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

# Final Audit Report

**Subject:**

## AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT WELLPOINT INC.

**Report No. 1A-10-00-13-012**

**Date:** September 10, 2013

**--CAUTION--**

**This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.**

# Audit Report

**FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM**
**CONTRACT CS 1039**
**WELLPOINT INC.**
**PLAN CODES 10 / 11**
**ROANOKE, VIRGINIA**

**Report No. 1A-10-00-13-012**

**Date:** September 10, 2013

**Michael R. Esser**
**Assistant Inspector General**
**for Audits**

**--CAUTION--**

**This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.**

# Executive Summary

**FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM**
**CONTRACT CS 1039**
**WELLPOINT INC.**
**PLAN CODES 10 / 11**
**ROANOKE, VIRGINIA**

**Report No. 1A-10-00-13-012**

**Date:** September 10,2013

This final report discusses the results of our audit of general and application controls over the information systems at WellPoint Inc. (WellPoint or Plan).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for WellPoint, as well as the various processes and information technology (IT) systems used to support these applications. We documented controls in place and opportunities for improvement in each of the areas below.

Security Management

WellPoint has established a series of IT policies and procedures to create an awareness of IT security at the Plan. We also verified that WellPoint has adequate human resources policies related to the security aspects of hiring, training, transferring, and terminating employees.

Access Controls

WellPoint has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. However, the physical access controls to one specific facility visited by auditors could be improved. We also noted weaknesses in WellPoint's implementation of segregation of duties and privileged user monitoring.

Network Security

WellPoint has implemented a thorough incident response and network security program. However, we noted several opportunities for improvement related to WellPoint's network security controls. WellPoint has not implemented technical controls to prevent rogue devices from connecting to its network. Also, several specific servers containing Federal data are not subject to routine vulnerability scanning, and we could not obtain evidence indicating that these servers have ever been subject to a vulnerability scan. In addition, WellPoint limited our ability to perform adequate testing in this area of the audit. As a result of this scope limitation and WellPoint's inability to provide additional supporting documentation, we are unable to independently attest that WellPoint's computer servers maintain a secure configuration.

Configuration Management

WellPoint has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes. However, we noted that WellPoint's mainframe password settings are not in compliance with its own corporate standards.

Contingency Planning

We reviewed WellPoint's business continuity plans and concluded that they contained the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis.

Claims Adjudication

WellPoint has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in WellPoint's claims application controls. Additionally, there is no auditing to ensure the manual process for debarring providers is done appropriately.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that WellPoint is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

# Contents

Page

Executive Summary ..... i

I. Introduction ..... 1

Background ..... 1

Objectives ..... 1

Scope ..... 1

Methodology ..... 2

Compliance with Laws and Regulations ..... 3

II. Audit Findings and Recommendations ..... 4

A. Security Management ..... 4

B. Access Controls ..... 4

C. Network Security ..... 7

D. Configuration Management ..... 11

E. Contingency Planning ..... 12

F. Claims Adjudication ..... 12

G. Health Insurance Portability and Accountability Act ..... 15

III. Major Contributors to This Report ..... 17

Appendix: WellPoint's June 14, 2013 response to the draft audit report issued April 10, 2013.

# I. Introduction

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims by WellPoint Inc. (WellPoint or Plan).

The audit was conducted pursuant to FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

## Background

The FEHBP was established by the Federal Employees Health Benefits Act (the Act), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our second audit of WellPoint's general and application controls. The first audit was conducted in 2006, and all recommendations from that audit were closed prior to the start of the current audit. We also reviewed WellPoint's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

## Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in WellPoint's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to WellPoint's claims processing systems; and
- HIPAA compliance.

## Scope

We obtained an understanding of WellPoint's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of WellPoint's internal controls was used in planning the audit by determining the extent of compliance testing and other

auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by WellPoint to process medical insurance claims for FEHBP members in the following states: Virginia, Connecticut, New Hampshire, Maine, Ohio, Kentucky, Indiana, Missouri, Wisconsin, Nevada, Colorado, and California (institutional only). The business processes reviewed are primarily located in WellPoint's facilities in Virginia. We also toured WellPoint's primary data center located in Missouri.

The on-site portion of this audit was performed in January and February of 2013. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at WellPoint as of March 2013.

