Privacy Impact Assessment
for the

Multi State Plan Portal System (MSPPS)

August 7, 2017

Contact Points

Ellen Heier
Healthcare & Insurance
National Healthcare Operations

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The purpose of the Multi-State Plan Program System (MSPPS) is to assist the Office of Personnel Management's Healthcare & Insurance in managing its responsibilities for the Multi-State Plan (MSP) Program as authorized by the Patient Protection and Affordable Care Act. Under the MSP Program, the Office of Personnel Management contracts with private health insurance companies to offer health insurance on the Health Insurance Marketplace. A consumer who purchases an MSP option is known as an MSP enrollee. The Privacy Impact Assessment (PIA) is being conducted because the MSPPS collects personally identifiable information from MSP enrollees.

Overview

The Office of Personnel Management's (OPM) Healthcare & Insurance is organized into two groups – Federal Employee Insurance Operations (FEIO) and National Healthcare Operations (NHO). FEIO is responsible for government-wide administration of health benefits and insurance programs for Federal employees, retirees, and their families through the Federal Employees Health Benefits Program. NHO is responsible for implementing and overseeing the MSP Program, which was established under the Patient Protection and Affordable Care Act (ACA). In this role, NHO reviews applications and proposed rates and benefits plans from health insurance companies (MSP Issuers).

If they meet the requirements of the MSP Program and the ACA, OPM certifies the plans as MSP options and readies them for sale on HealthCare.gov. NHO is responsible for all functions related to the MSP Program, including MSP Issuer support, communications, and contracting; External Review (appeals for MSP enrollees); and engagement with State officials.

The MSPPS is a web-based, paperless suite of systems which support NHO's administration of the MSP Program. The systems collect a variety of information, including information submitted by health insurance companies interested in being an MSP Issuer, business contact information for State officials, and personally identifiable information (PII) for MSP enrollees related to the External Review process. There are three project components

(MSP Application Portal, External Review, and Contact Account Management), each of which collects different types of information.

1. OPM uses the MSP Application Portal to communicate with potential and existing MSP Issuers. The MSP Application Portal contains the electronic application that health insurance companies must complete to become an MSP Issuer. Through this application, insurance companies submit information about their company and their proposed offerings. OPM reviews the information and decides which MSP options to sell on HealthCare.gov.

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. The MSP enrollee submits a request for External Review. This includes completing an intake form that asks for enrollee information, including details about his/her medical case and other PII. 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 will then make 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.

To help mitigate potential risks related to improper disclosure or handling of MSP enrollee PII, OPM uses a variety of system security controls, including access and account management, annual IT security and privacy awareness training, auditing and audit review, and information systems back-ups.

Section 1. 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. A security plan is an artifact within the Authority to Operate (ATO). The ATO was granted on October 27, 2016, and continuous monitoring is ongoing.

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. Characterization of the Information

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

The MSP Application Portal contains information submitted by health insurance companies that are interested in and/or currently participating in the MSP Program. Information includes organizational information, proposed plan rates and benefits, accreditation information, level of coverage (bronze, silver, gold, or platinum), service area, and status (OPM's approval and certification status). OPM staff uses this information to determine whether MSP Issuers meet the requirements of the MSP Program and the ACA to participate.

The MSP Program External Review component tracks and maintains MSP enrollee information. When an MSP enrollee contacts OPM to request external review, he/she provides information which is entered into the External Review system by OPM's External Review team. Enrollee information includes PII such as member name, address, identification number, date of birth, claim number, provider's name address, procedure codes, services rendered, diagnosis, and denial information. In addition, specifics 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. The system assists the MSP Program in managing its State government agency communications in a paperless environment. The information is collected by OPM State Engagement and Analysis staff and reviewed regularly to ensure that the information is current and up-to-date.

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 is submitted directly by health insurance companies that are interested in or are currently participating 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 is 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 Issuer Support team reviews information submitted by health insurance companies and checks it for compliance with the requirements of the ACA. The OPM External Review team reviews the information in the electronic log where MSP enrollee information is saved and works closely with the enrollee to ensure that the details of his/her case 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 the OPM Issuer Support, State Engagement and Analysis, and External Review teams, which 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. Uses of the Information

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

OPM uses the MSP Application Portal to review health insurance companies' information and then certify their plan(s), which can then be sold on HealthCare.gov. OPM also uses 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 is necessary for plans to be sold on HealthCare.gov.

OPM uses 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 is 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/offices with assigned roles and responsibilities within the system?

Within OPM, only the NHO project teams responsible for the three components of the MSPPS have access to the system.

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

Privacy Risk	Mitigation
There is a risk that OPM personnel who do not have a need to know the information in the system will be granted access.	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.
There is a risk that authorized persons may access information in the system for an unauthorized use.	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. Notice

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

Health insurance companies signal their interest in applying to be an MSP Issuer by submitting a Notice of Intent to Apply to gain access to OPM's MSP Application Portal. A notice is not required since they proactively and voluntarily submit information in their application to become an MSP Issuer.

For the MSP External Review component, MSP enrollees complete an intake form to request External Review. The form includes a Privacy Act Statement, which states that provision of information is voluntary but that OPM would use the information 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.

In the Contact Account Management component, no notice is provided, and it is inherently assumed that State officials' contact information is saved at OPM due to 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 includes language that states that provision of information is voluntary, and enrollees are informed that they can opt out of providing any information. MSP enrollees who decline to provide information cannot fully participate in the project. Enrollees are also allowed to opt-in to authorize OPM and its contracted Independent Review Organization to 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 Program web page and a Frequently Asked Questions web page to provide additional information to individuals.

Section 5. 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: OPM retains all MSP External Review records for 6 years in accordance with the NARA Records Schedule DAA-0478-2015-0001.

Mitigation: This risk is mitigated by ensuring that staff adheres to the applicable records schedule and deletes expired information, when appropriate.

Section 6. 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 his/her 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 the enrollee submitted in order for the IRO to make a decision. This potential sharing of information is stated in the External Review intake form.

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. Redress

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

MSP enrollees may access their own health information directly from their insurance company. 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 an MSP enrollee submits inaccurate or erroneous information, he/she can resubmit his/her 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

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. Auditing and Accountability

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

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.

Responsible Officials

Alan Spielman
Director, Healthcare & Insurance
Office of Personnel Management

Approval Signature

Kellie Cosgrove Riley
Chief Privacy Officer