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 BLUECROSS BLUESHIELD OF SOUTH CAROLINA

Report No. 1A-10-24-11-014

Date: 11/09/11

--CAUTION--

This audit report has been distributed to Federal and Non-Federal officials who are responsible for the administration of the audited contract. 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

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT CS 1039

BLUECROSS BLUESHIELD OF SOUTH CAROLINA
PLAN CODES 380 / 880

COLUMBIA, SOUTH CAROLINA

Report No. 1A-10-24-11-014

Date: 11/09/11

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

**FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT CS 1039**

**BLUECROSS BLUESHIELD OF SOUTH CAROLINA
PLAN CODES 380 / 880**

COLUMBIA, SOUTH CAROLINA

Report No. 1A-10-24-11-014

Date: 11/09/11

This final report discusses the results of our audit of general and application controls over the information systems at BlueCross BlueShield of South Carolina (BCBSSC).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for BCBSSC, 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

BCBSSC has established a comprehensive series of IT policies and procedures to create an awareness of IT security at the Plan. We also verified that BCBSSC has a thorough risk management methodology and adequate security-related human resources policies.

Access Controls

We found that BCBSSC has implemented numerous physical controls to prevent unauthorized access to its facilities, as well as logical controls to prevent unauthorized access to its information systems. However, we have found the following controls could use improvement:

- Segregation of duties;
- Logical access privileges approval and review;
- Tracking weaknesses identified in vulnerability scans;
- Email encryption;
- Laptop encryption; and,
- Network port scanning.

Configuration Management

BCBSSC has developed formal policies and procedures providing guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes.

Contingency Planning

We reviewed BCBSSC'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, updated, and tested on a periodic basis. However, BCBSSC stores its data backup tapes at a location near the data center that could be potentially impacted by the same disruptions.

Application Controls

BCBSSC has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we recommended that BCBSSC implement several system modifications to ensure that its claims processing systems adjudicate FEHBP claims in a manner consistent with the OPM contract and other regulations.

Health Insurance Portability and Accountability Act (HIPAA)

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

Contents

Page

Executive Summary i

I. Introduction 1

Background 1

Objectives 1

Scope 2

Methodology 2

Compliance with Laws and Regulations 3

II. Audit Findings and Recommendations 4

A. Security Management 4

B. Access Controls 4

C. Configuration Management 9

D. Contingency Planning 10

E. Application Controls 11

F. Health Insurance Portability and Accountability Act 16

III. Major Contributors to This Report 17

Appendix: BlueCross BlueShield Association's June 28, 2011 response to the draft audit report issued April 19, 2011.

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 BlueCross BlueShield of South Carolina (BCBSSC).

The audit was conducted pursuant to FEHBP contract 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 first audit of BCBSSC's general and application controls. We also reviewed BCBSSC's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All BCBSSC personnel that worked with the auditors were particularly 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 BCBSSC's 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 BCBSSC's claims processing systems; and,
- 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 BCBSSC’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 BCBSSC’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 BCBSSC to process medical insurance claims for FEHBP members, with a primary focus on the [redacted] and FEP Direct claims adjudication applications. The business processes reviewed are primarily located in BCBSSC’s Columbia, South Carolina facility.

The on-site portion of this audit was performed in February and March of 2011. 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 BCBSSC as of April 8, 2011.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSSC. 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 audit, we:

- Gathered documentation and conducted interviews;
- Reviewed BCBSSC’s business structure and environment;
- Performed a risk assessment of BCBSSC’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 evaluating BCBSSC’s control structure. This criteria includes, but is not limited to, the following publications:

- Title 48 of the Code of Federal Regulations (CFR);
- 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, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- 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 BCBSSC’s practices were consistent with applicable standards. While generally compliant, with respect to the items tested, BCBSSC 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 BCBSSC's overall IT security controls. We evaluated BCBSSC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSSC has implemented a series of formal policies and procedures that comprise a comprehensive security management program. BCBSSC's security management program is led by the company's Security Council; their responsibilities include creating policies to protect against threats or improper use of sensitive data, HIPAA compliance, and to provide central governance and coordination. BCBSSC has also developed a thorough risk management methodology, and has procedures to document, track, and alleviate or accept identified risks. We also reviewed BCBSSC's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

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

B. Access Controls

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

We examined the physical access controls of the several BCBSSC office buildings, data centers, tape vaults, and print facilities.