This performance audit was conducted in accordance with generally accepted government auditing standards (GAS) issued by the Comptroller General of the United States, except for specific applicable requirements that were not followed. There was one element of our audit in which WellPoint applied external interference with the application of audit procedures, resulting in our inability to fully comply with the GAS requirement of independence.

We routinely use our own automated tools to evaluate the configuration of a sample of computer servers. When we requested to conduct this test at WellPoint, we were informed that a corporate policy prohibited external entities from connecting to the WellPoint network. In an effort to meet our audit objective, we attempted to obtain additional information from WellPoint, but the Plan was unable to provide satisfactory evidence that it has ever had a program in place to routinely monitor the configuration of its servers (see the "Configuration Compliance Auditing" section on page 9 for additional details.)

As a result of the scope limitation on our audit work and WellPoint's inability to provide additional supporting documentation, we are unable to independently attest that WellPoint's computer servers maintain a secure configuration.

In conducting our audit, we relied to varying degrees on computer-generated data provided by WellPoint. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

## Methodology

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed WellPoint's business structure and environment;
- Performed a risk assessment of WellPoint's information systems environment and applications, and prepared an audit program based on the assessment and the Government

Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluate WellPoint's control structure. These criteria include, but are not limited to, the following publications:

- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30 Revision 1, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and
- HIPAA Act of 1996.

## Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether WellPoint's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, WellPoint was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

# II. Audit Findings and Recommendations

## A. Security Management

The security management component of this audit involved the examination of the policies and procedures that are the foundation of WellPoint's overall IT security controls. We evaluated WellPoint's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

WellPoint has implemented a series of formal policies and procedures that comprise its security management program. WellPoint's Chief Information Security Officer owns the Information Security Program and is responsible for developing, implementing, and enforcing the program's standards. WellPoint has also developed a thorough risk management methodology, and has procedures to document, track, and mitigate or accept identified risks. We also reviewed WellPoint's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that WellPoint does not have an adequate security management program.

## B. Access Controls

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls of WellPoint's facilities in St. Louis, Missouri and Roanoke, Virginia. We also examined the logical access controls protecting sensitive data on WellPoint's network environment and claims processing related applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting physical access to facilities and data centers;
- Procedures for revoking access to data centers for terminated employees;
- Procedures for removing Windows/network access for terminated employees; and
- Controls to monitor and filter email and Internet activity.

The following sections document several opportunities for improvement related to WellPoint's physical and logical access controls.

### 1. Privileged User Monitoring

WellPoint has configured its servers to record the activity of privileged users (i.e., system administrators). However, the event logs generated by these servers are only reviewed retroactively if a problem has been reported or detected.

NIST SP 800-53 Revision 3 requires that an organization "Reviews and analyzes information system audit records . . . for indications of inappropriate or unusual activity, and reports findings to designated organizational officials…."

Failure to routinely review elevated user activity increases the risk that malicious activity could go undetected and sensitive information could be compromised.

**Recommendation 1**

We recommend that WellPoint implement a process to routinely review elevated user (administrator) activity.

***WellPoint Response:***

***"The Plan stated that Management is in the process of implementing an automated monitoring program for privileged user access. The workflow process includes:***

- ***Automated 24X7 protected logging of 'events of interest' for the WellPoint mainframe, Unix and Intel environments;***
- ***Monitoring of WellPoint's environment to audit and validate events that are triggered by HIPAA-compliant auditing and logging (monitoring) criteria;***
- ***Integrating and leveraging of IBM's Security Intelligence portfolio, QRadar, within the e-SIEM workflow, and WellPoint's change management system; and***
- ***Implementation of the monitoring tools will be implemented by year-end 2013, with auditing and validation processes fully implemented by September 30, 2014."***

**OIG Reply:**

As part of the audit resolution process, we recommend that WellPoint provide OPM's Healthcare and Insurance office (HIO) with evidence that a process to routinely review elevated user activity has been implemented.

**2. Segregation of Duties**

WellPoint does not have a documented process to ensure proper segregation of duties in its Streamline claims adjudication application.

WellPoint uses role-based access control to grant access to Streamline, and many employees are granted multiple roles as they gain experience in their job function. However, there is no documented policy or procedure to indicate which roles would create a conflict (i.e., too much control over the claims adjudication process) if granted to the same individual.

FISCAM states that "Work responsibilities should be segregated so that one individual does not control critical stages of a process." FISCAM also states that "Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions."

