

## Attachment 2

### **Mandatory Information Sharing via Written Case Notifications and Referrals to OPM-OIG**

FEHBP Carriers are required to submit a written notification to OPM-OIG within 30 working days when there is a potential reportable FWA that has occurred against the FEHB Program. OPM-OIG considers a potential reportable FWA as, after a preliminary review of the complaint, the carrier takes an affirmative step to investigate the complaint. Case Notifications sent to OPM-OIG should include the identification of emerging fraud schemes; internal fraud, waste, or abuse by Carrier employees, contractors, or subcontractors; fraud by providers who supply goods or services to FEHBP members; fraud by individual FEHBP members; issues of patient harm, and Carrier participation in class action lawsuits. There is no financial threshold for these case notifications.

Please ensure that all evidence obtained related to FEHB FWA matters including, but not limited to, checks issued in payment of claims, hard copy claims, explanation of benefits, investigative notes, emails, taped statements, written statements, original receipts, customer service call sheets, and original documents submitted in support of or in opposition to a claim submitted for reimbursement by a provider, member, or third party, are identified, collected, and preserved in order to be turned over to OPM-OIG or any law enforcement agency requesting such information or in connection with a referral of cases to OPM-OIG or other law enforcement agencies

The format for case notifications and status updates can be found in **Attachment 3**.

Written notifications are generally expected to include (but are not limited to) the following information:

- 1) Complete identification on file for the health care provider(s) or FEHB enrollee(s), including but not limited to full name(s), business name(s), address(es), telephone number(s), date(s) of birth, social security number(s) (if available), enrollee/member number(s), tax identification number(s), and universal provider identification number(s);
- 2) A comprehensive written description of the nature of the suspected FWA;
- 3) A written summary of the evidence the Carrier has reviewed which caused the Carrier to suspect FWA occurred;
- 4) A written analysis of any suspected fraudulent claims pattern, specific CPT, ICD-10, and other types of codes utilized in the scheme (ex: of 1900 Billed services, 800 of them were not performed equating to 42% of the claims being false);
- 5) How the case was identified (ex: internal source such as customer service, medical review staff, pre-certification, proactive computer software usage/analysis, etc., or external source such as enrollee complaint, anonymous letter, Federal Bureau of Investigation, National Health Care Anti-Fraud Association (NHCAA), Law Enforcement Requests for Investigative Assistance (RIAs), Subpoena, etc.);
- 6) Total FEHB Program Billed and Paid Amount for a Four Year Time Period (Summary Exposure, not detailed claim information) ;
- 7) Fraud Type Indicator: Examples include but are not limited to Billing for Services Not Rendered, Ineligible Spouse, Up coding, Unbundling, Misrepresentation of Services, Medically

- Unnecessary Services, Stolen Health Benefit Card, Forged Prescription, False Application (SF-2809), False Diagnosis, Waiver of Co-pay, Altered Prescription, Identity Theft, Other;
- 8) Provider Type Indicator: An identification to include but not limited to Ambulance, Billing Company, Chiropractor, Dentist, Doctor Shopper, DME, Home Health, Hospital, Laboratory, Member, Nursing Home, Nurse Practitioner, Outpatient Surgery Center, Pharmacy, Physical Therapy, Physician, Physician Asst., Psychiatric, Other;
  - 9) If a provider, whether the provider is an In-Network/Participating or Non-Network/Non-Participating Provider;
  - 10) If FEHB Program Enrollee(s)/Member(s) or dependent(s), the Carrier should provide the member's employer information and/or a Copy of the members SF-2809 Health Benefit Election Form;
  - 11) Carrier Contact Information for specific Special Investigative Unit (SIU) or other Carrier personnel responsible for notification;
  - 12) Any specific knowledge of patient harm that could be a result of the suspect activity
  - 13) If necessary, Contact information for the Federal and/or State law enforcement/oversight agency, investigator, and/or attorney the Carrier is coordinating its investigation; and
  - 14) If the plan has provided a referral to another law enforcement/oversight agency, the referral is to be included and made available with the case notification to OPM/OIG.

### **OPM-OIG Response to Case Notifications**

Upon receipt of a case notification, OPM-OIG will review to determine if it is appropriate for OPM-OIG to share information from the case notification with other FEHBP Carriers potentially affected by the suspected fraud. OPM-OIG shall also provide the Carrier generating the notification with a written reply indicating OPM-OIG's level of interest in the case.