We also examined the logical controls protecting sensitive data in BCBSSC's network environment and claims processing related applications.

The access controls observed during this audit included, but were not limited to:

- Procedures for appropriately granting and revoking physical access privileges to the data centers;
- Multi-factor authentication requirements to enter the data center, print center, and tape vault;
- Use of intrusion detection and prevention techniques;
- Use of software tools to monitor and filter email and Internet activity; and,
- Strict identification and authentication requirements to access networks and applications.

However, the sections below document several opportunities for improvement related to BCBSSC's physical and logical access controls.

a) [redacted]

Twenty-five BCBSSC application programmers have administrator level access to the security tables governing access to the production claims processing environment. This access allows the programmers to grant themselves (and others) unrestricted access to [redacted] application data.

Failure to implement adequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, or that computer resources could be damaged or destroyed. FISCAM section 3.4 states that "Work responsibilities should be segregated so that one individual does not control all critical stages of a process." FISCAM also states that "Programmers should not be responsible for moving programs into production or have access to production libraries or data."

Recommendation 1

We recommend that BCBSSC remove all application programmers' [redacted] user accounts in the production application as well as their administrator rights to [redacted] security tables.

BCBSSC Response:

"The Plan agrees with this finding. BCBSSC will remove all application programmers' [redacted] user accounts from the production application access lists as well as their administrator rights to production [redacted] security tables. [redacted] and Data Security Management are developing a process that will allow programmers the ability to access the production [redacted] application on an as needed basis to resolve emergency production issues. The anticipated completion date for this project is 4th quarter 2011. Research and changes are required to assure that the application programmers can keep their test application security access when removed from the production application security tables."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that they have removed all application programmers' [redacted] user accounts in the production application as well as their administrator rights to security tables.

b) Logical Access Privileges Approval and Review

The BCBSSC Information Assurance Group (IAG) routinely facilitates an [redacted] access "recertification." IAG distributes lists of active [redacted] user accounts to business unit managers who must certify that their employees continue to require access to the application.

Although the recertification process verifies that users still need access to [redacted] managers are not required to verify that the specific application transactions/features that each user has access to are appropriate for that individual.

We also conducted a test to determine whether a user's initial system access was approved by that user's manager. We requested a sample of information system access request forms for employees who have active access to the claims processing system. However, the Plan was unable to retrieve the majority of requested access request forms, and we were unable to verify that these employees' system access was ever officially approved. The risk that these individuals have inappropriate access would be remediated by a recertification process that includes a transaction-level review.

FISCAM critical element AC-3.1 states the computer resource owner should "identify the nature and extent of access to each resource that is available to each user . . . . Access may be permitted at the file, record, or field level . . . . Owners should periodically review access authorization listings and determine whether they remain appropriate. Access authorizations should be documented on standard forms and maintained on file."

Failure to routinely recertify the appropriateness of transaction-level access could allow employees to perform functions or access sensitive information that they should not have approval to access.

<u>Recommendation 2</u>

We recommend that BCBSSC modify the [redacted] recertification process to include verification that the specific application transactions/features that each user has access to is appropriate for that individual.

<u>BCBSSC Response:</u>

"The Plan indicated that the application level security is the primary mechanism used to control access to [redacted] data and functions. Managers are responsible for requesting the required access for their employees to perform routine job functions and responsibilities.

Information System (I/S) areas of responsibility is to work with Corporate Audit IAG to enhance the current quarterly [redacted] application access recertification. Enhancements will include providing each manager with more information to determine if the level of access assigned is appropriate. First, the Plan's I/S staff must complete the design signoff and determine the cost of the project. Once the cost has been determined, a request for funding approval will be submitted to FEP. [The scheduled] completion date for these activities [is] 4th Quarter 2011."

<u>OIG Reply:</u>

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that the appropriate modifications to the current quarterly [redacted] application access recertification have been completed.

c) Tracking Weaknesses Identified in Vulnerability Scans

BCBSSC conducts vulnerability scans of its servers [redacted] using [redacted] [redacted]. The group scans [redacted] and uses a device matrix to ensure that all devices are included [redacted]. The results of the vulnerability scans are entered into a vulnerability matrix and forwarded to the appropriate system administrators for remediation.