Failure to enforce adequate segregation of duties in the claims processing application increases the risk that erroneous or fraudulent claims could be processed.

**Recommendation 2**

We recommend that WellPoint implement a process for ensuring Streamline application access is granted with proper segregation of duties.

***WellPoint Response:***

***"The Plan stated that job titles are utilized for granting security for associates. The three Attachments… include the matrix and procedures for granting security access that demonstrates the changes made to enhance this process."***

**OIG Reply:**

The evidence provided by WellPoint in response to the draft audit report indicates that the Plan has implemented a process to ensure access to Streamline is granted with proper segregation of duties; no further action is required.

### 3. Facility Physical Access Controls

The physical access controls at one of WellPoint's facilities in Virginia could be improved.

The facility uses an electronic card reader to control access to the building. However, we observed numerous occasions when the door was propped open for deliveries and people walked through the door without badging in or being checked by the security guard(s) stationed nearby.

In addition, WellPoint does not have physical access controls in place to prevent employees from piggybacking into secure areas (one person using an electronic access card to open a door, then holding that door open while others enter). FISCAM states that "Physical controls at entrances and exits vary, but may include[:] manual door locks or cipher key locks, magnetic door locks that require the use of electronic keycards, biometrics authentication, security guards, photo IDs, entry logs, and electronic and visual surveillance systems."

In addition, NIST SP 800-53 provides guidance for adequately controlling physical access to information systems containing sensitive data (see control PE-3, Physical Access Control).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to WellPoint facilities and the sensitive IT resources and confidential data they contain.

**Recommendation 3**

We recommend that WellPoint reassess the physical access controls at its Roanoke, Virginia facility, and implement controls that will ensure proper physical security. At a minimum, WellPoint should add an alarm to the facility entrances that will detect a door left propped open.

***WellPoint Response:***

***"The Plan stated that the facility currently has an access control system in place that alerts security officers when a door is being held open. This system and functionality has been in place for several years. The facility is undergoing a security upgrade and will have a new system that will not only alert the onsite security officers of a door held open, but will also notify corporate security officers at the security command center located in the corporate headquarters building. This installation will be completed by June 30, 2013. Upon completion of the system upgrade, the site will meet the risk and threat based standards developed for all sites across the enterprise."***

**OIG Reply:**

As part of the audit resolution process, we recommend that WellPoint provide OPM's HIO with evidence that the physical access security upgrades described in WellPoint's response to the draft audit report have been implemented.

## C. Network Security

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

WellPoint has implemented a thorough incident response and network security program. However, we noted several opportunities for improvement related to WellPoint's network security controls.

### 1. Preventing Rogue Devices

WellPoint has not implemented technical controls to prevent rogue devices (laptops, workstations, or routers not issued by or approved by the company) from connecting to its network.

NIST SP 800-53 Revision 3 states that information systems should uniquely identify and authenticate devices before establishing a connection. Failure to implement technical controls to detect rogue devices could allow anyone with physical access to WellPoint facilities to connect an unauthorized device to WellPoint's network. This risk is magnified by the relatively weak physical access controls observed at WellPoint's Roanoke, VA facility.

**Recommendation 4**

We recommend that WellPoint implement technical controls to prevent rogue devices from connecting to its network.

***WellPoint Response:***

***"The Plan stated that Management believes that the associated risk is adequately mitigated based upon the following controls:***

- ***Authentication is required for all applications on our network.***

- ***Direct wireless connectivity to the WellPoint network is prohibited.***

- ***Policies:***
  - ***Require training for all users, including annual employee certification.***
  - ***State who is/isn't authorized to physically be on WellPoint premises to help protect both physical PHI (such as printed materials) and electronic PHI. Also, devices that can/can't be connected to the WellPoint network are defined.***
  - ***State that a visitor must be escorted throughout the facility. Visitors coming to our buildings are escorted while on the premises and WellPoint associates are responsible for monitoring the activities of their visitors.***

- ***Controls are in place to enforce the physical security of our buildings, including guards, badge readers, cameras, etc. to help prevent unauthorized individuals from connecting rogue or unauthorized devices to the WellPoint network.***

- ***See physical access changes being implemented for the Roanoke, Virginia building (Recommendation #3 response).***

***WellPoint's focus is on protecting the data. As outlined in the mitigating controls above, along with our robust security event monitoring and network security program, we believe that the risk has been adequately addressed. We continually monitor security exposures and have built layers of defense to protect data, and will continue to implement programs that have been proven effective."***

**OIG Reply:**

The controls described in WellPoint's response to the draft audit report could prevent someone without authorized physical access to a WellPoint facility from connecting a device to the network. However, none of the controls would prevent someone with authorized access (e.g., employees, contractors, or guests) from connecting a personal device to the WellPoint network. Therefore, we continue to recommend that WellPoint implement technical controls to prevent rogue devices from connecting to its network.