In the OPM-OIG reply, they may:

- 1) Referral Accepted/Case Notification: See Additional Comments Below.
- 2) Request a Referral: OPM-OIG may request that the Carrier submit a case referral if OPM-OIG has a strong interest in the case based on the limited amount of information contained in the notification.
- 3) Monitor: OPM-OIG may request that the Carrier continue to investigate and provide OPM-OIG with a Status Update when the Carrier has more information available to substantiate or refute the allegation. Upon receipt of a Status Update, OPM-OIG may request the SIU to provide a referral, continue to investigate/monitor, or decline the case.
- 4) Decline: If the case is not of interest to OPM-OIG, OPM-OIG will advise the Carrier that OPM-OIG does not intend to investigate, absent the development of significant new information. The Carrier may proceed with its investigation and no further communication with OPM-OIG about the case is required, unless a triggering event occurs which warrants a Status Update. Triggering events are:
  - a. If the Carrier develops significant new information and believes OPM-OIG should reconsider the declination, the Carrier shall submit a Status Update that provides a brief summary of the new information;
  - b. If a case declined by OPM-OIG is subsequently accepted for investigation by another

Federal, state and/or local law enforcement agency, the Carrier shall submit a Status Update to OPM-OIG advising OPM-OIG of the identity of the investigating law enforcement agency;

- c. If a case declined by OPM-OIG is subsequently accepted for prosecution at the Federal level, such as by a United States Attorney's Office or U.S. Department of Justice.

OPM-OIG will provide a written response to the notifying Carrier Special Investigations Unit within 30 to 60 days of the receipt of a notification. During the time the carrier is waiting for an OIG response, the carrier should continue developing and investigating the allegations and continue to report updated findings.

### **Status Updates: Information Sharing After Initial Case Notification**

To further facilitate information sharing between the Carriers and OPM-OIG, in certain instances specifically defined below, Carriers shall provide OPM- OIG with Status Updates on cases that OPM-OIG is monitoring. The Status Updates shall:

- 1) Be in writing;
- 2) Follow the same general format as the initial notification;
- 3) Clearly indicate that it is a status update rather than an initial notification;
- 4) Provide a brief summary of new information; and
- 5) Be sent to either the assigned agent or reviewing supervisor as indicated in the OPM-OIG response.

While OPM-OIG is monitoring a case, the Carrier shall submit a Status Update to OPM-OIG in the following instances:

- 1) The Carrier develops significant new information that the Carrier believes would aid OPM-OIG in determining whether to request a referral or decline the case;
- 2) The Carrier determines that the allegations have no merit and/or no false or fraudulent activity took place as alleged;
- 3) OPM-OIG specifically requests a Status Update;
- 4) The Carrier closes their investigation or inquiry;
- 5) The Carrier wishes to proceed with administrative debt collection, recovery or settlement of an FEHBP overpayment in reference to below section "Notification of Carrier Settlement Agreements."

### **Referral Process**

When OPM-OIG requests a referral based on a case notification or status update, the Carrier shall submit a written referral as defined below within 90 days of OPM-OIG's request for referral.

If the Carrier is unable to provide the full referral as described below within 90 days, the carrier is required to provide monthly Status Updates in writing beginning on day 91. The Status Updates shall indicate not only the current status of the case, but shall also provide OPM-OIG with an estimated date on which OPM-OIG will receive the full referral.

If at any point after OPM-OIG has requested a referral the Carrier determines the allegation(s) have no merit and/or no false or fraudulent activity took place as alleged, in lieu of the requested referral the Carrier shall promptly provide the OIG with a Status Update explaining the final conclusion/disposition of the allegation(s).

Referrals to OPM-OIG must be in writing and shall include, but are not limited to, the following:

- 1) Complete Identification on file for the suspected health care provider(s) or enrollee(s), including but not limited to name(s), business name(s), address(es), telephone number(s), dates of birth, social security number(s) if available, enrollee/member number(s) and a copy of the member SF-2809 form, tax identification number(s), Participating Network/Non-Participating Non-Network Provider status, and universal provider identification number(s);
- 2) A comprehensive written description of the nature of the suspected FWA;
- 3) A written summary of the evidence the Carrier has reviewed which has caused the Carrier to suspect FWA has occurred;
- 4) A written analysis of any suspected fraudulent claims pattern, specific CPT, ICD-10, and other types of codes utilized in the scheme (i.e., of 1900 Billed services, 800 of them were not performed equating to 42% of the claims being false);
- 5) How the case was identified (i.e., internal source such as customer service, medical review staff, pre-certification, proactive computer software usage/analysis, etc., or external source such as enrollee complaint, anonymous letter, FBI, NHCAA, etc.);
- 6) At least three examples of suspected false claims to include copies of the hard copy submitted claim(s), explanation of benefits, and copies of the front and back of any issued check for payment to the suspect provider;
- 7) A Copy of any Carrier specific medical policy statements that guides the Carrier in processing claims related to the suspected fraudulent or misrepresented claims submitted by the subject provider;
- 8) A four year claims history for the provider or enrollee in electronic format using the "Standard OIG Format";
- 9) Copies of any and all relevant or supporting documents obtained or produced by the Carrier or the Carrier's SIU during the preliminary investigation (i.e., internal provider audits, medical review findings, Carrier cease and desist letters, medical records, provider applications, network provider agreements, provider relations rep contacts, customer service records of contact, patient surveys, interview reports, Reports of Investigation, etc.);
- 10) Any and all research performed, including any background information obtained via investigative databases, information found on the internet, and/or other medical procedure research performed;
- 11) Any and all suspected State and Federal laws researched and believe the suspect activities have violated;
- 12) Any specific knowledge of patient harm that could be a result of the suspect activity;
- 13) Contact information for the Carrier personnel or SIU investigator responsible for preparing the referral; and,
- 14) If necessary, Contact information for the Federal and/or State law enforcement/oversight agency, investigator, and/or attorney the Carrier is coordinating its investigation with.