When the Plan determines that a system change should be implemented to address a vulnerability, the BCBSSC change management process is used to track the modification (see section C). However, if a system change is not immediately implemented, BCBSSC does not currently have a process to continuously track the status (i.e., false positive, risk accepted, etc.) of all other items contained within the vulnerability matrix. BCBSSC is planning to purchase [redacted] and track the status of each vulnerability identified.

FISCAM critical element SM-6 states that "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. Procedures should be established to reasonably assure that all IS control weaknesses, regardless of how or by whom they are identified, are included in the entity's remediation processes."

Failure to continuously track the status of all issues identified during vulnerability scanning could result in system weaknesses being overlooked, increasing the risk of a successful system attack.

Recommendation 3

We recommend that BCBSSC continue its efforts to develop a methodology to track the current status of all potential weaknesses identified during vulnerability scans.

BCBSSC Response:

"The Plan agrees with this finding and will continue to develop a methodology to track the current status of potential weaknesses identified through vulnerability scans. The target completion date is the 4th Quarter 2011."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that the Plan has developed a methodology to track the current status of all potential weaknesses identified during vulnerability scans.

d) Email Encryption

BCBSSC has implemented an email encryption policy that requires the encryption of all messages sent outside of the corporate email system that contain sensitive, confidential, or protected health information (PHI). BCBSSC uses [redacted] to secure email messages. In order to encrypt an outgoing email message, users manually include the word "secure" in the subject line of the e-mail. However, [redacted] is not currently configured to scan the content of emails and attachments and automatically encrypt emails containing sensitive information.

HIPAA Security Standards § 164.312(a) (2) (iv) states that covered entities must "Implement a mechanism to encrypt and decrypt electronic protected health information." The lack of controls to automatically encrypt outgoing email messages increases the risk of BCBSSC employees sending insecure emails containing sensitive information.

Recommendation 4

We recommend that BCBSSC configure ProofPoint to automatically scan and encrypt all outgoing email that contains sensitive information.

BCBSSC Response:

"The Plan agrees with this finding. There is currently a project under way to configure and implement this functionality for email across all lines of business. The completion date for this project cannot be determined until certain phases of these activities have been completed. The target completion date is the 4th Quarter 2011."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that ProofPoint has been configured to automatically scan and encrypt all outgoing email that contains sensitive information.

e) Laptop Encryption

BCBSSC has not implemented encryption controls on all laptops issued to employees.

The current BCBSSC policy for laptop encryption states that the hard drive must be encrypted if it contains PHI and is transported outside of the BCBSSC facility. The policy is currently being revised to state that all laptop hard drives must be encrypted regardless of location.

We reviewed an inventory of BCBSSC laptops that listed the employee to which each laptop is assigned and type of hard drive encryption implemented. Out of the 844 laptops on the inventory, 250 are not encrypted.

HIPAA Security Standards § 164.312(a) (2) (iv) states that covered entities must "Implement a mechanism to encrypt and decrypt electronic protected health information." NIST 800-53 requires that the information system use cryptographic mechanisms to protect and restrict access to information on portable digital media. Failure to encrypt all laptop hard drives increases the risk that unauthorized individuals could gain access to sensitive information.

Recommendation 5

We recommend that BCBSSC implement encryption controls on all company issued laptops.

BCBSSC Response:

"The Plan agrees with this finding. Encryption controls have already been deployed to all company issued laptops that reside on Medicare networks. A project is under way to extend

this functionality to all remaining company issued laptops. Target completion date is July 31, 2011. Once this project is completed, documentation to support the action taken will be provided to OPM."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that BCBSSC has implemented encryption controls on all company issued laptops.

f) Network Port Scanning

BCBSSC has implemented thorough intrusion detection and incident response capabilities to protect its network from external threats. However, the Plan has not implemented technical controls to identify [redacted].

NIST SP 800-53 Rev 3 requires that an information system uniquely identify and authenticate before establishing a connection. Section IA-3 of the NIST guide states that the information system should uniquely identify and authenticate devices before establishing a connection. Failure to continuously scan the network for rogue devices could allow someone with physical access to BCBSSC facilities to connect an unauthorized device to the Plan's network.