**2. Full Scope Vulnerability Scanning**

We conducted an extensive review of WellPoint's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities. We determined that WellPoint has a mature vulnerability management program and that the vast majority of devices are scanned on a routine basis. All detected vulnerabilities are analyzed, prioritized, and tracked to remediation.

However, during our review we discovered that several specific servers containing Federal data are not subject to routine vulnerability scanning, and we could not obtain evidence indicating that these servers have ever been subject to a vulnerability scan. NIST SP 800-53 Revision 3 states that the organization should scan "for vulnerabilities in the information system and hosted applications…."

Failure to perform full scope vulnerability scanning increases the risk that WellPoint's systems are compromised and sensitive data stolen or destroyed.

**Recommendation 5**

We recommend that WellPoint ensure that vulnerability scanning is conducted on all servers, specifically the servers housing Federal data that are not currently part of WellPoint's vulnerability management program.

***WellPoint Response:***

***"The Plan stated that the only devices identified during the review that were not being scanned were desktop devices that:***

- ***Do not contain FEP data, and are only used for additional computing power for tasks that are generally performed on user desktops.***

- ***The Desktop Devices are being retired within the next 60 days. The Plan believes that it has demonstrated that it scans all servers that contain FEP data. WellPoint Information Security has processes in place to help ensure that newly provisioned servers are scanned and certified prior to production use, and are added to the scanning inventory that is used for conducting our periodic vulnerability scans. The Plan will continue to work to help ensure that our scanning inventory is kept up-to date and reflects the latest WellPoint server inventory."***

**OIG Reply:**

The fact that a specific server does not contain FEP data has no bearing on the importance of keeping the device secure when it operates in the same environment as other devices that do process FEP data. Any server not subject to routine scanning may contain a vulnerability that an attacker could exploit to gain access to the WellPoint network. Once on the network, it is much easier for the attacker to gain unauthorized access to FEP data. Therefore, we continue to recommend that WellPoint conduct vulnerability scanning on all servers.

### 3. Configuration Compliance Auditing

Configuration compliance auditing refers to the process of routinely comparing the actual security configuration of computer servers to an approved baseline configuration. Our audit objective with regards to configuration compliance auditing is to determine whether the organization has a process in place to ensure that servers remain securely configured and up-to-date with security patches.

In order to evaluate an FEHBP carrier's configuration compliance auditing program, we typically use automated tools to document the actual configuration of a sample of servers. We then manually compare the results to the company's approved baseline configuration. When the actual settings generally match the approved baseline, we gain confidence that the company's servers are securely configured.

When we requested to conduct this test at WellPoint, we were informed that a corporate policy prohibited external entities from connecting to the WellPoint network. In an effort to meet our audit objective, we attempted to obtain additional information about WellPoint's configuration compliance auditing program. We were initially provided a description of what appeared to be a thorough configuration compliance auditing program at WellPoint. However, when we requested documentation to support this description, WellPoint was unable to provide any evidence that a configuration compliance auditing program had ever been in place at the company.

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers remain undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

As a result of the scope limitation on our audit work and WellPoint's inability to provide additional supporting documentation, we are unable to independently attest that WellPoint's computer servers maintain a secure configuration.

**Recommendation 6**

We recommend that WellPoint implement a configuration compliance auditing program.

