U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Flash Audit Alert

Obstruction by Health Net of California

Report Number 1C-LB-00-18-023
February 12, 2018

ABBREVIATIONS

CISO	**Chief Information Security Officer**
FEHBP	**Federal Employees Health Benefits Program**
Health Net	**Health Net of California**
HI	**Healthcare and Insurance**
IT	**Information Technology**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
PHI	**Protected Health Information**
PII	**Personally Identifiable Information**

TABLE OF CONTENTS

I. BACKGROUND

The U.S Office of Personnel Management (OPM) Office of the Inspector General (OIG) performs information technology (IT) audits of all insurance carriers that participate in the Federal Employees Health Benefits Program (FEHBP). These organizations contract with OPM to provide health insurance coverage for Federal employees, retirees, and their families. The objective of our IT audits is to ensure that the insurance carriers have controls in place to protect the confidentiality, integrity, and availability of highly sensitive protected health information (PHI) and personally identifiable information (PII) of FEHBP members.

Our IT audits primarily focus on the information systems that directly process and/or store FEHBP data. However, almost without exception, FEHBP carriers do not segregate FEHBP data from data for its other commercial and/or Federal customers. From a technical perspective, a control weakness on one system poses a threat to all other systems in the same logical and/or physical technical environment. Therefore, the scope of certain test work must include all parts of the organization's technical infrastructure that have a logical and/or physical nexus with FEHBP data.

On September 17, 2017, as is our normal procedure, we issued an IT audit notification letter to Health Net of California (Health Net). From October 2017 through January 2018, we engaged in pre-audit discussions and planning with Health Net, and two site visits were scheduled for this IT audit. The first site visit was January 22 - 26, 2018, and consisted of multiple interviews with subject matter experts at Health Net to discuss their IT security controls. The second site visit was scheduled for February 12 - 16, 2018, to conduct appropriate tests of those controls.

Although we completed the audit interviews during the first site visit, it subsequently became apparent that Health Net did not intend to cooperate with our planned testing. During our audit planning, we issued 13 data requests for supporting documentation that were discussed in the audit interviews, with due dates between January 22 and February 1, 2018. As of February 6, not a single document had been provided to us. Furthermore, Health Net refused to confirm that it would deliver the requested items or let us perform critical vulnerability and configuration management testing.

We became increasingly concerned that Health Net's delaying tactics and lack of cooperation regarding our testing would negatively impact not only this audit engagement, but also our oversight of other FEHBP carriers and of OPM itself. Accordingly, we issued a formal memorandum on February 6, 2018 to Health Net requesting that they state in writing whether

they intended to comply with our audit. On February 7, 2018, we received an e-mail from Heath Net stating that the company did NOT intend to comply with our requests. Specifically, the response stated:

1. Health Net will not allow the OIG to conduct vulnerability and configuration management testing.

2. Health Net will not provide the OIG with the documentation required to perform testing related to Health Net's ability to effectively remove information system access to terminated employees and contractors.

Health Net's actions are in direct violation of the company's contract with OPM, and also disregard the statutory authority of the OIG. Of greater concern, however, is that the auditors cannot evaluate Health Net's IT security controls in the above two critical areas – which are discussed further in this report. As a result, we are unable to attest whether Health Net is acting as a responsible custodian of critically sensitive PHI and PII of FEHBP members.

II. HEALTH NET IS OBSTRUCTING A FEDERAL AUDIT

Vulnerability and configuration management testing involves using commercially available software tools to scan a sample of computer servers within a technical environment. The vulnerability scans are able to automatically detect security weaknesses such as missing patches, unsupported software, and insecure configuration settings. Our test work is designed to identify systemic weaknesses in an organization's patching, system configuration, and vulnerability management processes. These weaknesses can be exploited by unauthorized individuals to obtain access to sensitive resources including PHI and PII.

Although many organizations perform vulnerability scans on their own environment, the results of these scans are not sufficient for an auditor to provide an independent evaluation. The auditors do not have any insight or control of the organization's scans, and therefore cannot validate that they were performed appropriately. In fact, we commonly find that the organization's internal vulnerability management program is inadequate, a conclusion that can only be drawn by evaluating the results of independently performed vulnerability scans.

