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 FLORIDA

Report No. 1A-10-41-09-063

Date: May 21, 2010

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 FLORIDA
PLAN CODES 090/590
JACKSONVILLE, FLORIDA

Report No. 1A-10-41-09-063

Date: May 21, 2010

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 FLORIDA
PLAN CODES 090/590
JACKSONVILLE, FLORIDA

Report No. 1A-10-41-09-063

Date: May 21, 2010

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

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

BCBSFL has established a comprehensive series of IT policies and procedures to create an awareness of IT security at the Plan. We verified that BCBSFL's policies and procedures are maintained on the Plan's intranet site in a manner that is easily accessible by employees.

Access Controls

We found that BCBSFL 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, the logical access controls for one application critical to the claims adjudication process could be improved. In addition, BCBSFL is analyzing the effectiveness of its current controls related to the secure transmission of electronic data.

Configuration Management

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

Application Controls

BCBSFL has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we recommended that BCBSFL 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 BCBSFL is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Contents

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 at BlueCross BlueShield of Florida (BCBSFL or Plan).

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

Background

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

BCBSFL headquarters is located in Jacksonville, Florida. Employees responsible for processing FEHBP (also, Federal Employee Program or FEP) claims are also located in Jacksonville, Florida.

This was the OIG's second audit of general and application controls at BCBSFL. During this audit we verified that the audit findings from the first audit, conducted in 2003, have been closed.

All BCBSFL 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 BCBSFL's IT environment.

These objectives were accomplished by reviewing the following areas:

- Security management;
- Access controls;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to BCBSFL'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, the OIG obtained an understanding of BCBSFL'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 BCBSFL'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 OIG evaluated the confidentiality, integrity, and availability of BCBSFL's computer-based information systems used to process FEHBP claims, and found that there are opportunities for improvement in the information systems' internal controls. These areas are detailed in the "Audit Findings and Recommendations" section of this report.

The scope of this audit centered on the claims processing systems that process FEHBP claims for BCBSFL, as well as the business structure and control environment in which they operate. These systems include the "Diamond" local claims processing system owned and operated by BCBSFL, and the FEP Express system owned and operated by the BlueCross BlueShield Association (BCBSA). BCBSFL is an independent licensee of the BCBSA.

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

The audit was performed at BCBSFL offices in Jacksonville, Florida. These on-site activities were performed in September and October 2009. The OIG completed additional audit work before and after the on-site visits at OPM's 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 BCBSFL as of November 6, 2009.

Methodology

In conducting this review the OIG:

- Gathered documentation and conducted interviews;
- Reviewed BCBSFL's business structure and environment;
- Performed a risk assessment of BCBSFL'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 were functioning as intended. As appropriate, the auditors used judgmental sampling in completing their compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating BCBSFL's control structure. This criteria includes, but is not limited to, the following publications:

- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's Federal Information System Controls Audit Manual;
- 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 800-53 Revision 2, 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
- The Health Insurance Portability and Accountability Act of 1996.

Compliance with Laws and Regulations

In conducting the audit, the OIG performed tests to determine whether BCBSFL's practices were consistent with applicable standards. While generally compliant with respect to the items tested, BCBSFL 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 BCBSFL's overall IT security controls. The OIG evaluated the adequacy of BCBSFL's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSFL has implemented a series of formal policies and procedures that comprise a comprehensive entity-wide security program. The Plan has organized a Policy Committee that has the responsibility for creating, maintaining, and routinely reviewing security-related policies and procedures.

The OIG also reviewed BCBSFL's human resources policies and procedures related to the security aspects of hiring, training, transferring, and terminating employees. We verified that BCBSFL's policies and procedures are maintained on the Plan's intranet site in a manner that is easily accessible by employees.

B. Access Controls

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

The OIG examined the physical access controls of BCBSFL's primary facilities in Jacksonville, Florida, as well as the additional physical and environmental controls protecting the Plan's data center, mail room, and check printing facilities.

