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 BLUE SHIELD OF CALIFORNIA

**Report No. 1A-10-67-14-006**

**Date:** July 9, 2014

**--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**
**CONTRACTS 1039 AND 2639**

**BLUE SHIELD OF CALIFORNIA**

**PLAN CODES 10/11/SI**

**SAN FRANCISCO, CALIFORNIA**

**Report No. 1A-10-67-14-006**

**Date:** July 9, 2014

**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**
**CONTRACTS 1039 AND 2639**

**BLUE SHIELD OF CALIFORNIA**

**PLAN CODES 10/11/SI**

**SAN FRANCISCO, CALIFORNIA**

**Report No. 1A-10-67-14-006**

**Date:** July 9, 2014

This final report discusses the results of our audit of general and application controls over the information systems at Blue Shield of California (BSC or Plan).

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

Security Management

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

Access Controls

BSC has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. All weaknesses identified during the audit were remediated during the draft reporting period.

Network Security

BSC has implemented a thorough incident response and network security program. However, we noted several areas of concern related to BSC's network security controls:

- A full scope vulnerability management program has not been implemented, and some servers have never been subject to a vulnerability scan;
- A methodology to track and remediate weaknesses identified in vulnerability scans has not been implemented;
- [redacted]; and
- [redacted].

Configuration Management

BSC has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured, updated, and changes are controlled. However, BSC has not documented formal baseline configurations that detail the approved settings for its server operating systems, and therefore cannot effectively audit its security configuration settings.

Contingency Planning

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

Claims Adjudication

BSC has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in BSC's claims application controls.

Health Insurance Portability and Accountability Act (HIPAA)

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

# Contents

**Page**

# 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 Blue Shield of California (BSC or Plan).

The audit was conducted pursuant to FEHBP contracts CS 1039 and CS 2639; 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. A previous audit of BSC was conducted over 10 years ago. All recommendations from that audit have been closed.

All BSC personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

## Objectives

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

- Security management;
- Access controls;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to BSC's claims processing systems; and
- Health Insurance Portability and Accountability Act (HIPAA) compliance.

## Scope

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of BSC's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of BSC'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.

BSC has two separate plans that service federal employees, a Health Maintenance Organization (HMO) plan referred to as Access+ HMO, and a nationwide fee-for-service plan sponsored by the BlueCross and BlueShield Association (BCBSA) Federal Employee Program (FEP).

The scope of this audit centered on the information systems used by BSC to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. BSC processes claims on local systems for both the Access+ HMO and FEP plans. FEP claims are also submitted through FEP Express, BCBSA's nationwide claims adjudication system. The business processes reviewed during this audit are primarily located in BSC's facilities in Lodi, Redding, Rancho Cordova, and El Dorado Hills, California.

The on-site portion of this audit was performed in October and November of 2013. We completed additional audit work before and after the on-site visits 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 BSC as of December 2013.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BSC. 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 BSC's business structure and environment;
- Performed a risk assessment of BSC'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 BSC's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- 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, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-61 Revision 2, 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 BSC’s practices were consistent with applicable standards.  While generally compliant, with respect to the items tested, BSC 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 BSC's overall IT security controls. We evaluated BSC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BSC has implemented a series of formal policies and procedures that comprise its security management program. BSC's Enterprise Security group is responsible for reviewing and approving IT security policies. BSC's IT Audit group conducts annual risk assessments to determine which functional areas are at risk. We also reviewed BSC's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BSC 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 at BSC's facilities in San Francisco, Lodi, and Redding, California. We also examined the physical access controls at data centers located in El Dorado Hills and Rancho Cordova, California. We examined the logical controls protecting sensitive data in BSC's network environment and claims processing 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 facilities and data centers for terminated employees;
- Procedures for removing Windows/network access for terminated employees;
- Controls to monitor and filter e-mail and Internet activity; and
- Procedures for recertifying employees' access to systems and applications.

However, the following sections document several opportunities for improvement related to BSC's access controls.

### 1. Physical Access Removal

BSC's procedures for removing physical access privileges for terminated employees, including temporary employees, could be improved.

BSC uses a ticketing system to facilitate the granting, adjusting, and removal of physical access for employees. Each request must be approved and initiated by the employee's manager.

We compared a list of BSC employees terminated within the last year to a list of employees with active access cards, and discovered that the access cards assigned to 20 terminated employees still allowed access to BSC facilities. We also evaluated a list of temporary employees and determined that there were 29 access cards assigned to temporary employees that remained active after the individual's termination date.

