HIPAA Privacy and Security Rules and covers topics such as allowable uses and disclosures of information, and the use of safeguards to protect sensitive information. This training examines administrative, physical, and technical safeguards. The FLTCIP Contractor's human resources department coordinates the training and maintains documentation of completion for each employee. This training is first administered at the time of hire, and then annually thereafter.

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 FLTCIP Contractor's transactional systems have unique IDs. The FLTCIP 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 FLTCIP Contractor requires documentable evidence of its separation of duties, and information system-specific permissions separate how users have access to the system.

The FLTCIP Contractor requires its management to review access requests for applications and systems. These access requests must be documented and approved, and access is reviewed on a regular basis for appropriateness.

Additionally, the FLTCIP 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 FLTCIP Contractor subject matter experts. The documents go through a review and approval process across multiple layers of personnel to ensure completeness and accuracy.

OPM staff also review any information sharing agreements every three years for renewal or sooner when 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

Delon G. F. Pinto, System Owner
Healthcare and Insurance
Life and Ancillary Benefits

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy (SAOP)
Office of Personnel Management

Please note that the FLTCIP enrollment process has been suspended since December 2022. HI should contact the System Owner before enrolling new members in the FLTCIP.