Recommendation 6

We recommend that BCBSSC implement controls to continuously scan active ports in its network environment [redacted].

BCBSSC Response:

"The Plan agrees with this finding. A review of the recommended adoption of Network Access Control technology is currently in process. Once the review has been complete and the project cost is determine, a request for funding approval will be sent to FEP. The anticipated completion date for this project is 1st Quarter 2012."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSSC provide OPM's Audit Resolution group with evidence that BCBSSC has implemented controls to continuously scan active ports in its network environment [redacted].

C. Configuration Management

BCBSSC's local claims adjudication system, [redacted] is housed on a mainframe environment with the [redacted] and access controls managed by [redacted] We evaluated BCBSSC's management of the configuration of the system software housing [redacted] and determined that the following controls were in place:

- Policies and procedures for ensuring that operating platforms are securely configured;

- Controls for securely managing changes to the operating platform and claims processing application;
- Controls for monitoring privileged user activity on the operating platform;
- Procedures for routinely updating and patching the operating platforms; and,
- Procedures for monitoring configuration through vulnerability scans.

Nothing came to our attention to indicate that BCBSSC does not have adequate controls related to configuration management.

D. Contingency Planning

We reviewed BCBSSC's contingency planning program to determine whether it contained adequate procedures and controls for maintaining critical services for its customers should business operations be disrupted. The following elements of BCBSSC's contingency planning program were reviewed:

- Business continuity plans for several business units including claims processing, data center operations, print operations, mail services, and customer care;
- Disaster recovery plan for the [redacted] claims processing system;
- Disaster recovery plan for the [redacted] database; and,
- Emergency response procedures and training.

Although BCBSSC has implemented a thorough contingency planning program, we did note one opportunity for improvement in this area.

a) Location of Backup Tape Vault

BCBSSC stores its backup data tapes in a vault that is not an adequate distance away from the primary data center.

BCBSSC has a "hot site" available in another state that has the infrastructure in place to quickly restore the Plan's critical information systems in the event that the primary data center is disrupted. However, the data tapes required to recover these systems are stored in a vault that is less than 4 miles away from the data center housing the production systems. In the event of a disaster, BCBSSC would load the tapes into a truck and drive them to the hot site.

The fact that BCBSSC has procured a disaster recovery hot site indicates that they understand the risks that a disruptive event (natural disaster, hazardous material spill, widespread power outages, etc.) could render the data center inaccessible. It is reasonable to expect that such an event could also impact the nearby tape vault facility or the route from the tape vault to the hot site.

NIST SP 800-34 Section 3.41 suggests that "When selecting an offsite storage facility and vendor, the following criteria should be considered . . . Geographic area - distance from the organization and the probability of the storage site being affected by the same disaster as the organization."

We believe that the tape vaulting methodology implemented by BCBSSC is notably weaker than the controls in place at other FEHBP carriers visited by the OIG. Many other Plans utilize modern technology such as electronic vaulting, real-time data mirroring, or at a minimum contract with an outside company that has the infrastructure to adequately manage their data tapes.

Recommendation 7

We recommend BCBSSC reevaluate its methodology for storing data tapes off-site and consider implementing the additional controls typically found at other FEHBP insurance carriers.

BCBSSC Response:

"Information has not been provided to BCBSSC regarding the controls in place at other FEHBP carriers. The NIST SP 800-34 Section 3.41 standards do not contain definitive criteria as to the location of the vault. In addition, BCBSSC is audited by numerous external agencies annually with no findings relative to the vault location.

BCBSSC will, based upon the recommendation of this report, commence an effort, with approval by the FEPDO, to review alternative methodologies as recommended by the auditors. Once identified, a plan of action can be developed based on the options determined appropriate by FEPDO and BCBSSC. The target completion date for this project is the 3rd Quarter 2011.

OIG Reply

Although NIST SP 800-34 does not contain definitive criteria as to the location of a tape vault, it does state that the probability of the storage site being affected by the same disaster as the data center should be considered. We continue to believe that it is reasonable to expect that a single disruptive even could impact BCBSSC's data center and tape vault.

As part of the audit resolution process, we recommend that BCBSSC update OPM's Audit Resolution group with evidence it has considered alternative storage methodologies and developed appropriate plans of action.