NIST SP 800-53 Revision 4 states that an organization must terminate access upon termination of employment. NIST SP 800-53 Revision 4 also states that an organization must review and analyze systems audit records for indication of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

**Recommendation 1**

We recommend that BSC implement a process to routinely audit all active access cards to ensure that they are not assigned to terminated employees.

***BSC Response:***

***"The Plan agrees with this recommendation. In addition to the current process where notifications of employee terminations are sent to our Security team in real time and also audits are performed weekly based off of a list from our HRMS Workday of the prior week's terminations, we plan to institute a new process. By the end of every month, our HR Shared Services team will pull a report of all active employees for our Security team. By the 5th of the next month, the security team will run an audit on all active badges to ensure that only active employees are assigned active badges. This process became active on April 5, 2014. The first active employee report was run out of Workday in April, 2014. The results of this report were compared to the active badge report in CCure. 59 discrepancies were identified which signaled a data problem in the CCure system. All 59 discrepancies were corrected in CCure after validating the Workday information. The Workday and CCure systems now match and show consistent information."***

**OIG Reply:**

The evidence provided by BSC in response to the draft audit report indicates that the Plan has implemented a monthly audit process; no further action is required.

**2. Password Configuration Settings**

BSC's mainframe password settings do not conform to the Plan's approved password policy.

BSC maintains an approved password standard that describes the requirements for login passwords for network, systems and applications access. We compared the mainframe security configuration to the BSC password standard and determined that the current mainframe configuration was not in compliance with the Plan's password standard.

**Recommendation 2**

We recommend that BSC configure the mainframe password settings to conform to its corporate password standard.

***BSC Response:***

***"The Plan contests this recommendation. BSC's password standard requires users to maintain passwords that conform to a variety of requirements, such as minimum length and complexity. However, the mainframe only enforces selected password requirements. BSC completed a risk assessment that considered the mainframe's password configuration capabilities and concluded that the risk associated with the potential variance between BSC standards and the mainframe password configuration does not warrant modifying the mainframe's password enforcement configuration."***

**OIG Reply:**

While we cannot independently attest that BSC's mainframe password settings provide adequate security, we acknowledge that BSC has adequately researched this issue and accepts any risk associated with its current settings; no further action required.

## C. Network Security

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

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

### 1. Vulnerability Management Program

We reviewed BSC's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate security vulnerabilities. BSC utilizes two data centers for its business operations. One data center contains the mainframe, servers, and databases that support the claims processing application, and is managed by a third party contractor. The other data center is managed by the Plan and contains the majority of the network infrastructure, and is housed within a BSC facility.

The third party contractor conducts its own vulnerability scans on the servers and databases within its data center. Our review of the contractor's vulnerability scanning program indicated that there were sufficient controls in place to detect, track, and remediate any vulnerabilities discovered through scanning. The results were also communicated to BSC in a timely manner.

However, we determined that BSC has not implemented a full scope vulnerability management program for servers housed in the data center it maintains, and that some servers have never been subject to a vulnerability scan. We provided BSC with a list of 45 randomly selected servers and asked them to conduct vulnerability scans on those devices using its own scanning tool. The results indicated that only 12 servers were successfully scanned, and a variety of vulnerabilities were detected on each server. Furthermore, BSC was unable to produce historical scan results on the servers selected. We also determined that BSC has not implemented a process to track and remediate weaknesses identified as a result of vulnerability scans.

Due to BSC's inability to perform adequate vulnerability scans during our audit, and its objection to allowing us to perform the scans ourselves, we are unable to provide independent assurance that BSC's network environment is adequately protected against security threats.

NIST SP 800-53 Revision 4 states that an organization should identify, report, and remediate information system flaws. This includes incorporating flaw remediation into the organization configuration management process.

NIST SP 800-53 Revision 4 also 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 BSC's systems could be compromised and sensitive data stolen or destroyed.

### Recommendation 3

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

***BSC Response:***

***"The Plan agrees with this recommendation. BSC will ensure all servers are included in the routine vulnerability scanning, including those housing Federal employee plan data, effective May 31, 2014."***

### OIG Reply:

As part of the audit resolution process, we recommend that BSC provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this audit report that the Plan agrees with.

### Recommendation 4

We recommend that BSC implement policies and procedures to ensure that all vulnerabilities identified from network vulnerability scans are tracked and remediated in a timely manner.

