Privacy Impact Assessment for

Multi-State Program Plan System (MSPPS)

February 21, 2020

Contact Point
Dennis Hardy, Program Manager
System Development and Implementation

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OPM Form 5003

Abstract

The Multi-State Plan Program System (MSPPS) was established to assist the Office of Personnel Management's Healthcare & Insurance in managing its responsibilities for the MultiState Plan (MSP) Program as authorized by the Patient Protection and Affordable Care Act. Under the MSP Program, the Office of Personnel Management contracted with private health insurance companies to offer health insurance on the Health Insurance Marketplace, processed MSP enrollees' requests for external review of an insurance carrier's decision, and maintained certain business contact information for external entities. Effective January 1, 2020, the MSP Program has been suspended. There are no longer any individuals enrolled in the MSP Program nor are there further options to enroll in the program. However, those individuals who were previously enrolled with an MSP health insurance carrier may still request external review of denied claims and all information previously collected within the MSPPS will be retained pursuant to the applicable records retention schedule. This Privacy Impact Assessment (PIA) is being conducted because the MSPPS collected and may continue to collect personally identifiable information from MSP enrollees who request external review of their denied claims.

Overview

The Multi-State Plan Program System (MSPPS) was established to assist the Office of Personnel Management's Healthcare & Insurance (H&I) in managing its responsibilities for the Multi-State Plan (MSP) Program as authorized by the Patient Protection and Affordable Care Act (ACA). The ACA authorized OPM to contract with private health insurance companies to offer individual and small group health insurance on the Health Insurance Marketplace established by the ACA. This involved H&I reviewing applications and proposed rates and benefits plans from the health insurance companies (MSP Issuers). Effective January 1, 2020, the MSP Program has been suspended and new MSP options will not be offered on the Health Insurance Marketplace. In addition, there are no current enrollees in the MSP Program and individuals can no longer choose to enroll in an MSP option. However, the MSPPS will remain active and in use for some time as H&I will continue to process and evaluate former enrollee's requests for external review of MSP Issuers' decisions. Former enrollees have up to five years to request

such review after the denial of a claim. In addition, all information contained in MSPPS will be maintained pursuant to the applicable records retention schedule.

MSPPS is a web-based, paperless suite of systems which support administration of the MSP Program. There are three project components within the MSPPS related to the MSP Program. These include the MSP Application Portal, External Review, and Contact Account Management.

1) The MSP Application Portal contains the electronic application that health insurance carriers completed to become an MSP Issuer. After January 1, 2020, no new applications will be accepted or processed.

2) The MSP External Review component is used as the official system of record for when an MSP Issuer denies a claim or request for benefits coverage to an MSP enrollee, and the enrollee decides to appeal the MSP Issuer's decision. To request External Review, the MSP enrollee submits a request to OPM for External Review by completing an intake form that asks for personally identifiable information about the enrollee, to include details about the relevant medical case. OPM External Review staff saves the information in an electronic log and uses the information to render a determination. In cases that require independent medical judgment, OPM shares the MSP enrollee's information, upon written permission from the MSP enrollee, with an Independent Review Organization, which makes the final determination.

3) The Contact Account Management component serves as an electronic address book for OPM staff and contains the business contact information for State Departments of Insurance and State Exchanges.

In addition to the MSP Program components referenced above, the MSPPS also contains the Federal Employees Health Benefits (FEHB) Disputed Claims system, which tracks and processes requests for review of FEHB carrier decisions. The FEHB Disputed Claims system is currently undergoing a separate PIA, which will be published upon completion.

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?

Section 1334 of the Affordable Care Act, 42 U.S.C. § 18054, and 45 C.F.R. § 800.503, cover OPM's administration of the External Review Process for disputed adverse benefit determinations submitted by MSP enrollees.

In determining the MSP Program External Review Process standards, OPM also relies on section 2719 of the Public Health Service Act (PHSA) and 45 C.F.R. § 147.136(d) (amended effective January 19, 2016).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?
The records contained in the MSPPS are covered by the OPM/Central-19: External Review Records for MSP Program SORN.

1.3. Has a system security plan been completed for the information system(s) supporting the project?
Yes. The system is currently undergoing security assessment to be completed by the end of February 2020, at which time a new Authority to Operate will be granted. The system security plan is an artifact within the security assessment package.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?
Yes. Records Schedule Number DAA-0478-2015-0001 has been approved by NARA.

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 MSP Program External Review Intake Form (OPM Form 1840), and the OMB Control number is 3206-0263.

Section 2.0. Characterization of the Information

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

The MSP Application Portal maintains information submitted by health insurance companies that previously participated in the MSP Program. Information includes organizational information, plan rates and benefits, accreditation information, level of coverage (bronze, silver, gold, or platinum), service area, and status (OPM's approval and certification status).