E. Application Controls

Application Configuration Management

The OIG evaluated the policies and procedures governing software development and change control of the BCBSSC's [redacted] claims processing application.

BCBSSC has an extensive Information Systems Standards Manual which contains detailed policies and procedures related to application configuration management. BCBSSC has adopted a traditional system development life cycle methodology that IT personnel follow during routine software modifications. The following controls related to testing and approvals of software modifications were observed:

- BCBSSC 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,
- BCBSSC utilizes a tool called [redacted] to move the code between software libraries and ensure adequate segregation of duties.

Claims Processing System

The OIG evaluated the input, processing, and output controls associated with [redacted] In terms of input controls, the OIG documented the policies and procedures adopted by BCBSSC to help ensure that: 1) there are controls over the inception of claims data into the system; 2) the data received comes from the appropriate sources; and 3) the data is entered into the claims database correctly. We also reviewed BCBSSC's quality assurance methods for reconciling processing totals against input totals and for evaluating the accuracy of its processes. Finally, we examined the security of physical input and output (paper claims, checks, explanation of benefits, etc.).

Debarment

The OIG evaluated the policies and procedures governing BCBSSC's debarment process. We determined that BCBSSC meets the OPM OIG guidelines with regard to routinely acquiring and updating debarment files, as well as making reasonable efforts to preclude further payment of claims for items or services rendered after the date of debarment or suspension.

However, we noted one area for improvement within the debarment process.

a) Auditing of Debarment Database

BCBSSC uses a manual process to flag debarred providers in its provider database. Although the procedures for updating the database appeared thorough, any manual process is prone to error. At the beginning of this audit, BCBSSC did not have any procedures for routinely auditing the debarment database for accuracy, increasing the risk that errors would remain undetected indefinitely.

During the fieldwork phase of this audit, BCBSSC implemented new procedures that require a manager to audit updates to the provider database on a monthly basis.

<u>Recommendation 8</u>

We recommend that BCBSSC provide evidence that the monthly audits have been conducted in accordance with the new procedures.

<u>BCBSSC Response:</u>

"The Plan agrees with this recommendation and has implemented new procedures that require management to audit updates to the provider data base on a monthly basis.

Attachment Recommendation # 8 is a copy of the most current report that has been reviewed to ensure the data base was updated accurately. The initials of management staff are noted on each report.”

OIG Reply:

This evidence provided by BCBSSC indicates that the Plan now conducts monthly audits in accordance with its new procedures; no further action is required.

Special Investigations and Fraud

The OIG evaluated the BSBCSC policies and procedures governing special investigations and fraud. We determined that BCBSSC has substantial policies and procedures in place to detect, manage, and report fraud. There were no areas of improvement noted during our review.

Application Controls Testing

To validate the claims processing controls, a testing exercise was conducted on the BCBSSC local [redacted] system and the BCBSA’s FEP Express system that is used to process claims from all BCBS plans. This test was conducted at BCBSSC’s Columbia, South Carolina facility with the assistance of BCBSSC personnel. The exercise involved processing claims designed with inherent flaws in the test environment of the claims adjudication applications. Upon conclusion of the testing exercise, the expected results were compared with the actual results obtained during the exercise.

The sections below document the opportunities for improvement that were noted related to application controls.

a) Chiropractor Claims

The [redacted] system automatically denied claims for services rendered by a chiropractor within the scope of his license.

The OIG entered a test claim into [redacted] with an ankle x-ray procedure and an ankle fracture diagnosis. A chiropractor license in South Carolina allows the provider to perform ankle x-rays, but [redacted] denied this claim because the diagnosis code was invalid for a chiropractor. In this scenario, a chiropractor would be unable to determine the diagnosis until after the procedure was already performed.

The existence of this denial edit increases the risk that chiropractors will not get paid for performing an ankle x-ray and that members will be held liable for this service that should be a covered benefit.

Recommendation 9

We recommend that BCBSSC make the appropriate system modifications to ensure that ankle x-rays performed by a chiropractor are not denied because of an invalid diagnosis.