***BSC Response:***

***"The Plan agrees with this recommendation. BSC will enhance policies and procedures to ensure vulnerabilities are appropriately addressed commensurate with their level of risk, by August 31, 2014."***

## 2. Firewall Management

BSC has implemented firewalls to help protect its network environment. However, a firewall hardening policy has not been developed, and [redacted]

BSC maintains a Network Security Management Policy that states "Appropriate firewall rule sets shall be established and maintained to control traffic flows into and out of the network." Although this policy discusses the management of a firewall at a high level, NIST SP 800-41 Revision 1 states that a firewall policy should dictate how firewalls should handle network traffic based on the organization's information security policies, and a risk analysis should be performed to determine types of traffic needed by the organization. The policy should also include specific guidance on how to address changes to the rule set.

Failure to implement a thorough firewall configuration policy and continuously manage the devices' settings increases the organization's exposure to insecure traffic and vulnerabilities.

**Recommendation 5**

We recommend that BSC document a formal firewall management policy.

***BSC Response:***

***"The Plan agrees with this recommendation. BSC will enhance firewall management policies as recommended by September 30, 2014."***

**Recommendation 6**

We recommend that BSC implement a process to [redacted], as defined by the organizational policies.

***BSC Response:***

***"The Plan agrees with this recommendation. BSC will enhance processes*** [redacted] ***as recommended by March 31, 2015."***

## 4. Privileged User Access Monitoring

BSC has configured its network monitoring tools to record the activity of privileged users (i.e., system administrators). However, the event logs generated by these tools are only [redacted].

NIST SP 800-53 Revision 4 requires that, "the organization reviews and analyzes information system audit records . . . for indications of inappropriate or unusual activity, and reports findings to organization-defined personnel or roles."

[redacted]

**Recommendation 7**

We recommend that BSC implement a process to [redacted]

***BSC Response:***

***"The Plan agrees with this recommendation. BSC will complete an in-progress project to*** [redacted] ***by March 31, 2015."***

## D. Configuration Management

BSC's claims processing application is housed in a mainframe environment. The platform includes many supporting applications and system interfaces. The mainframe and several supporting applications are hosted by the third party contractor discussed in Section C. Additional supporting applications are hosted in a data center within one of BSC's facilities. We evaluated BSC's configuration management of the server environment supporting the claims processing applications, and determined that the following controls were in place:

- Documented server hardening policy; and
- Thorough change management procedures for system software.

The sections below document areas for improvement related to BSC's configuration management controls.

### 1. Baseline Configuration Policy

BSC has created corporate configuration policies to establish configuration management responsibilities within IT functional areas and to ensure security requirements are met. While the third party contractor has documented detailed security configuration baselines for the mainframe and servers, BSC has not documented a formal baseline configuration outlining the approved security settings for the servers it hosts internally.

NIST SP 800-53 Revision 4 states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not meet performance requirements defined by the organization.

**Recommendation 8**

We recommend that BSC document approved security configuration settings/baselines for all network server operating systems.

***BSC Response:***

***"The Plan agrees with this recommendation. At the time of the audit, BSC was in the process of implementing new security configuration baselines. BSC has updated security***

***configuration baselines, established a process for maintaining them on an ongoing basis and will continue to refine them to reflect BSC-specific settings."***

**OIG Reply:**

The evidence provided by BSC in response to the draft audit report indicates that the Plan has developed an Infrastructure and System Hardening Framework that creates a process for documenting and implementing configuration baselines using Center for Internet Security (CIS) benchmarks. While this is an important step towards documenting approved security configuration settings/baselines, the Plan has not provided evidence that the framework has been fully implemented. We recommend that BSC provide HIO with evidence that approved security configuration baselines have been documented for all network server operating systems; this should include approved deviations and exceptions from CIS standard benchmarks as stated in the hardening framework.

### 2. Configuration Compliance Auditing

BSC's third party contractor conducts configuration compliance auditing on the mainframe and servers hosted in its data center. The contractor has developed approved security configuration settings for all system software and hardware, and uses those settings as a baseline in a compliance auditing process. BSC conducts compliance audits using generic Center for Internet Security baselines. However, as mentioned above, BSC does not maintain approved server configurations, and therefore cannot effectively audit those security settings (i.e., there are no approved settings to which to compare the actual settings). We were told that BSC is in the process of developing company specific configuration standards, and will conduct compliance auditing utilizing the new standards as soon as they are completed.