Access to all BCBSFL facilities and secure areas within those facilities is controlled by an electronic access card system. Card readers are located on interior and exterior doors throughout the buildings, and the system is capable of limiting an individual's access to the physical areas required by their job function.

The OIG also examined the logical controls protecting sensitive data on BCBSFL's network environment and claims processing related applications. The controls documented during this review include, but were not limited to:

- Appropriate management of firewalls, remote access, and wireless access;
- Monitoring potential security configuration weaknesses through vulnerability testing;
- Procedures for controlling sensitive data transferred to portable media;
- Procedures for appropriately granting and disabling access to information systems;
- Procedures for reviewing existing system access for appropriateness;
- Procedures for controlling and monitoring access of privileged system users; and
- Procedures for appropriately removing system and physical access for terminated employees.

Although BCBSFL has implemented a variety of techniques to protect its IT environment, we did document two opportunities for improvement related to access controls.

1. Authentication Controls for Scanning and Data Verification Application

A software application critical to BCBSFL's claims adjudication process does not have adequate authentication controls.

BCBSFL has contracted with [redacted] to perform its front-end claims processing operations. [redacted] uses an application called [redacted] to scan paper claims and perform optical character recognition and data verification before the claims are loaded into the claims adjudication system.

The authentication controls governing access to [redacted] require [redacted] However, there are no additional password complexity requirements. This configuration does not meet the requirements of BCBSFL's Authentication Security Standard which requires all passwords to maintain a history of six passwords, and [redacted]

[redacted] acknowledged the risk associated with non-compliance with password policy at the application level and stated that the risk is mitigated by the inability of users to launch the [redacted] from an outside network and the fact that access is controlled by the [redacted]. However, many of BCBSFL's applications cannot be launched from outside the Plan's network and also require [redacted] yet these applications are still subject to the requirements of the Plan's Authentication Security Standard.

[redacted] informed the OIG of its efforts to roll out additional [redacted] to several [redacted] applications over the next year.

Recommendation 1

We recommend that ACS and BCBSFL continue their efforts to ensure that the authentication controls for all applications that process FEP data meet the requirements of BCBSFL's Authentication Security Standard.

BCBSFL Response:

"BCBSFL agrees with this recommendation. The ACS CISO Policy and Governance team recognizes the risks associated with non-compliance with password policy at the application level and is monitoring remediation efforts across the enterprise. One such effort involves the WebDE application in use within the BCBSFL operations. . . .

The ACS Security Engineering team is deploying a federated solution from the Novell Identity Management product line to provide front-end authentication to several internal ACS applications. This product is to be piloted in an ACS business unit using the WebDE application and should be rolled out to all WebDE instances over the course of next year. The pilot process began in September 2009 and is expected to be

completed by the end of the calendar year. On December 16, 2009, this policy was amended for clarification regarding the ACS pilot group. ACS WebDE team had pre-determined groups they would utilize during the pilot phase. This pilot group does not include any of the BCBSFL SBU's. ACS anticipates the successful completion of the pilot phase by the end of the first quarter of 2010. Barring unforeseen technical issues, BCBSFL hopes to implement this solution within the SBU's by the end of Second Quarter of 2010."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSFL provide OPM's RBO with supporting documentation detailing progress made in addressing this recommendation.

2. Secure Transmission of Electronic Data

BCBSFL has implemented content filters designed to encrypt sensitive data sent via email or transmitted to a portable media device. However, the email filter was unable to detect social security numbers (SSN) that were not formatted in the traditional manner (###-##-####).

BCBSFL has policies and procedures in place to manage the protection of physical and electronic data. The Plan has implemented controls to detect sensitive data such as SSNs that are transmitted to portable media or sent through email. When a transmission of sensitive data to a portable media device is detected, the filtering software will warn the user of their responsibility to protect sensitive data, and will send an alert of the transmission to BCBSFL's information security team. When sensitive data is sent over email, the filter is designed to automatically encrypt the message and send it to the recipient through a secure web link.

