OPM/Central-19, External Review Records for Multi-State Plan (MSP) Program

78 FR 65011 (10/30/2013), 87 FR 5874 (2/2/2022)

This unofficial consolidation of OPM/Central-19 is from the U.S. Office of Personnel Management Privacy Website at https://www.opm.gov/privacy.

SYSTEM LOCATION:
Office of Personnel Management, 1900 E Street NW., Washington, DC 20415.

SYSTEM MANAGER(S):
The system manager is Edward M. DeHarde, U.S. Office of Personnel Management, Healthcare and Insurance, 1900 E Street NW., Room 2347, Washington, DC 20415.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
This system will contain records on MSP enrollees who request external review of adverse benefit determinations, and MSP enrollees who contact OPM about an inquiry or complaint.

CATEGORIES OF RECORDS IN THE SYSTEM:
In order to process a request for external review, OPM may require an MSP enrollee or an authorized representative to submit the following information about the enrollee, which OPM may also collect, as necessary, to process enrollee inquiries and complaints:

a. The adverse benefit determination that the individual received from the MSP issuer.
b. Name.
c. Date of birth.
d. Gender.
e. Social Security Number.
f. Phone number(s), postal address(es) (current and mailing), and email address(es).
g. Insurance identification (ID) number.
h. Group number.
i. Scanned copy of insurance ID card.
j. The State and county of coverage.
k. An indication of whether the external review request is for an urgent claim.
l. A brief statement of the reason for the external review request.
m. The MSP issuer's name.
n. The name of the MSP option that covers the MSP enrollee.
o. The claim number.
p. Subscriber's information: Name, Social Security Number, date of birth, gender, phone number(s), postal address(es) (current and mailing), and email address(es).
q. In cases where an authorized representative requests external review, evidence of authorization and the following information about the authorized representative: name, phone number(s), postal address(es) (current and mailing), and email address(es).
r. Name of health care provider.
s. Health care provider address(es).
t. Any additional information necessary to process the request for external review.

In addition, MSP enrollees may choose to submit additional information that will become part of the system of records. This information may include, but is not limited to, the following:

a. A statement about why the MSP enrollee believes the MSP issuer's adverse benefit determination was wrong, based on specific benefit provisions in the plan brochure, contract, or statement of benefits.
b. Copies of documents that support the request for external review, such as physicians' letters, operative reports, bills, medical records, and explanation of benefits (EOB) forms.
c. Copies of all letters the MSP enrollee sent to the MSP issuer about the claim.
d. Copies of all letters the MSP issuer sent to the MSP enrollee about the claim.

MSP issuers will provide additional information and documentation. Consequently, the records in the system may include the following information about the MSP enrollee:

a. Personal identifying information (name, Social Security Number, date of birth, gender, phone number, etc.).
b. Postal address(es) (current and mailing).
c. Dependent information (spouse, dependents and their addresses).
d. Employment information.
e. Health care provider information.
f. Health care coverage information.
g. Health care procedure information.
h. Health care diagnoses information.
i. Provider charges and reimbursement information on coverage, procedures and diagnoses.
j. Any other letters or other documents submitted in connection with the adverse benefit determination by MSP enrollees, health care providers, or MSP issuers.

The aforementioned information may also be collected, as necessary, to process MSP enrollee inquiries and complaints.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
OPM has authority to administer the MSP Program under section 1334 of the Affordable Care Act (42 U.S.C. 18054).

PURPOSE(S) OF THE SYSTEM:
OPM operates this system of records to support the administration of the MSP Program. The primary purpose of this system of records is to aid in the administration of external review of adverse benefit determinations for MSP enrollees. OPM must have the capacity to collect, manage, and access health insurance benefits appeals information and documents on an ongoing basis in order for OPM to:

a. Determine eligibility for the MSP Program external review process.
b. Review adverse benefit determinations by MSP issuers to provide effective external review.
c. Track the progress of individual requests for external review and ensure that MSP enrollees do not submit duplicative requests.
d. Make information available for any subsequent litigation related to a disputed external review decision.
e. Monitor whether MSP issuers are providing benefits to which MSP enrollees are entitled under the terms of the applicable MSP Program contract.
f. Maintain records for parties to the dispute so that the MSP enrollee and MSP issuer can obtain a record of past external reviews in which they were involved.
g. Track and report information about the administration of the MSP Program.
h. Refer MSP enrollees to appropriate entities about their inquiries or complaints.
i. Correspond with MSP enrollees.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures otherwise permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system may be disclosed outside of OPM, for a routine use under 5 U.S.C. 552a(b)(3) as follows:

1. For Claims Adjudication—To disclose information to agency contractors conducting claim reviews for the purpose of adjudicating an appeal.
2. For Law Enforcement Purposes—To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where OPM becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
3. For Congressional Inquiry—To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of that individual.
4. For Judicial/Administrative Proceedings—To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding. In those cases where the Government is not a party to the processing, records may be disclosed if a subpoena has been signed by a judge.
5. For the National Archives and Records Administration or the General Services Administration—To disclose information to the National Archives and Records Administration (NARA) or General Services Administration for use in records management inspections conducted pursuant to 44 U.S.C. 2904 and 2906.
6. For Litigation—To disclose to the Department of Justice or in a proceeding before a court, adjudicative body, or other administrative body before which OPM is authorized to appear, when—
    (1) OPM, or any component thereof; or
    (2) Any employee of OPM in his or her official capacity; or
    (3) Any employee of OPM in his or her individual capacity where the Department of Justice or OPM has agreed to represent the employee; or
    (4) The United States, when OPM determines that litigation is likely to affect OPM or any of its components—

    is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or OPM is deemed by OPM to be relevant and necessary to the litigation, provided, however, that the disclosure is compatible with the purpose for which records were collected.
7. For Non-Federal Personnel—To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government, where the disclosure is compatible with the purpose for which records are collected.
8. In the Event of a Data Breach—In the event of a data breach, records may be disclosed to appropriate Federal agencies and agency contractors that have a need to know the information for the purpose of assisting the agency's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.
9. To researchers inside and outside the Federal Government, approved in advance by OPM on the basis of demonstrated aptitude and a written research plan, for the purpose of conducting

analysis of health care and health insurance trends and topical health-related issues compatible with the purposes for which the records were collected and formulating health care program changes and enhancements to limit cost growth, improve outcomes, increase accountability, and improve efficiency in program administration. In all cases, researchers external to OPM will access a public use file that will be maintained for such purposes; will contain only de-identified data; and will be structured, where appropriate, to protect MSP enrollee confidentiality where identities may be discerned because there are fewer records under certain demographic or other variables. In all disclosures to analysts under this routine use, only de-identified data will be disclosed.

10. If OPM determines that jurisdiction over an MSP enrollee's inquiry or complaint lies with another Federal or State agency, information in this system of records may be disclosed to other agencies, such as a State insurance department, a State Consumer Assistance Program, or the U.S. Department of Health and Human Services.

- To appropriate agencies, entities and persons when (1) OPM suspects or has confirmed that there has been a breach of the system of records, (2) OPM has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, OPM (including its information systems, programs and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with OPM's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- To another Federal agency or Federal entity, when OPM determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:
Paper records will be maintained in locked file cabinets within OPM and/or any contractors. Any electronic records will be maintained in electronic systems.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:
Records will primarily be manipulated, managed and summarized using a unique number assigned to each external review or case about an inquiry or complaint. However, information may also be accessible by other identifying information, including name, date of birth, or Social Security Number.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:
OPM will maintain records within its secure headquarters in Washington, DC. Electronic records will be maintained on password-protected computers and systems. Computer firewalls will be maintained to prevent access by unauthorized personnel. Any paper records will be delivered to a locked P.O. Box and kept in locked file cabinets.

Federal employees and employees of Federal contractors are required to have been the subject of a favorable adjudication following an appropriate background investigation before they are allowed physical access to OPM and access to any records. OPM's environment is equipped with electronic badge readers restricting access to authorized personnel only and has safeguards in place to alert security personnel if unauthorized personnel attempt to gain access to OPM's environment. OPM

employs armed physical security guards 365 days a year, 24 hours a day, who patrol OPM headquarters, including entry and exit points. Closed Circuit Video cameras are strategically located on every floor and external to the facility.

The system will employ National Institute of Standards and Technology (NIST) Security Controls identified in the most recent version of Special Publication SP 800-53. NIST 800-53 security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. OPM will perform a Security Assessment and Authorization (SA&A) following the NIST 800-53 standard in order to obtain an Authority to Operate (ATO). The system will employ role-based access controls to further restrict access to data, based on the functions that users are authorized to perform. The system will be fully compliant with all applicable provisions of the Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Federal Records Act, Office of Management and Budget (OMB) guidance, and NIST guidance.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
The records in this system will be retained for at least 6 years. Records may be retained for a longer period for the system purposes established in this system of records notice, or for other purposes as required under law (e.g., for purposes of litigation). A records retention schedule will be established with NARA, and no records will be destroyed until that schedule has been established. Once that schedule is established, it will set forth methods for disposing records that would no longer be eligible for retention.

NOTIFICATION AND RECORD ACCESS PROCEDURES:
Individuals wishing to determine whether this system of records contains information about them may do so by writing to the U.S. Office of Personnel Management, FOIA/PA Requester Service Center, 1900 E Street NW., Room 5415, Washington, DC 20415-7900 or by emailing foia@opm.gov.

Individuals must furnish the following information for their records to be located:

1. Full name.
2. Date and place of birth.
3. Social Security Number.
4. Signature.
5. 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.
6. The reason why the individual believes this system contains information about him/her.
7. The address to which the information should be sent.

Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297). In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

- If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on [date]. [Signature].”

- If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on [date]. [Signature]."

CONTESTING RECORD PROCEDURES:
Individuals wishing to request amendment of records about them should 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:

1. Full name.
2. Date and place of birth.
3. Social Security Number.
4. Signature.
5. 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 also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297). In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

- If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on [date]. [Signature]."
- If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on [date]. [Signature]."

RECORD SOURCE CATEGORIES:
Information in this system of records is obtained from:

a. MSP enrollees who request external review, or who contact OPM about an inquiry or complaint.
b. Authorized representatives of MSP enrollees.
c. Health care providers.
d. MSP issuers.
e. Medical professionals providing expert medical review under contract with OPM.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.