NIST SP 800-53 Revision 4 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures. FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system.

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.

**Recommendation 9**

We recommend that BSC routinely audit security configuration settings using approved baselines.

***BSC Response:***

***"The Plan agrees with this recommendation. BSC routinely audits security configuration settings against both industry and BSC-specific standards. BSC will complete the activities to ensure all servers are covered by these audits by May 31, 2014."***

## E. Contingency Planning

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

- Disaster response plan;
- Business continuity plan for data center operations;
- Business continuity plans for claims processing operations and claims support;
- Disaster recovery plan tests conducted in conjunction with the alternate data center; and
- Emergency response procedures and training.

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34 Revision 1, "Contingency Planning Guide for IT Systems." BSC 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 BSC has not implemented adequate controls related to contingency planning.

## F. Claims Adjudication

BSC has two separate claims adjudication systems, one for the Access+ HMO plan and one for the FEP PPO plan. We conducted tests and reviewed controls over both systems. The following sections detail our review of the applications and business processes supporting BSC's claims adjudication process. Unless otherwise noted, all findings and recommendations described below apply to both systems.

### 1. Application Configuration Management

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

BSC has implemented policies and procedures related to application configuration management and has also 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:

- Code, unit, system, and quality testing are all conducted in accordance with industry standards; and
- BSC uses a business unit independent from the software developers to move code between development and production environments to ensure adequate segregation of duties.

However, we requested a recently completed change package with all required deliverables and approvals, but BSC was unable to provide all of the artifacts required by its own policy. FISCAM states that "for the methodology to be properly applied, it should be sufficiently documented to provide staff with clear and consistent guidance." It also states that "authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made."

**Recommendation 10**

We recommend that BSC ensure that all changes made to applications are documented and approved in accordance to the corporate application management policy.

***BSC Response:***

***"The Plan agrees with this recommendation. At the time of the audit, BSC was in the process of implementing a new tool for managing application change. This implementation has completed and ensures changes are documented and approved per the application management policy."***

**OIG Reply:**

The evidence provided by BSC in response to the draft audit report indicates that a tool has been implemented that ensures all necessary approvals and supporting documentation for a change is housed in one location; no further action is required.

### 2. Claims Processing System

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

- Routine audits are conducted on BSC'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 BSC has not implemented adequate controls over the claims processing system.

### 3. Enrollment

We evaluated BSC's procedures for managing its database of member enrollment data. Electronic enrollment data is processed weekly and paper files are processed daily. BSC has a reconciliation process to ensure all data that was sent to the plan was received and processed.

Nothing came to our attention to indicate that BSC has not implemented adequate controls over the enrollment process.

### 4. Debarment

BSC has adequate procedures for updating its claims processing system for both the Access+ HMO and FEP plans with debarred provider information. However, the plan does not routinely audit the debarment databases for accuracy.

BSC receives the OPM OIG debarment list every month and compares the monthly changes to the claims processing system debarred provider file for both plans. Any debarred providers are manually flagged within the system. However, BSC does not fully audit the modifications to provider files for either the HMO or PPO plans to ensure that all manually entered changes are accurate and complete.

Failure to fully audit the accuracy of manual changes to the provider file increases the risk that claims are being paid to providers that are debarred.

In addition, BSC does not comply with the OIG's "Guidelines for Implementation of FEHBP Debarment and Suspension Orders" for its Access+ HMO plan. BSC's claim processing procedures are to deny all claims coming from a debarred provider immediately after the provider is debarred. OIG guidance states that claims should be paid during a 15-day "grace period" after members have been notified that a doctor has been debarred.

#### Recommendation 11

We recommend that BSC implement processes to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate for both the HMO and PPO plans.

#### Recommendation 12

We recommend that BSC make the appropriate changes to its debarment policies and procedures for the Access+ HMO plan to comply with the OIG's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.

#### Recommendation 13

We recommend that BSC make the appropriate changes to its claims processing systems for the HMO plan to ensure FEHBP claims are processed in accordance with the OIG's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.

***BSC Response:***

***"HMO response - Plan agrees with this recommendation.***

***The Plan will implement debarment processes outlined by OIG's 'Guidelines for Implementation of FEHBP Debarment and Suspension Orders' by the end of August 2014. Actions include implementation of quarterly audit, updated debarment procedure guide, and appropriate claims adjudication practices."***

## 5. Application Controls Testing

We conducted a test on BSC's claims adjudication applications to validate the systems' claims processing controls. Claims for the Access+ HMO were entered and processed in BSC's local system, while claims for the FEP PPO were entered into a separate BSC local system and then routed to FEP Express, BCBSA's nationwide claims adjudication system, for processing. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which BSC's system adjudicated the claims. While we entered test claims into both BSC systems, the recommendations below only apply to the FEP PPO plan.

