FEHB Program Carrier Letter
All FEHB Carriers

U.S. Office of Personnel Management
Healthcare and Insurance

Letter No. 2015-04 **Date: 03/23/2015**

Fee-for-Service [4] Experience-rated HMO [4] Community-rated [3]

SUBJECT: Notification of Data Breach

The purpose of this communication is to provide you with updated information concerning the importance of data security and notification to OPM.

Any breach of security in Federal Employees Health Benefits (FEHB) enrollee data is considered a significant event as defined in Section 1.10 Notice of Significant Events (FEHBAR 1652.222-70) of the FEHB Standard Contracts. This includes any breach of security in a carrier IT network that may potentially affect FEHB enrollee data. Although the contracts require notification of a significant event within 10 working days after the carrier becomes aware of it, due to privacy concerns and the potential impact on FEHB enrollees, we require notice to OPM immediately if you know or suspect that a breach has occurred. For any security breach or potential breach, immediate notification means that carriers will notify OPM within 30 minutes of becoming aware of the risk, regardless of the time or day of the week. This procedure is consistent with the provisions of the standard FEHB carrier contract applicable to reporting a Letter of Credit security breach. OPM has issued previous carrier letters on this topic – please reference Carrier Letter 2007-21, dated June 22, 2007 and Carrier Letter 2010-14, dated May 25, 2010.

A breach of data, system access, etc. includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of information whether physical or electronic. As an agency, OPM is required to immediately report all potential security and data breaches -- whether they involve paper documents or electronic information. In order to ensure FEHB carriers also comply with this requirement, we are issuing the following guidance.

FEHB carriers, by contract, must report any breach, suspected breach, or potential breach to OPM. We are updating our guidance to notify you that this report should be made to the **OPM Situation Room** and to the Contracting Officer immediately upon becoming aware of the risk. A suspected breach, potential breach or breach must be reported, even if it is believed the breach is limited, small, or insignificant. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail. Below are further instructions.

1. OPM carriers must report a breach, suspected breach, or potential security breach to the OPM Situation Room at: sitroom@opm.gov, (202) 418-0111, Fax (202) 606-0624.
2. When notifying the OPM Situation Room, please copy your Contracting Officer.

3. If you need assistance with WinZip, please contact the OPM Help Desk at: helpdesk@opm.gov, (202) 606-4927, TTY (202) 606-1295.
4. If you have questions regarding these procedures, please contact your Contracting Officer.

In addition, FEHB carriers, by contract, are required to cooperate with OPM's Office of the Inspector General (OIG) in their evaluation of your organizations' ability to protect the confidentiality, availability, and integrity of sensitive or mission-critical data. The OIG conducts independent evaluations to determine whether organizations have the controls in place to ensure its computer systems are securely configured and up-to-date. These evaluations involve the use of OIG hardware and/or software to conduct vulnerability scans and configuration compliance audits against a sample of the carrier's computer systems. The data obtained during the scans allows the auditors to form an opinion as to whether the organization has sufficient controls in place to protect sensitive or mission critical data. These evaluations are conducted in accordance with rules of engagement that provide assurance that the audit will not have a negative impact to the IT systems involved in the review. We expect all FEHB carriers to provide prompt and complete cooperation to allow the OIG to carry out its responsibilities in conducting its audits.

If you have any questions concerning the guidance in this Carrier Letter, please contact your Contracting Officer.

Sincerely,

John O'Brien
Director
Healthcare and Insurance