FEHB Program Carrier Letter

All FEHB Carriers

Letter No. 2017-14 **Date: December 8, 2017**

Fee-for-Service [10] Experience-rated HMO [10] Community-rated [13]

SUBJECT: Reports to OPM of Information Security Incident and Data Breach

This letter provides guidance regarding FEHB carriers' responsibility to report information security incidents (incidents) and data breaches to OPM. Federal Acquisition Regulations require that each FEHB Carrier must perform its contract in accordance with prudent business practices which include timely compliance with OPM instructions and directives.[1] Pursuant to the FEHB Act, each FEHB contract must contain provisions requiring Carriers to furnish such reasonable reports as OPM determines to be necessary to carry out its functions under the FEHB Program,[2] and OPM's FEHB contracts include reporting provisions including a statement that the Carrier shall furnish such reasonable reports as the Contracting Officer may request for carrying out OPM's functions under Chapter 89 of title 5. [3]

Based on inquiries regarding Carrier Letter 2015-04, OPM convened an Information Technology (IT) Security Carrier working group to discuss incident and data breach reporting requirements and develop FEHB Program Carrier security practices that are complete, sufficient, and uniform with regard to reporting. We appreciate the input that we received from participating Carriers, and believe the reporting requirements formulated in this Carrier Letter were improved by your input. We will continue the group going forward, we thank those Carriers that participated in the group thus far, and we encourage all FEHB carriers to participate in the future.

Our policy regarding reporting of incidents and data breaches for OPM-owned systems (including the Letter of Credit (LOC) Account system) remains unchanged. For any incident, breach, or potential incident or breach of the LOC Account or any other OPM-owned systems or systems that interface with them, Carriers must comply with the provisions of the standard FEHB Carrier contracts applicable to reporting an LOC incident or breach, including the requirement to report any suspected or actual breach within 30 minutes of becoming aware of the risk.

The following questions and answers clarify Carrier Letter 2015-04 and, where applicable, supersede it.

[1] 48 C.F.R. § 1609.7001
[2] 5 U.S.C. § 8910
[3] FEHB Contract § 1.7

Question 1: What type of incident or breach requires a Carrier or its agent to report to OPM?

A Carrier must report to OPM incidents and breaches where the confidentiality, integrity, or availability of FEHB member protected health information (PHI) is compromised or if a Carrier notifies law enforcement of an incident or breach that: (1) compromises its systems that contain or process FEHB Program data or (2) compromises its systems operating in the same general information technology control environment as the information systems that process FEHB Program data. Reporting requirements are clarified and more fully defined in this letter.

Question 2: How are the terms "incident," "breach," and "compromise" defined?

To define "incident" in this Carrier Letter, OPM uses and refers to the definitions set forth in 44 U.S.C. § 3552(b)(2) and applicable OMB guidance.

To define "breach," OPM uses and refers to the definition set forth in HHS regulations 45 CFR Part 164 Subpart D.

To define "compromise" OPM uses and refers to the glossary of the source document NIST SP 800-32 (2001) as incorporated into the NIST Glossary of Key Information Security Terms NISTIR 7298 Revision 2 (May 2013) available at http://dx.doi.org/10.6028/NIST.IR.7298r2.[4]

Question 3: To whom and in what timeframe does OPM want the Carrier to provide reports?

The Carrier must report to OPM via email to Cybersolutions@opm.gov or via phone to (844) 377-6109. Any data shared with OPM that relates to an incident or breach must be transmitted in a secure manner.

The Carrier must report to OPM as quickly as possible, but in no case later than 24 hours after its incident response team determines the confidentiality, integrity, or availability of FEHB member PHI is compromised, or it has notified law enforcement of an incident or breach that: (1) compromises its systems that contain or process FEHB data, or (2) compromises its systems operating in the same general information technology control environment as the information systems that process FEHB Program data, and before any other external notifications are made (excluding notification to necessary parties for incident response).

Carriers may also timely report, to the OPM Contracting Officer, incidents and breaches of systems that are outside the general information technology control environment of systems that contain or process FEHB data and, if possible, such report will be made prior to the first media notice. If a law enforcement agency requires confidentiality regarding a breach or incident involving FEHB data or systems containing FEHB data, notification to OPM that the Carrier is

[4] Compromise - Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

working with law enforcement must be shared with OPM within 24 hours of the initial notification to the law enforcement agency.

Incidents and breaches affecting subcontractors must be reported to OPM by the Carrier no later than the calendar day following notice to the Carrier.

Question 4: What information about the incident or breach does OPM want the Carrier to provide?

Provide to OPM (via Cybersolutions@opm.gov or (844) 377-6109):

1. A brief description of the nature of the incident or breach.
2. An estimate of the number of affected FEHB members, if feasible.
3. A brief description of the remedial steps that the Carrier has already taken and those they plan to take.

The Carrier is responsible for providing additional detailed information as soon as it becomes available.

Question 5: Will OPM hold these reports confidential?

OPM will, consistent with applicable law, hold reports confidential whenever law enforcement has required holding such reports confidential in order to protect the interests of its members. In addition, it is the Carrier's responsibility to notify OPM that confidentiality is required and to identify any proprietary information. OPM will, to the extent practicable and consistent with law, consult with the Carrier prior to releasing any confidential report to allow the Carrier to request redactions or markings and/or take other appropriate action, though this decision lies with OPM.

Question 6: In the event of a subcontractor breach, must the Carrier send out a breach notice to enrollees if the subcontractor has assumed this responsibility?

OPM generally requires one notice to the FEHB enrollee which can be provided either by the Carrier or its subcontractor. If the subcontractor provides the notice, it must be in a form that allows the enrollee to easily identify the Plan. Alternatively, if such specific identification is not practical under the circumstances, Plan identification shall be otherwise accomplished in a manner agreed upon with OPM. The Contracting Officer reserves the right to direct the Carrier to issue a separate notice in order to avoid enrollee confusion.

Question 7: What are the requirements for sending a breach notice to a FEHB enrollee?

For a breach of PHI, the notice to FEHB enrollees will comport with 45 CFR § 164.404 for breaches as defined in the FEHB contract or guidance, and will be coordinated with OPM before any communication with FEHB enrollees. All other notices must be coordinated with OPM and the Carriers should follow OPM guidance to the extent practicable.

Question 8: What are the implementation requirements of this Carrier Letter?

Carriers must update their incident response policies to include a section on reporting consistent with this Carrier Letter within 120 days from the date this letter is issued.

Thank you for your support in administering the FEHB Program and the important benefits you provide to Federal employees, annuitants, and their families. If you have any questions concerning the guidance in this Carrier Letter, please contact your Contracting Officer.

Sincerely,

Alan P. Spielman
Director
Healthcare and Insurance