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

- Invalid members and providers;
- Member eligibility;
- Gender;
- Overlapping hospital stays;
- Timely filing; and
- Chiropractic benefits.

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

### a. Medical Editing

Our claims testing exercise identified several scenarios where BSC's local system and the FEP Express system [redacted] in FEP claims. For each of the following scenarios, a test claim was [redacted]

- [redacted]
- [redacted] and
- [redacted]

[redacted]

**Recommendation 14**

We recommend that BCBSA make the appropriate system modifications to prevent [redacted]

***BCBSA Response:***

***"The FEP Claims system will be modified by 2nd quarter 2014 to perform certain types of medical editing."***

### b. Near Duplicate

Two separate test FEP claims were processed for the same patient, procedure code, diagnosis code, service date and billed amounts, [redacted]

[redacted]

**Recommendation 15**

We recommend that BCBSA ensure the appropriate system modifications are made to [redacted]

***BCBSA Response:***

***"An enhancement request was submitted to the FEP Operations Center on March 6, 2014 to enhance the national FEP Claims system to implement system modifications to [redacted] We will provide an update on this recommendation once feedback on the request is obtained."***

### c. Procedure Code Billing Guidelines Not Enforced

Test FEP claims were processed that violate standard billing guidelines.

We entered test claims [redacted]

Failure to detect this system weakness increases the risk that benefits are being paid for procedures that were not actually performed.

**Recommendation 16**

We recommend that BSC FEP and BCBSA make the appropriate system modifications to enforce proper procedure code billing guidelines.

***BCBSA Response:***

***"An enhancement request was submitted to the FEP Operations Center on March 6, 2014 to limit certain types of services."***

## G. Health Insurance Portability and Accountability Act

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

BSC has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule.  BSC has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule.  BSC reviews its HIPAA privacy and security policies annually and updates when necessary.  BSC'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 BSC 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], Group Chief
- [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

April 21, 2014

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

[redacted] Group Chief
Claims & IT Audits Group,
U.S. Office of Personnel Management
1900 E Street, Room 6400
Washington, D.C. 20415-1100

**Reference: OPM DRAFT AUDIT REPORT**
**Blue Shield of California IT Audit**
**Plan Codes 542**
**Audit Report Number 1A-10-67-14-006**
**(Dated February 11, 2014)**

The following represents the Plan's response as it relates to the recommendations included in the draft report.

## B. Access Controls

### 1. Physical Access Removal

**Recommendation 1**

We recommend that BSC implement a process to routinely audit all active access cards to ensure that they are not assigned to terminated employees.

**Plan Response**

The Plan agrees with this recommendation. In addition to the current process where notifications of employee terminations are sent to our Security team in real time and also audits are performed weekly based off of a list from our HRMS Workday of the prior week's terminations, we plan to institute a new process. By the end of every month, our HR Shared Services team will pull a report of all active employees for our Security team. By the 5th of the next month, the security team will run an audit on all active badges to ensure that only active employees are assigned active badges. This process became active on April 5, 2014. The first active employee report was run out of Workday in April, 2014. The results of this report were compared to the active badge report in CCure. 59 discrepancies were identified which signaled a data problem in the CCure system. All 59 discrepancies were corrected in CCure after validating the Workday information. The Workday and CCure systems now match and show consistent information. See Attachment 1.

### 2. Password Configuration Settings

**Recommendation 2**

We recommend that BSC configure the mainframe password settings to conform to its corporate password standard.

**Plan Response**

The Plan contests this recommendation. BSC's password standard requires users to maintain passwords that conform to a variety of requirements, such as minimum length and complexity. However, the mainframe only enforces selected password requirements. BSC completed a risk assessment that considered the mainframe's password configuration capabilities and concluded that the risk associated with the potential variance between BSC standards and the mainframe password configuration does not warrant modifying the mainframe's password enforcement configuration. See Attachment 2.

## C. Network Security

### 1. Vulnerability Management Program

**Recommendation 3**

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

**Plan Response**

The Plan agrees with this recommendation. BSC will ensure all servers are included in the routine vulnerability scanning, including those housing Federal employee plan data, effective May 31, 2014.