__BCBSSC Response:__

"BCBSSC agrees with this recommendation and has made the appropriate modification to its benefit files table which did not require a change sheet on March 31, 2011 to ensure that ankle x-rays performed by a chiropractor are not denied because of an invalid diagnosis. Attachment Recommendation # 9 is the support documenting that the system correction was implemented in the Plan's local system."

__OIG Reply:__

This evidence provided by BCBSSC indicates that the Plan has made appropriate modifications to ensure that ankle x-rays performed by chiropractors are not denied because of an invalid diagnosis; no further action is required.

b) Procedure to Diagnosis Inconsistency Claims

A test claim was processed where benefits were paid for a procedure associated with an inappropriate diagnosis.

The OIG entered a test claim into [redacted] with a procedure code [redacted] and a diagnosis of a [redacted]. Despite the procedure/diagnosis inconsistency, the claim processed through the local system without encountering any edits and was sent to FEP Express. FEP Express also processed and paid the claim.

This system weakness increases the risk that benefits are being paid for procedures associated with a diagnosis that may not warrant such treatment.

Multiple OIG audits of other BCBS plans have detected a variety of weaknesses and inconsistencies between the plans' medical edit capabilities. We believe that comprehensive medical edit software is needed for FEP Express to ensure that all BCBS claims are subject to the same level of quality control.

__Recommendation 10__

We recommend that BCBSA implement comprehensive medical edit software on FEP Express.

__BCBSSC Response:__

"In order to comply with the recommendation, BCBSA will issue a Request for Information to obtain additional information on the types of medical edit software packages available for implementation in the FEP Claims System by July 2011. Once responses have been received, a determination will be made as to whether FEP will implement a commercial software package or develop the medical edits internally."

__OIG Reply:__

As part of the audit resolution process, we recommend that BCBSSC continue to provide OPM's Audit Resolution group with evidence of its progress in implementing comprehensive medical edits on FEP Express.

c) [redacted] Modifier Claims

A test claim was processed where [redacted] was automatically altered by [redacted] to include an additional modifier.

The OIG entered two test claims with different [redacted] applied to each claim. An [redacted] indicates a [redacted] assisted with [redacted] whereas an [redacted] modifier indicates another [redacted] assisted with the [redacted]. The test claim with only an [redacted] modifier claim was automatically adjusted by [redacted] to include *both* modifiers before sending the claim to FEP Express. As a result, the claim with an [redacted]' modifier was priced as though it had an [redacted] modifier.

These test claims were subject to OBRA 93 pricing because the members had Medicare A but no Medicare B coverage. We understand that the current FEP Express test environment must simulate the pricing of OBRA93 claims because the OBRA93 pricing vendor does not have a functional test environment. However, the risk remains that the production environment of the OBRA93 pricer could price the claims incorrectly because the BCBS systems are providing it with the incorrect modifier code.

Recommendation 11

We recommend that BCBSSC make the appropriate system modifications to ensure that its system does not make adjustments to assistant surgeon modifier codes.

BCBSSC Response:

"The Plan agrees with the recommendation and implemented the required system modifications to correct this exception on April 9, 2011. Attachment Recommendation # 11 is the support documenting that the change was implemented in the Plan's local system."

OIG Reply:

This evidence provided by BCBSSC indicates that the Plan has made the appropriate system modifications to ensure that its system does not make adjustments to assistant surgeon modifier codes and that it addresses the recommendation; no further action is required.

d) Pricing of [redacted] Claims

Test claims for [redacted] were paid incorrectly.

The BCBS benefit structure states that preventative care [redacted] are a covered benefit for females age 60 and over. This benefit would not be covered for females under 60.

The OIG entered several test claims for osteoporosis screenings for individuals both over and under the age of 60 receiving [redacted]. The [redacted] System processed and priced all claims the same regardless of the member's age.

This system weakness increases the risk that the Plan is paying benefits in excess of what is allowed. BCBSSC stated that they have reported this issue to the BCBS FEP Operations Center for correction.

Recommendation 12

We recommend that BCBSSC make the appropriate system modifications to ensure that [redacted] are being paid in accordance with the benefit structure.

BCBSSC Response:

"After the implementation of the 2011 Benefit changes, it was discovered that the [redacted] was not administered correctly in FEPExpress. A claims system modification to correct processing of [redacted] was implemented on May 26, 2011. Attachment Recommendation # 12 provides support for this change in the FEP Claims System."