Furthermore, it is critical that our testing includes the entire technical environment in which FEHBP data resides. Although we focus on servers that directly process or store FEHBP data, we judgmentally select other high-risk servers to include in the scope of testing. A vulnerability on *any* server in the environment poses a threat to *all* data within that environment. For example, a missing patch on a Windows domain controller (that does not contain any FEHBP data) could allow an attacker to gain control of that server and subsequently compromise a different (otherwise secure) FEHBP server.

On February 7, 2018, Health Net stated in writing that it would not allow us to perform the vulnerability scanning test work. Health Net's refusal to allow this standard audit test work as part of our audit leaves multiple questions about Health Net's vulnerability and configuration management programs unanswered. [redacted]

As mentioned above, we perform vulnerability scan testing as part of all audits of FEHBP insurance carriers, and have done so for over 10 years in approximately 70 unique technical environments.

Although we understand the concerns associated with work of this nature, we take great care to minimize risk. Our procedures were developed as part of a collaborative working group

comprised of health insurance industry Chief Information Officers and Chief Information Security Officers. There is nothing unique about Health Net, its technical environment, or the nature of our proposed testing that would exempt Health Net from our oversight and this testing.

Another critical element of an IT audit involves performing tests to ensure that information system access is promptly removed for individuals who are terminated from the organization. This test involves comparing lists of organization employees and contractors with active access to information systems to a complete list of individuals who have recently been terminated. If terminated employees appear on the current access list, it could indicate a weakness in the organization's controls for managing user accounts. Failure to promptly remove system access increases the risk that these user accounts could be exploited to inappropriately access sensitive resources including PHI and PII.

Health Net officials' obstruction also extends to this section of our audit. These officials have refused to produce complete lists of individuals with network access (i.e., [redacted] accounts) and recently terminated individuals. Rather, Health Net offered to provide a scope-limited list of individuals that it deems relevant to our audit (e.g., employees and contractors who have access to specific systems that process FEHBP data).

However, these scope-limited lists will not allow us to effectively achieve our audit objective, which is to assess Health Net's company-wide process for removing system access. We cannot draw adequate conclusions about a process without the ability to test it in its entirety. For example, the organization may be vigilant in removing network access for the scope-limited set of employees, but may have weaknesses in its procedures for removing access for employees in another part of the organization. [redacted]

Health Net's refusal to provide complete access and termination lists is unprecedented in our IT audits. We request only the individual's name (or a unique identifier such as employee ID) and the employment termination date. This information is not considered PHI or PII, so there is limited risk to these individuals in the unlikely event that the lists were somehow inadvertently released.

III. ENFORCEMENT OF OPM CONTRACT

OPM Enforcement of Contractual Authority

We have worked closely with OPM's Healthcare and Insurance office throughout our engagement with Health Net. The Healthcare and Insurance contracting officer has been very supportive of our audit, and made it clear that Health Net officials' refusal to cooperate would violate the company's contract with OPM. On February 12, 2018, the contracting officer sent a letter to the Director of Health Net reiterating the necessity to comply with the audit requirements of the contract. In addition, the OPM Chief Information Security Officer (CISO) also participated in discussions of security concerns with Health Net and encouraged full cooperation with the test work. While we sincerely appreciate OPM's support of our audit objectives, it is clear that additional action is required.

The contract between OPM and Health Net contains language that requires the organization to comply with the audit requests outlined in this report. Specifically, section 1.28 of contract CS-2002 states that:

> "The Contracting Officer or an authorized representative of the Contracting Officer may use NIST SP 800-53 (or its current equivalent) requirements as a benchmark for conducting audits of Carrier information systems and may recommend that the Carrier adopt a best practice drawn from NIST SP 800-53 (or its current equivalent) to the following Carrier information systems:
>
> (i) Information systems that directly process FEHBP data for contract purposes; and
> (ii) All other information systems operating in the same general information technology control environment as the information systems in (i) above."

As discussed with Health Net, Healthcare and Insurance, and OPM's CISO on January 18, 2018, all documentation that we have requested and all information systems that we wish to test are contained within "the same general information technology control environment" as the systems that directly process or store FEHBP data. It is clear that our audit is within the scope of contract CS-2002.

Recommendation 1

We recommend that the OPM Director require Health Net to cooperate and immediately permit the requested IT testing described in the OIG procedure document.

Recommendation 2

We recommend that the OPM Director require Health Net to cooperate and immediately provide all records requested pursuant to our audit.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100