**Recommendation 4**

We recommend that BSC implement policies and procedures to ensure that all vulnerabilities identified from network vulnerability scans are tracked and remediated in a timely manner.

**Plan Response**

The Plan agrees with this recommendation. BSC will enhance policies and procedures to ensure vulnerabilities are appropriately addressed commensurate with their level of risk, by August 31, 2014.

### 2. Firewall Management

**Recommendation 5**

We recommend that BSC document formal firewall management policies.

**Plan Response**

The Plan agrees with this recommendation. BSC will enhance firewall management policies as recommended by September 30, 2014.

**Recommendation 6**

We recommend that BSC implement a process to [redacted] as defined by the organizational policies.

**Plan Response**

The Plan agrees with this recommendation. BSC will enhance processes [redacted] as recommended by March 31, 2015.

### 4. General and Privileged User Access Monitoring

**Recommendation 7**

We recommend that BSC implement a process to [redacted]

**Plan Response**

The Plan agrees with this recommendation. BSC will complete an in-progress project to [redacted] by March 31, 2015.

## D. Configuration Management

### 1. Baseline Configuration Policy

**Recommendation 8**

We recommend that BSC document approved security configuration settings/baselines for all network server operating systems.

**Plan Response**

The Plan agrees with this recommendation. At the time of the audit, BSC was in the process of implementing new security configuration baselines. BSC has updated security configuration baselines, established a process for maintaining them on an ongoing basis and will continue to refine them to reflect BSC-specific settings. See Attachment 3. See Attachment 4 for a copy of Win2008 Server Security Baseline.

### 2. Configuration Compliance Auditing

**Recommendation 9**

We recommend that BSC routinely audit security configurations settings using approved baselines.

**Plan Response**

The Plan agrees with this recommendation. BSC routinely audits security configuration settings against both industry and BSC-specific standards. BSC will complete the activities to ensure all servers are covered by these audits by May 31, 2014.

## F. Claims Adjudication

### 1. Application Configuration Management

**Recommendation 10**

We recommend that BSC ensure that all changes made to application systems are documented and approved in accordance to the corporate application management policy.

**Plan Response**

The Plan agrees with this recommendation. At the time of the audit, BSC was in the process of implementing a new tool for managing application change. This implementation has completed and ensures changes are documented and approved per the application management policy. See Attachment 5.

### 4. Debarment

**Recommendation 11**

We recommend that BSC implement process to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate for both the HMO and PPO plans.

**Plan Response**

HMO response - Plan agrees with this recommendation.

The Plan will implement debarment processes outlined by OIG's "Guidelines for Implementation of FEHBP Debarment and Suspension Orders" by the end of August 2014. Actions include implementation of quarterly audit, updated debarment procedure guide, and appropriate claims adjudication practices.

### 5. Application Control Testing

### a. Medical Editing

**Recommendation 14**

We recommend that BSC make the appropriate system modifications to prevent [redacted]

**Plan Response**

***Section deleted by OIG because it is not relevant to the final report***

**BCBSA Response**

The FEP Claims system will be modified by 2nd quarter 2014 to perform certain types of medical editing. See Attachment 6 for a monthly update provided to the Contracting Office, describing the progress of this project.

### b. Near Duplicates

**Recommendation 15**

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

**Plan Response**

***Section deleted by OIG because it is not relevant to the final report***

**BCBSA Response**

An enhancement request was submitted to the FEP Operations Center on March 6, 2014 to enhance the national FEP Claims system to implement system modifications to [redacted] from processing. See Attachment 7, Request # 20141648 and 20141651. We will provide an update on this recommendation once feedback on the request is obtained.

### c. Procedure Code Billing Guidelines Not Enforced

**Recommendation 16**

We recommend that BSC make the appropriate system modifications to enforce proper procedure code billing guidelines.

**Plan Response**

***Section deleted by OIG because it is not relevant to the final report***

**BCBSA Response**

An enhancement request was submitted to the FEP Operations Center on March 6, 2014 to limit certain types of services. See Attachment 7, Request #20141652-54. We will provide an update on this recommendation once feedback on the request is obtained.

Thank you for the opportunity to provide an update to the Final Report. If you have any questions in the interim, please contact [redacted] at [redacted]

Sincerely,

[redacted], CISA, CRSA
Managing Director, FEP Program Assurance

Attachments

cc: [redacted], BSC
[redacted] OPM
[redacted], FEP