***WellPoint Response:***

***"The Plan stated that its' Vulnerability Management Program includes ongoing patching. Security patches for high severity vulnerabilities are applied within 90 days on DMZ servers and 180 days on internal servers. For the configuration management compliance program, WellPoint is finalizing its transition to the Tivoli Endpoint Manager (TEM) tool from the Blade Logic tool. The tool transition is scheduled to be complete by June 30, 2013, with the configuration management compliance program targeted to be fully operational by October 31, 2013 for midrange and Intel servers.***

***The Plan's contract with its outsource IT partner requires ongoing compliance to WellPoint's technical configuration standards (TCS). Variances to a TCS parameter require a security exception to be formally approved. Governance over this outsourced arrangement is provided through WellPoint's configuration management compliance program."***

**OIG Reply:**

During the fieldwork phase of the audit, WellPoint provided us with conflicting statements regarding its plans to transition to Tivoli Endpoint Manager (TEM). These conflicting statements along with WellPoint's inability to provide evidence that it performs configuration compliance scans ultimately led to us documenting a formal scope limitation. As part of the audit resolution process, we recommend that WellPoint provide OPM's HIO with evidence that the TEM tool has been fully implemented, and that it is routinely performing configuration compliance audits. OPM's HIO should carefully scrutinize any supporting documentation submitted by WellPoint related to this issue before considering closure of this recommendation.

## D. Configuration Management

We evaluated WellPoint's controls to securely configure its mainframe, databases, and servers that support the applications used to process FEHBP claims. We determined that the following controls are in place:

- Controls for securely managing changes to the operating platform and claims processing application;
- Detailed operating system configuration standards; and
- Thorough patch management procedures.

However, we discovered that WellPoint's mainframe password settings are not in compliance with its own corporate standards.

WellPoint has created Technical Configuration Standards (TCS) that outline approved configuration settings for server and mainframe security software. We reviewed the Technical Configuration Standards to determine if they conformed to industry best practices. We also compared the approved TCS settings to the actual settings of WellPoint's servers and mainframes. We determined that the TCS were created in accordance with best practices. However, we found several mainframe security settings that were not in compliance with the TCS.

Failure to configure password security settings in compliance with approved settings increases the risk that unauthorized users could gain access to sensitive resources.

**Recommendation 7**

We recommend that WellPoint modify its mainframe password settings to comply with its corporate policy.

***WellPoint Response:***

***"The Plan stated that when Technical Configuration Standards (TCS) parameters are updated, a transition timeline is defined to comply with new or modified parameters for each LPAR. The audit team reviewed ACF TCS version 1.0 which reflected recent password setting updates to comply with HITRUST requirements, which the audit team noted as compliance gaps. Since the completion of the audit, the WellPoint security team has updated and published ACF TCS version 2.0.***

***As of April 26, 2013, the password settings have been updated to comply with ACF TCS version 2.0, which was published on April 23, 2013. Procedures for the review process were documented…."***

**OIG Reply:**

The evidence provided by WellPoint in response to the draft audit report indicates that the Plan has made system modifications to align the mainframe password settings with its corporate policy; no further action is required.

## E. Contingency Planning

We reviewed the following elements of WellPoint's contingency planning program to determine whether controls were in place to prevent or minimize damage and interruptions to business operations when disastrous events occur:

- Business continuity plans for several business locations and data center operations;
- Disaster recovery plan for the claims processing system;
- Disaster recovery plan tests conducted in conjunction with the recovery site; and
- Emergency response procedures and training.

We determined that WellPoint's contingency planning documentation contained the critical elements suggested by NIST SP 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems." WellPoint has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that WellPoint has not implemented adequate controls related to contingency planning.

## F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting WellPoint's claims adjudication process.

### 1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of WellPoint's claims processing systems.

WellPoint has implemented policies and procedures related to application configuration management, and has adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- WellPoint has adopted practices that allow modifications to be tracked throughout the change process;
- Code, unit, system, and quality testing are all conducted in accordance with industry standards; and
- WellPoint uses a business unit independent from the software developers to move the code between development and production environments to ensure adequate segregation of duties.

Nothing came to our attention to indicate that WellPoint has not implemented adequate controls related to the application configuration management process.

## 2. Claims Processing System

We evaluated the input, processing, and output controls associated with WellPoint's claims processing system. We have determined the following controls are in place over WellPoint's claims adjudication system:

- Routine audits are conducted on WellPoint's front-end scanning vendor for incoming paper claims;
- Claims are monitored as they are processed through the systems with real time tracking of the system's performance; and
- Claims output files are fully reconciled.

Nothing came to our attention to indicate that WellPoint has not implemented adequate controls over the claims processing system.

## 3. Debarment

WellPoint has adequate procedures for updating its claims system with debarred provider information, but it does not routinely audit its debarment database for accuracy.

WellPoint receives the OPM OIG debarment list every month and compares the monthly changes to its internal provider file. Any debarred providers that appear in WellPoint's provider database are flagged to prevent claims submitted by that provider from being processed by the claims processing system.

