OPM/Central-18, Federal Employees Health Benefits Program Claims Data Warehouse.

76 FR 35052 (6/15/2011), *Prefatory Statement of Routine Uses*, 87 FR 5874 (2/2/2022)

This unofficial consolidation of OPM/Central-18 is from the U.S. Office of Personnel Management Privacy Website at https://www.opm.gov/privacy.

SYSTEM LOCATION:
Office of the Inspector General, U.S. Office of Personnel Management, 1900 E Street, NW., Washington, DC 20415.

SYSTEM MANAGER(S):
The system manager is the Chief, Information Systems Audit Group, Office of the Inspector General, 1900 E Street, NW., Room 6400, Washington, DC 20415-1100.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
This system contains claims records on the Federal Employees Health Benefits Program (FEHBP). Participation in these programs is voluntary.

Participants in the FEHBP include Federal employees, Postal employees, annuitants under the Civil Service Retirement System and the Federal Employees Retirement System, former spouses, and their family members. Health care providers that submit claims to the FEHBP plans will also be stored in the system as part of the claims records. The Office of the Inspector General (OIG) has oversight responsibility under the Inspector General Act over the FEHBP.

CATEGORIES OF RECORDS IN THE SYSTEM:
The records in the system may contain the following types of information on participating enrollees and covered dependents:

a. Personally identifiable Information (PII) (Name, Social Security Number, Date of Birth, Gender, and FEHBP Member ID number).
b. Home Address.
c. Covered dependent information (Spouse, Dependents)—names and genders.
d. Enrollee's employing agency.
e. Names of health care providers including health care providers debarred under 5 U.S.C. 8902a.
f. Health care provider address.
g. Health Care Provider Taxpayer Identification Number (TIN) or identifier issued by a carrier.
h. Health care coverage information regarding benefit coverage for the plan in which the person is enrolled.
i. Health care procedure information regarding procedures performed on the individual.
j. Health care diagnoses in the form of ICD codes, and treatments, including prescribed drugs, derived from clinical medical records.
k. Provider charges, including amounts paid by the plan and amounts paid by the enrollee for the above coverage, procedures, and diagnoses.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
The OIG is authorized to maintain FEHBP health claims information under § 6(a) of the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 6(a). Authority is provided to OPM for maintenance of FEHBP health claims information by 5 U.S.C. 8910; 45 CFR 164.501, 164.512(d), which allow OPM

access to records held by FEHBP contractors and require these contractors to submit reports on services provided to enrollees.

PURPOSE(S) OF THE SYSTEM:
The primary purpose of this system of records is to provide a central database from which the OIG may use claims data from carriers for audit and investigative purposes to meet its oversight obligations under the Inspector General Act of 1978, as amended, 5 U.S.C. App., to detect fraud, waste and abuse in OPM programs. The Office of the Inspector General will use the data to detect and pursue fraud in the FEHBP and to audit the contracts with the various FEHBP carriers.

The secondary purpose of this system of records is to provide a mirror image of the Federal Employees Health Benefits Program Claims Data Warehouse data feeds to OPM so it can establish a central database (OPM/Central-15) from which it may analyze FEHBP data and actively manage the FEHBP to ensure the best value for the enrollees and taxpayers. OPM will collect, manage, and analyze health services data provided by FEHBP carriers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:
Only routine uses 1, 7, and 11 of the Prefatory Statement at the beginning of OPM's current Systems of Record notice apply to the records maintained within this system.

1. 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.
7. For Litigation—To disclose information 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.
11. 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.

The routine uses listed below are specific to this system of records only:
1. 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.
2. To disclose information to the contractor that originally provided the data to audit health care claims or investigate fraud.

- 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:
These records will be maintained in electronic systems.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:
These records are retrieved by various means:

1. Name, address, and/or social security number of an individual enrollee or patient,
2. Name, address, and/or TIN or other identifier of health care providers,
3. Claim payment information, and
4. Diagnostic or other procedure codes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:
The system will be located within space controlled by the OIG in OPM Headquarters. All employees and contractors are required to have an appropriate background investigation before they are allowed physical access to OIG office spaces and access to the system. The system is in a secured space that is equipped with a two factor authorization device, restricting access to authorized personnel only and has alarms to alert security personnel if unauthorized access is attempted. OPM employs armed physical security guards 365 days a year, 24 hours a day that patrol OPM Headquarters, to include every entry/exit point. Closed Circuit Video cameras are strategically located on every floor and external to the facility. Multiple layers of computer firewalls are maintained to prevent access by unauthorized personnel. The system employs National Institute of Standards and Technology (NIST) technical, physical and environmental Security Controls identified in Special Publication (SP) 800-53 revision 3. The OIG will perform an Assessment and Authorization following the NIST 800-53 revision 3 standard in order to obtain an Authority to Operate (ATO). The OIG will operate the system in compliance with the Privacy Act, Federal Information Security Management Act (FISMA) and NIST guidance. Transmission of the data feed from the carriers to this system is encrypted in compliance with NIST Federal Information Processing Standards Publication 197.

The OPM Health Claims Data Warehouse is hosted on the OIG IT systems, however the operation of, maintenance of, and security of the OPM Health Claims Data Warehouse is the responsibility of OPM not the OIG. Notice to the public of the OPM Health Claims Data Warehouse system of records is contained in a separate System of Records Notice.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system will be retained for at least 7 years but may be maintained for a longer period as required by litigation or open investigations or audits. Computer records are destroyed by electronic erasure. A records retention schedule is being established with the National Archives and Records Administration (NARA).

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 e-mailing 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.
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 297).

CONTESTING RECORD PROCEDURES:
Individuals wishing to request amendment of records about them should write to the Office of Personnel Management, FOIA/PA Requester Service Center, 1900 E Street, NW., Room 5415, Washington, DC 20415-7900. Attn: Office of Inspector General.

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. City, state, and zip code of their Federal Agency.
5. Signature.
6. Precise identification of the information to be amended.

Individuals requesting amendment must also follow OPM's Privacy Act regulations regarding verification of identity and amendment to records (5 CFR 297).

RECORD SOURCE CATEGORIES:
Information in this system of records is obtained from health care insurers contracted by the U.S. Office of Personnel Management as FEHBP carriers.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.