The MSP Program External Review component tracks and maintains information about former MSP enrollees who request external review of denied claims. When MSP enrollees contact OPM to request external review, they provide information which is entered into the External Review system by OPM's External Review team. Enrollee information includes member name, address, identification number, date of birth, claim number, provider's name address, procedure codes, services rendered, diagnosis, and denial information. In addition, other specific details are recorded in the system, including case category (contractual, medical necessity, both contractual and medical necessity), and case decision (ineligible for external review, insufficient information, administrative reversal, issuer denial upheld, issuer denial partially upheld, issuer denial overturned, withdrawn by enrollee/authorized representative).

The Contact Account Management component contains business contact information for State Departments of Insurance and State Exchanges, which assisted the MSP Program in managing its State government agency communications in a paperless environment.

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

The information in the MSP Application Portal was submitted directly by health insurance companies that sought to participate in the MSP Program.

The MSP enrollee information that is collected is submitted directly by enrollees through email, telephone, or fax and then entered in the MSP External Review electronic database by the OPM External Review team.

The business contact information contained in the Contact Account Management component was obtained by the OPM State Engagement and Analysis team through communications with State Departments of Insurance and State Exchanges.

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 project does not use information from commercial sources or publicly available data. However, the business contact information saved in the Contact Management system may be checked or verified through internet searches, specifically through State Departments of Insurance or State Exchange websites.

2.4. Discuss how accuracy of the data is ensured.

The OPM External Review team reviews the information in the electronic log where MSP enrollee information is saved and works closely with the enrollees to ensure that the details of their cases are accurately represented and captured. The OPM State Engagement and Analysis Team may check business contact information in the Contact Management component by verifying it against what is available on public websites.

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

Privacy Risk: There is a risk that information collected through the project is not accurate or correct.

Mitigation: This risk is mitigated by H&I personnel, who conduct reviews of the information submitted and work with enrollees, including comparing the information received from the enrollee with information received from the MSP Issuer, to ensure the accuracy of the information.

Privacy Risk: There is a risk that MSPPS collects more information than is required for the review.

Mitigation: This risk is mitigated by the project teams carefully considering what information they need to achieve their business purpose and only

requesting that information from the enrollees. This risk cannot be fully mitigated, however, because enrollees may send information that was not requested and that OPM does not need.

Section 3.0. Uses of the Information
3.1 Describe how and why the project uses the information.

OPM used the MSP Application Portal to review health insurance companies' information and then certify their plan(s)to be sold on HealthCare.gov. OPM also used the Portal to transmit plan information to the Department of Health & Human Services, the National Association of Insurance Commissioners, and States which run their own Exchanges. This transmittal was necessary for plans to be sold on HealthCare.gov.

OPM uses the information in the MSP External Review component to adjudicate appeals submitted by an MSP enrollee. If an MSP Issuer denies a claim or request for benefits coverage to an MSP enrollee, the enrollee has the right to request External Review to appeal the issuer's decision. OPM conducts external reviews of adverse benefit determinations subject to the standards and timeframes set forth in 45 CFR 147.136(d). An MSP Issuer must pay a claim or provide a health-related service or supply pursuant to OPM's final decision or the final decision of an independent review organization without delay, regardless of whether the plan or issuer intends to seek judicial review of the external review decision and unless or until there is a judicial decision otherwise.

The Contact Account Management system was used by the OPM State Engagement and Analysis team to manage communications with State Departments of Insurance and State Exchanges.

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 project does not use technology to conduct electronic searches, queries, or analysis to identify predictive patterns or anomalies.

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

Within OPM, only members of HI project teams with a need to know have access to the MSPPS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that OPM personnel who do not have a need to know the information in the system will be granted access.

Mitigation: This risk is mitigated through established Standard Operating Procedures and project plans that describe which personnel should be granted access and levels of access based on their roles and responsibilities.

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 defined user roles and access, which permit authorized users to only access information for which they have a need to know.

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.

MSP enrollees complete an intake form to request External Review. The form includes a Privacy Act statement that explains that their information will be used to determine eligibility for external review, to conduct the external review, to provide record of the external review, and for general management of the external review system. The Privacy Act statement also lists other possible routine uses of the enrollee's records.

No notice was provided to those whose business contact information is included in the Contact Account Management component, and it is assumed that State officials understand that their contact information is saved at OPM for the purpose of ongoing communications between OPM and State officials.

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

For MSP enrollees who request External Review, the Privacy Act statement states that providing information is voluntary but that MSP enrollees who

decline to provide information may not have their requests fully processed. Enrollees are also provided the opportunity to consent to authorize OPM to provide information to its contracted Independent Review Organization (IRO) and have the IRO conduct a medical review. The opt-in also allows the release of any appropriate medical records for use by OPM to conduct external review of a claim.

4.3. Privacy Impact Analysis: Related to Notice
Privacy Risk: There is a risk that individuals will not receive adequate notice concerning how their information will be used.