However, this process is done manually, and WellPoint does not have an auditing process in place to ensure that all modifications are accurate and complete.

Failure to audit the accuracy of the debarment file increases the risk that claims are being paid to providers that are debarred.

**Recommendation 8**

We recommend that WellPoint implement a process to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate.

***WellPoint Response:***

***"The Plan stated that based on the recommendation a new audit process was implemented effective June 1, 2013 to review the Debarred Provider Listings to ensure all debarment related modifications to the Provider Files are complete and accurate. Procedures for the review process were documented…."***

**OIG Reply:**

The evidence provided by WellPoint in response to the draft audit report indicates that the Plan has created a procedure to audit modifications to the debarment file; no further action is required.

## 4. Application Controls Testing

We conducted a test on WellPoint's claims adjudication application to validate the system's claims processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which WellPoint's system adjudicated the claims.

Our test results indicate that the system has controls and edits in place to identify the following scenarios:

- Invalid members and providers;
- Member eligibility;
- Gender;
- Timely filing; and
- Catastrophic maximum.

The sections below document opportunities for improvement related to WellPoint's claims application controls.

### a. Provider/Procedure Inconsistency

Two test claims were processed where a provider was paid for services outside the scope of their license.

We entered a test claim for a [redacted]. Both claims were performed by a [redacted] who was billing as a [redacted] Although a [redacted] can act as an [redacted], their license does not allow them to provide services as [redacted] However, these test claims were processed by the system without encountering any edits.

Failure to detect provider/procedure inconsistencies increases the risk that fraudulent claims are paid or that providers are paid more than is allowed for the services rendered (i.e., [redacted] being paid the [redacted] rate when an [redacted] rate would be appropriate).

**Recommendation 9**

We recommend that WellPoint ensure the appropriate system modifications are made to detect provider/procedure inconsistencies.

***WellPoint Response:***

***"The Plan stated that it made a request to pend claims with the specific instance identified in the audit and this change should be complete within 60 days. We have also requested from the FEP Director's Office a listing of providers and the specialties that are considered outside of their license. A request to pend claims with specific criteria will be set up to stop each situation that is identified. The request for this wider***

***net will be dependent upon the identification of providers and specialties. Once identified, the necessary changes will be added to the system within 60 days."***

**OIG Reply:**

As part of the audit resolution process, we recommend that WellPoint provide OPM's HIO with evidence that system modifications have been made to detect provider/procedure inconsistencies.

**b.** [redacted]

Two separate test claims were processed for the [redacted]

Due to the potential fraudulent nature of this scenario, we expected the system to suspend these claims for further review; however no edit was generated by the system. Failure to detect [redacted] increases the risk that fraudulent or erroneous claims are paid.

**Recommendation 10**

We recommend that WellPoint ensure the appropriate system modifications are made to prevent [redacted] claims from processing without proper verification.

***WellPoint Response:***

***"The Plan stated that it has requested that Washington set up a deferral code that would capture only claims that are*** [redacted]. ***This would allow WellPoint Plans to capture the claims in one location. Streamline automation would then be created to deny these claims. FEP EOB information would provide a denial reason similar to*** [redacted]

**OIG Reply:**

As part of the audit resolution process, we recommend that WellPoint provide OPM's HIO with evidence that system modifications have been made to prevent [redacted] claims from being processed.

## G. Health Insurance Portability and Accountability Act

We reviewed WellPoint's efforts to maintain compliance with the security and privacy standards of HIPAA.

WellPoint has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. WellPoint has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. WellPoint reviews its HIPAA privacy and security policies annually and updates when necessary. WellPoint's Privacy Office oversees all HIPAA activities, and helps develop,

publish, and maintain corporate policies. Each year, all employees must complete compliance training which encompasses HIPAA regulations as well as general compliance.

Nothing came to our attention to indicate that WellPoint is not in compliance with the various requirements of HIPAA regulations.