OIG Reply:

This evidence provided by BCBSSC indicates that the Plan has made the appropriate system modifications to ensure that [redacted] are being paid in accordance with the benefit structure; no further action is required.

F. Health Insurance Portability and Accountability Act

The OIG reviewed BCBSSC's efforts to maintain compliance with the security and privacy HIPAA standards.

BCBSSC has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. BCBSSC has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. Each line of business, subsidiary, and some individual departments have designated a Privacy Official who has the responsibility of ensuring their area is compliant with HIPAA privacy regulations. BCBSSC employees receive HIPAA-related training during new hire orientation, as well as annual refresher training.

Nothing came to our attention that caused us to believe that BCBSSC is not in compliance with 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]r, Group Chief
- [redacted], Senior Team Leader
- [redacted], IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

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 28, 2011

[redacted] Chief
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
South Carolina Blue Cross Blue Shield
Audit Report Number 1A-10-24-11-014

Dear [redacted]:

This letter 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 South Carolina Blue Cross Blue Shield Plan's interface with the FEP claims processing system, access and security controls. Our comments regarding the findings in the report are as follows:

A. <u>ACCESS CONTROLS</u>

a) Segregation of Duties

<u>Recommendation 1</u>

The OIG Auditors recommended that BCBSSC remove all application programmers' [redacted] user accounts in the production application as well as their administrator rights to [redacted] security tables.

<u>Response to Recommendation 1</u>

The Plan agrees with this finding. BCBSSC will remove all application programmers' [redacted] user accounts from the production application access lists as well as their administrator rights to production [redacted] security tables. [redacted] and Data Security Management are developing a process that will allow programmers the ability to access the production [redacted] application on an as needed basis to resolve emergency production issues. The anticipated completion date for this project is 4th quarter 2011. Research and changes are required to assure that the application programmers can keep their test application security access when removed from the production application security tables.

b) Access Logical Privileges Approval and Review

Recommendation 2

The OIG Auditors recommended that BCBSSC modify the [redacted] recertification process to include verification that the specific application transactions/features that each user has access to is appropriate for that individual.

Response to Recommendation 2

The Plan indicated that the application level security is the primary mechanism used to control access to [redacted] data and functions. Managers are responsible for requesting the required access for their employees to perform routine job functions and responsibilities.

Information System (I/S) areas of responsibility is to work with Corporate Audit IAG to enhance the current quarterly [redacted] application access recertification. Enhancements will include providing each manager with more information to determine if the level of access assigned is appropriate. First, the Plan's I/S staff must complete the design signoff and determine the cost of the project. Once the cost has been determined, a request for funding approval will be submitted to FEP. It is completion date for these activities 4th Quarter 2011.

c) Tracking Weaknesses Identified in Vulnerability Scans

Recommendation 3

The OIG Auditors recommended that BCBSSC continue its efforts to develop a methodology to track the current status of all potential weaknesses identified during vulnerability scan weaknesses.

Response to Recommendation 3

The Plan agrees with this finding and will continue to develop a methodology to track the current status of potential weaknesses identified through vulnerability scans. The target completion date is the 4th Quarter 2011.

Email Encryption

Recommendation 4

The OIG Auditors recommended that BCBSSC configure [redacted] to automatically scan and encrypt all outgoing email that contains sensitive information.

Response to Recommendation 4

The Plan agrees with this finding. There is currently a project under way to configure and implement this functionality for email across all lines of business. The completion date for this project cannot be determined until certain phases of these activities have been completed. The target completion date is the 4th Quarter 2011.

d) Laptop Encryption

Recommendation 5

The OIG Auditors recommended that BCBSSC implement encryption controls on all company issued laptops.

Response to Recommendation 5

The Plan agrees with this finding. Encryption controls have already been deployed to all company issued laptops that reside on Medicare networks. A project is under way to extend this functionality to all remaining company issued laptops. Target completion date is July 31, 2011. Once this project is completed, documentation to support the action taken will be provided to OPM.

e) Network Port Scanning

Recommendation 6

The OIG Auditors recommended that BCBSSC implement controls to continuously scan active ports in its network environment for [redacted].