Mitigation: This risk is mitigated by providing MSP enrollees with a Privacy Act statement on their intake form, which clearly outlines why their information is being collected and how it will be used. OPM also provides a maintains an MSP Program web page and a Frequently Asked Questions web page to provide additional information to individuals.

Section 5.0. Data Retention by the Project
5.1. Explain how long and for what reason the information is retained.
OPM retains all MSP External Review records for 6 years in accordance with the NARA Records Schedule DAA-0478-2015-0001.

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 is mitigated by ensuring that staff adheres to the applicable records schedule and deletes information when required.

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.
When an MSP enrollee requests external review of their MSP Issuer's denial of a claim, OPM conducts independent review for contractual cases; but for medical judgment cases, OPM contracts with an IRO to provide a final, binding

decision. In medical judgment cases, OPM will share information in order for the IRO to make a decision.

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

Sharing information with the IRO is done in order to review an adverse benefit determination at the request of the enrollee, which is directly compatible with the purposes outlined in OPM/Central 19. The enrollee provides written consent, through an opt-in on the intake form, to permit OPM to share information with the IRO. However, in addition to that consent, sharing information with the IRO is permissible pursuant to routine use "a" in the SORN, which allows disclosure to contractors for the purpose of adjudicating the appeal.

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

Yes. The IRO, by contract, is only permitted to use the information that OPM provides to make the necessary medical determination and cannot re-disseminate the information for any other purpose.

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

The project saves and maintains records of any disclosures in an electronic log within the MSP External Review component.

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 through training project team members on the proper handling of the information in the system, including appropriate disclosures. In addition, the contract with the IRO clearly defines the purpose for which the medical information is being provided to the IRO.

Section 7.0. Redress

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

MSP enrollees may request access to any records related to their External Review case by writing to the U.S. Office of Personnel Management, FOIA/PA Requester Service Center, 1900 E Street, NW, Washington, D.C. 20415-7900. Individuals must furnish the following information when making their request: full name; date and place of birth; Social Security Number; signature; available information regarding the type of information requested, including the name of the MSP Issuer involved in any external review and the approximate date of the request for external review; the reason why the individual believes the system contains information about them; and the address to which the information may be sent.

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) and provide a notarized statement or unsworn declaration made in accordance with 28 U.S.C. § 1746.

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

If MSP enrollees submit inaccurate or erroneous information, they can resubmit their intake files and send in the new information, new health documentation, and/or previously omitted documentation.

In addition, individuals wishing to request amendment of records about them may write to the U.S. Office of Personnel Management, FOIA/PA Requester Service Center, 1900 E Street NW, Room 5415, Washington, DC 20415–7900. ATTN: Healthcare and Insurance, National Healthcare Operations. Individuals must furnish the following information in writing for their records to be located: full name; date and place of birth; Social Security Number; signature; and available information regarding the type of information that the individual seeks to have amended, including the name of the MSP issuer involved in any external review and the approximate date of the request for external review.

Individuals requesting access must comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297) and

provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. § 1746.

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

Individuals are informed about the procedures for correcting their information in interactions with the OPM External Review Staff, through the published OPM/Central 19 SORN, and this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that MSP enrollees will not know how to access and amend their records.

Mitigation: This risk is mitigated through OPM External Review staff providing notice to enrollees that they can amend their information, as necessary, and by publication of the OPM/Central 19 SORN and this PIA.

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?

OPM maintains Standard Operating Procedures around the collection and maintenance of the information, and all OPM staff working on the MSPPS complete IT security and privacy training on an annual basis.

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 training on an annual basis. OPM External Review staff also take additional training specific to the project, including topics such as general customer service, information handling procedures, and sensitivity of information.

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 a web-based tool for the project that allows for administrator provided account and role management. The tool allows account managers within the system the ability to create and modify user accounts.

Additionally, these same account management users have the ability to assign system roles to accounts.

The tool is a password restricted subcomponent that requires given roles to access functionality. It also allows for account management administration of user accounts, including locking or unlocking accounts, enabling or disabling accounts, resetting passwords, email addresses, or other user account information, and adding or removing roles from individual accounts.

All actions within the tool are fully logged with a date and time of action, data changed with recorded history, and the user responsible for the change. This includes creation of or updates to user accounts, addition of or removal from roles, and any emails triggered by the system through new account creation, password reset, or account unlock actions.

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?

At the beginning of every project, the OPM project team reviews potential situations or arrangements that could require information sharing, new uses of the information, and/or new access by other organizations. The project team works with the appropriate offices within OPM to execute the most appropriate plan or strategy depending on the situation.

Responsible Official

Laurie Bodenheimer
Acting Director, Healthcare & Insurance

Approval Signature

Signed copy on file with the Chief Privacy Officer

_____
Kellie Cosgrove Riley
Chief Privacy Officer