# III. Major Contributors to This Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Deputy Assistant Inspector General for Audits
- [redacted], Senior Team Leader
- [redacted], Auditor-In-Charge
- [redacted], Lead IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

Appendix

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans
Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

June 14, 2013

[redacted], Lead
Information Systems Audits Group
Insurance Service Programs
Office of Personnel Management
1900 E Street, N.W., Room 6400
Washington, D.C. 20415

**Reference: OPM DRAFT EDP AUDIT REPORT**
**WellPoint BlueCross BlueShield Plans**
**Audit Report Number 1A-10-00-13-012**
**Report Dated April 10, 2013 and Received April 10, 2013**

Dear [redacted]:

This report is in response to the above-referenced U.S. Office of Personnel Management (OPM) Draft Audit Report covering the Federal Employees Health Benefits Program (FEHBP) Audit of Information Systems General and Application Controls for the Plan's interface with the FEP claims processing system, access, and security controls. Our comments regarding the recommendations in this report are as follows:

## A. Access Controls

### 1. Privileged User Monitoring

**Recommendation 1**

The OIG Auditors recommend that WellPoint implement a process to routinely review elevated user (administrator) activity.

**Response to Recommendation 1**

The Plan stated that Management is in the process of implementing an automated monitoring program for privileged user access. The workflow process includes:

- Automated 24X7 protected logging of 'events of interest' for the WellPoint mainframe, Unix and Intel environments;

- Monitoring of WellPoint's environment to audit and validate events that are triggered by HIPAA-compliant auditing and logging (monitoring) criteria;

- Integrating and leveraging of IBM's Security Intelligence portfolio, QRadar, within the e-SIEM workflow, and WellPoint's change management system; and

- Implementation of the monitoring tools will be implemented by year-end 2013, with auditing and validation processes fully implemented by September 30, 2014.

**2. Segregation of Duties**

**Recommendation 2**

The OIG Auditors recommend that WellPoint implement a process for ensuring Streamline application access is granted with proper segregation of duties.

**Response to Recommendation 2**

The Plan stated that job titles are utilized for granting security for associates. The three Attachments (Rec 2 Attachment A; Rec 2 Attachment B; and Rec 2 Streamline Security should this be Attachment C) include the matrix and procedures for granting security access that demonstrates the changes made to enhance this process.

**3. Facility Physical Access Controls- Greg Wurm/ Data Center**

.

**Recommendation 3**

The OIG Auditors recommend that WellPoint reassess the physical access controls at its Roanoke, Virginia facility, and implement controls that will ensure proper physical security. At a minimum, WellPoint should add an alarm to the facility entrances that will detect a door left propped open.

.

**Response to Recommendation 3**

The Plan stated that the facility currently has an access control system in place that alerts security officers when a door is being held open. This system and functionality has been in place for several years.

The facility is undergoing a security upgrade and will have a new system that will not only alert the onsite security officers of a door held open, but will also notify corporate security officers at the security command center located in the corporate headquarters building. This installation will be completed by June 30, 2013. Upon completion of the system upgrade, the site will meet the risk and threat based standards developed for all sites across the enterprise.

## B. Network Security

### 1. Detection of Rogue Devices

**Recommendation 4**

The OIG Auditors recommend that WellPoint implement technical controls to prevent rogue devices from connecting to its network.

**Response to Recommendation 4**

The Plan stated that Management believes that the associated risk is adequately mitigated based upon the following controls:

- Authentication is required for all applications on our network.
- Direct wireless connectivity to the WellPoint network is prohibited.
- Policies:
    - Require training for all users, including annual employee certification.
    - State who is/isn't authorized to physically be on WellPoint premises to help protect both physical PHI (such as printed materials) and electronic PHI. Also, devices that can/can't be connected to the WellPoint network are defined.
    - State that a visitor must be escorted throughout the facility. Visitors coming to our buildings are escorted while on the premises and WellPoint associates are responsible for monitoring the activities of their visitors.
- Controls are in place to enforce the physical security of our buildings, including guards, badge readers, cameras, etc. to help prevent unauthorized individuals from connecting rogue or unauthorized devices to the WellPoint network.

- See physical access changes being implemented for the Roanoke, Virginia building (Recommendation #3 response).

WellPoint's focus is on protecting the data. As outlined in the mitigating controls above, along with our robust security event monitoring and network security program, we believe that the risk has been adequately addressed. We continually monitor security exposures and have built layers of defense to protect data, and will continue to implement programs that have been proven effective.

**2. Vulnerability Scanning**

**Recommendation 5**

The OIG Auditors recommend that WellPoint ensure that vulnerability scanning is conducted on all servers, specifically the servers housing Federal data that are not currently part of WellPoint's vulnerability management program.

.