## **Carrier Settlement Agreements**

Reference is made to the provisions in this letter concerning Mandatory Information Sharing via Written Case Notifications to OPM-OIG, specifically the requirement to notify OPM-OIG of all cases where potential reportable FWA has occurred. No case involving recovery of FEHBP overpayments which result from apparent or suspected false, fictitious, fraudulent, or misleading claims should reach the settlement stage without prior communication with OPM-OIG regarding the allegations.

In cases where OPM-OIG has requested a referral from the Carrier and/or has advised the Carrier that OPM-OIG has an open investigation, the Carrier may not enter into a Settlement Agreement for the recovery of FEHBP funds without communicating with and obtaining authorization from OPM-OIG.

In cases where OPM-OIG has advised a Carrier that OPM-OIG is monitoring the allegations, prior to recovering FEHBP funds, the Carrier shall send OPM-OIG a Status Update to advise OPM-OIG of the Carrier's intent to proceed with a settlement agreement, or any other form of debt collection or recovery.

In cases that OPM-OIG has declined, the Carrier may proceed with any resolution the Carrier deems appropriate, to include pursuit of a settlement agreement. The Carrier is reminded to report any such recoveries to OPM on their annual Fraud, Waste, and Abuse Reports.

When a Carrier (as a sole participant<sup>1</sup>) resolves claims with any type of health care services provider or manufacturer for recovery of overpayments which resulted from apparent or suspected false, fictitious, fraudulent, or misleading claims submitted to the Carrier AND at least \$20,000 of the identified overpayments is money paid through the FEHB program, then the Carrier must:

1. include the language listed below in the settlement agreement, AND
2. not include a confidentiality clause in the settlement agreement which restricts the Government's access to the agreement,

Language for the settlement agreement: *"This settlement agreement in no way waives the rights of the United States Government under any Federal statute to pursue civil and/or criminal fines, penalties, recoveries, etc., for claims submitted to the carrier under the Federal Employees Health Benefits (FEHB) Program."* The requirement to include specific language in settlement agreements does not apply to Class Action Lawsuits, because the Carrier is not the "sole participant" in such litigation.

If a Carrier enters into negotiations with a provider such as those described above and there were monies identified paid through the FEHB Program, but the FEHB Program overpayments were excluded from the final settlement agreement for any reason, the Carrier must send notification to the OPM-OIG without delay.

---

<sup>1</sup> The requirement to include specific language in settlement agreements does not apply to Class Action Lawsuits, because the Carrier is not the "sole participant" in such litigation.

## **Response to OPM-OIG Requests for Information**

Upon request, all Carriers must furnish the OPM-OIG Office of Investigations with FEHB Program claims information and supporting documentation relevant to open criminal, civil, or administrative investigations.

Special Agents and/or Analysts of the OPM-OIG will make initial requests for claims information on the “OPM/OIG Exposure Data Request Form” (Attachment 4).

- 1) In response to exposure requests, Carriers must furnish a claims history via electronic media for the subject of the exposure request. The scope of the claims history required will be specified by OPM-OIG Special Agent on the exposure request.
- 2) Absent extenuating circumstances, carriers are expected to furnish requested data within 30 calendar days.
- 3) Unless directed otherwise, Carriers must comply with the standard data format established by OPM-OIG. A list of the specific data fields required is attached.
- 4) Any spreadsheets or documents containing sensitive or proprietary data forwarded to OPM-OIG by the Carrier via email must be encrypted.
- 5) Any sensitive or proprietary data sent via mail or delivery service should, at a minimum, be password protected.
- 6) Any request from OPM-OIG marked “Confidential” or similar language, **MUST NOT BE SHARED** with Private Lines of Business, Local Plans, or the Public. Contact the OIG Agent/Analyst directly before engaging in any investigative activities.

During the course of investigation, OPM-OIG Special Agents may require additional documentation from the Carrier (hard copy claims, checks, correspondence, etc.) and/or investigative support in the form of data analysis, prosecutorial witnesses, discovery documentation, medical expertise, provider applications/contracts, etc. An OPM-OIG Special Agent will contact the Carrier SIU investigator assigned to the initial exposure request when additional documentation or assistance is needed.

## **OPM-OIG Contact Information for Notifications:**

Please send all case notifications to: [OIGCaseNotifications@opm.gov](mailto:OIGCaseNotifications@opm.gov)

If you want to discuss any FWA guidance issue related to the enclosed guidelines please contact either:

Drew Grimm, Special Agent in Charge  
Office of Personnel Management – OIG  
Headquarter Operations  
Email: [Drew.Grimm@opm.gov](mailto:Drew.Grimm@opm.gov)

or

Scott A Rezendes, Special Agent in Charge  
Office of Personnel Management – OIG  
Field Operations  
Email: [Scott.Rezendes@opm.gov](mailto:Scott.Rezendes@opm.gov)