FEHB Program Carrier Letter
All Carriers

U.S. Office of Personnel Management
Insurance Operations

Letter No. 2010-14 **Date**: May 25, 2010

Fee-for-service [10] Experience-rated HMO [10] Community-rated HMO [10]

SUBJECT: Clarification of Data Breach Notification Requirements

On June 22, 2007, the Office of Personnel Management (OPM) issued Carrier Letter 2007-21, which provided notification requirements in the event of a breach of security in Federal Employees Health Benefits (FEHB) enrollee data. These requirements remain in effect.

On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule amending 45 CFR Parts 160 and 164 concerning notification of breaches of unsecured protected health information. FEHB Carriers must comply with this regulation in accordance with the Administrative Simplification-HIPAA clause of the standard contract (section 1.22 of the fee-for-service contract and section 1.21 of the HMO contracts.)

The HHS regulations require Health Insurance Portability and Accountability Act (HIPAA) covered entities to notify individuals when their **unsecured** protected health information is breached. Covered entities must notify affected individuals within 60 days of a breach, as well as the HHS Secretary and the media if a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. In addition, business associates of covered entities are required to notify the covered entity of breaches at or by the business associate. The rules also provide guidance concerning encryption standards for secured protected health information. For more information please see the Federal Register publication at 74 FR 42740-42770. However, these HHS regulations do not preclude you from also complying with OPM requirements.

Carrier Letter 2007-21 specifies that **any** breach in security in FEHB enrollee data is considered to be a significant event as defined in Section 1.10 Notice of Significant Events (FEHBAR 1652.222-70) of the standard contract. Carriers are still required to notify OPM in accordance with the significant events clause, **regardless of whether the breach is of secured or unsecured protected health information** as defined by the HHS rules.

You should continue to follow the requirements for notification in the case of any breach in security of FEHB enrollee data described in Carrier Letter 2007-21 (www.opm.gov/carrier/carrier_letters/2007/2007-21.pdf), as it includes **additional requirements beyond those contained in the HHS rules**. This includes requirements as to the content of the notice to enrollees and the time period required for notification.

We appreciate your cooperation in this matter. If you have any questions, please contact your Contract Specialist.

Sincerely,

Kathleen McGettigan
Acting Associate Director
for Retirement and Benefits