**Response to Recommendation 5**

The Plan stated that the only devices identified during the review that were not being scanned were desktop devices that:

- Do not contain FEP data, and are only used for additional computing power for tasks that are generally performed on user desktops.

- The Desktop Devices are being retired within the next 60 days. The Plan believes that it has demonstrated that it scans all servers that contain FEP data. WellPoint Information Security has processes in place to help ensure that newly provisioned servers are scanned and certified prior to production use, and are added to the scanning inventory that is used for conducting our periodic vulnerability scans. The Plan will continue to work to help ensure that our scanning inventory is kept up-to-date and reflects the latest WellPoint server inventory.

**3. Configuration Compliance Auditing**

**Recommendation 6**

The OIG Auditors recommend that WellPoint implement a configuration compliance auditing program.

**Response to Recommendation 6**

The Plan stated that its' Vulnerability Management Program includes ongoing patching. Security patches for high severity vulnerabilities are applied within 90 days on DMZ servers and 180 days on internal servers. For the configuration management compliance program, WellPoint is finalizing its transition to the Tivoli Endpoint Manager (TEM) tool from the Blade Logic tool. The tool transition is scheduled to be complete by June 30, 2013, with the configuration management compliance program targeted to be fully operational by October 31, 2013 for midrange and Intel servers.

The Plan's contract with its outsource IT partner requires ongoing compliance to WellPoint's technical configuration standards (TCS). Variances to a TCS parameter require a security exception to be formally approved. Governance over this outsourced arrangement is provided through WellPoint's configuration management compliance program.

## C. Configuration Management

**Recommendation 7**

The OIG Auditors recommend that WellPoint modify its mainframe password settings to comply with its corporate policy.

**Response to Recommendation 7**

The Plan stated that when Technical Configuration Standards (TCS) parameters are updated, a transition timeline is defined to comply with new or modified parameters for each LPAR. The audit team reviewed ACF TCS version 1.0 which reflected recent password setting updates to comply with HITRUST requirements, which the audit team noted as compliance gaps. Since the completion of the audit, the WellPoint security team has updated and published ACF TCS version 2.0.

As of April 26, 2013, the password settings have been updated to comply with ACF TCS version 2.0, which was published on April 23, 2013. Procedures for the review process were documented. See attachments Rec 7 IS-TCS-009 ACF2v2.0 and Rec 7 VA ACF2 Mainframe Co provide details of the changes made.

## Claims Adjudication

### 1. Debarment

#### Recommendation 8

The OIG Auditors recommend that WellPoint implement a process to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate.

#### Response to Recommendation 8

The Plan stated that based on the recommendation a new audit process was implemented effective June 1, 2013 to review the Debarred Provider Listings to ensure all debarment related modifications to the Provider Files are complete and accurate. Procedures for the review process were documented. See embedded attachment entitled Rec 8 Debarred Provider Audit.

### 2. Provider/Procedure Inconsistency

#### Recommendation 9

The OIG Auditors recommend that WellPoint ensure the appropriate system modifications are made to detect provider/procedure inconsistencies

#### Response to Recommendation 9

The Plan stated that it made a request to pend claims with the specific instance identified in the audit and this change should be complete within 60 days. We have also requested from the FEP Director's Office a listing of providers and the specialties that are considered 'outside of their license. ) A request to pend claims with specific criteria) will be set up to stop each situation that is identified. The request for this wider net will be dependent upon the identification of providers and specialties. Once identified, the necessary changes will be added to the system within 60 days.

**3.** [redacted]

**Recommendation 10**

The OIG Auditors recommend that WellPoint ensure that the appropriate system modifications are made to prevent [redacted] claims from processing without proper verification.

**Response to Recommendation 10**

The Plan stated that it has requested that Washington set up a deferral code that would capture only claims that are [redacted]
This would allow WellPoint Plans to capture the claims in one location. Streamline automation would then be created to deny these claims. FEP EOB information would provide a denial reason similar to "A [redacted]

We appreciate the opportunity to provide our response to this Draft Audit Report and request that our comments be included in their entirety as an amendment to the Final Audit Report.

Sincerely,

[redacted]

[redacted], CPA
Sr. Program Manager, Government Audit Resolution and Coordination
Program Assurance

[redacted]

Attachments (6)

cc: [redacted], WellPoint BCBS
[redacted], WellPoint BCBS
[redacted], WellPoint BCBS
[redacted], OPM
[redacted], OPM
[redacted], FEP
[redacted], FEP