Response to Recommendation 6

The Plan agrees with this finding. A review of the recommended adoption of Network Access Control technology is currently in process. Once the review has been complete and the project cost is determine, a request for funding approval will be sent to FEP. The anticipated completion date for this project is 1st Quarter 2012.

B. Configuration Management

a) Location of Backup Tape Vault

Recommendation 7

The OIG Auditors recommended that BCBSSC re-evaluate its methodology for storing data tapes off-site and consider implementing the additional controls typically found at other FEHBP insurance carriers.

Response to Recommendation 7

Information has not been provided to BCBSSC regarding the controls in place at other FEHBP carriers. The NIST SP 800-34 Section 3.41 standards do not contain definitive criteria as to the location of the vault. In addition, BCBSSC is audited by numerous external agencies annually with no findings relative to the vault location.

BCBSSC will, based upon the recommendation of this report, commence an effort, with approval by the FEPDO, to review alternative methodologies as recommended by the auditors. Once identified, a plan of action can be developed based on the options determined appropriate by FEPDO and BCBSSC. The target completion date for this project is the 3rd Quarter 2011.

BCBSSC's tape storage process does not impact the FEP Portability Project. There are no tapes used for transferring FEP data to and from the CareFirst data center to the Contingency environment at Blue Cross and Blue Shield of South Carolina. The transmission of this data used to recover the environment is electronic over a dedicated circuit between the CareFirst data center and the BCBSSC facility. Upon declaration of a triggering event, data would be transmitted over this dedicated circuit to BCBSSC and BCBSSC would recover the environment using this data.

C. Claims Adjudication

Debarment

a) Auditing of Debarment Database

Recommendation 8

The OIG Auditors acknowledge the steps that BCBSSC has taken to address this recommendation. As part of the audit resolution process, we recommend that BCBSSC provide Healthcare and Insurance Office (HIO) with evidence that the monthly audits have been conducted in accordance with the new procedures.

Response to Recommendation 8

The Plan agrees with this recommendation and has implemented new procedures that require management to audit updates to the provider data base on a monthly basis. Attachment Recommendation # 8 is a copy of the most current report that has been reviewed to ensure the data base was updated accurately. The initials of management staff are noted on each report.

Application Controls Testing

a) Chiropractor Claims

Recommendation 9

The OIG recommended that BCBSSC make the appropriate system modifications to ensure that ankle x-rays performed by a chiropractor are not denied because of an invalid diagnosis.

Response to Recommendation 9

BCBSSC agrees with this recommendation and has made the appropriate modification to its benefit files table which did not require a change sheet on March 31, 2011 to ensure that ankle x-rays performed by a chiropractor are not denied because of an invalid diagnosis. Attachment Recommendation # 9 is the support documenting that the system correction was implemented in the Plan's local system.

b) Procedure to Diagnosis Inconsistency Claims

Recommendation 10

The OIG Auditors recommended that BCBSA implement comprehensive medical edit software on FEP Express.

Response to Recommendation 10

In order to comply with the recommendation, BCBSA will issue a Request for Information to obtain additional information on the types of medical edit software packages available for implementation in the FEP Claims System by July 2011. Once responses have been received, a determination will be made as to whether FEP will implement a commercial software package or develop the medical edits internally.

c) [redacted] Modifier Claims

<u>Recommendation 11</u>

The OIG Auditors recommended that BCBSSC make the appropriate system modifications to ensure that its system does not make adjustments to [redacted] modifier codes.

<u>Response to Recommendation 11</u>

The Plan agrees with the recommendation and implemented the required system modifications to correct this exception on April 9, 2011. Attachment Recommendation # 11 is the support documenting that the change was implemented in the Plan's local system.

d) Pricing of [redacted] Screening Claims

<u>Recommendation 12</u>

The OIG Auditors recommend that BCBSSC make the appropriate system modifications to ensure that [redacted]benefits are being paid in accordance with the benefit structure.

<u>Response to Recommendation 12</u>

After the implementation of the 2011 Benefit changes, it was discovered that the [redacted] was not administered correctly in FEPExpress. A claims system modification to correct processing of [redacted] claims was implemented on May 26, 2011. Attachment Recommendation # 12 provides support for this change in the FEP Claims System.

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] Executive Director
Program Integrity

[redacted]

Attachments (4)

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