Auditors tested these controls by attempting to move files containing valid SSNs to a portable media device and by sending them through emails. The filter for portable media devices appeared to be functioning as intended. In addition, SSNs sent via email in the traditional format (###-##-####) were appropriately detected and secured by the filtering controls. However, valid SSNs formatted without dashes (#########) were not detected and were transmitted in an unencrypted, insecure manner.

HIPAA Security Standard §164.312(e)(1) requires that Plans "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

Recommendation 2

We recommend that BCBSFL make the appropriate changes to its email filter settings to ensure that all social security numbers and other sensitive data are blocked from being transmitted in an insecure manner.

BCBSFL Response:

"BCBSFL is in the process of performing an analysis of current traffic patterns and preliminary results indicate that the recommended change in the email filter would result in primarily capturing and encrypting non-privacy related emails that include zip codes, addresses and phone numbers. However, the Plan will finalize its analysis of the results by April 30, 2010 and make appropriate enhancements as required to mitigate risks."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSFL provide OPM's RBO with documentation detailing the final results of its analysis and any enhancements made to its controls related to protecting the electronic transmission of sensitive data.

C. Configuration Management

BCBSFL's local claims processing system is housed in a sever environment with the AIX operating platform.

BCBSFL 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.

The following policies and procedures were examined:

- Change Management Policy
- Vulnerability Testing Procedures
- Vulnerability Patch Management Standard
- AIX Configuration Security Baseline
- Web Server Security Standard
- Application Server Security Standard

Auditors verified that these policies are being appropriately followed and did not detect any weaknesses in BCBSFL's configuration management methodology. We also conducted a limited review of the security settings of BCBSFL's AIX configuration and did not identify any weaknesses in the settings.

D. Contingency Planning

The OIG reviewed BCBSFL's service continuity program to determine if (1) procedures were in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan existed to recover critical operations should interruptions occur.

In an effort to assess BCBSFL's contingency planning capabilities, we evaluated documentation related to the Plan's procedures that ensure continuity of its FEP business unit, including:

- BCBSFL's Mission Critical Employees Standard Operating Procedure;

- IT Disaster Recovery/Systems Continuity Standard; and
- Several business units' continuity plans including the claims department and check printing plans.

The OIG found that each of these documents contain a majority of the key elements of a comprehensive service continuity program suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems." BCBSFL's service continuity documentation explicitly identifies the systems that are critical to continuing business operations, prioritizes these systems, and outlines the specific resources needed to support each system. Each of these documents is reviewed, updated, and tested regularly.

E. Application Controls

Application Configuration Management

The OIG evaluated the policies and procedures governing software development and change control of the Plan's claims processing application.

BCBSFL has adopted a traditional system development life cycle methodology that IT personnel follow during routine software modifications. The Plan has also implemented a formal approval process for change requests. The following controls related to testing and approvals of software modifications were observed:

- BCBSFL has adopted practices that allow modifications to be tracked;
- Parallel testing and unit testing are conducted in accordance with industry standards; and
- BCBSFL has a team dedicated to testing FEP modifications.

The OIG also observed the following controls related to the maintenance of software libraries:

- BCBSFL utilizes a "Build and Release Tool" to move the code between the segregated libraries.
- BCBSFL clearly segregates application development and change control activities along organizational lines.
- BCBSFL utilizes versioning of the source code to determine if appropriate changes are implemented as expected.

Claims Processing System

The OIG evaluated the input, processing, and output controls associated with BCBSFL's local claims processing system and the FEP Express system. In terms of input controls, the OIG documented the policies and procedures adopted by BCBSFL 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. BCBSFL's methods for reconciling processing totals against input totals and for evaluating the accuracy of its processes were also reviewed. Auditors also examined the security of physical input and output (paper claims, checks, explanations of benefits, etc.).

Application Controls Testing

To validate the claims processing controls, a testing exercise was conducted on the BCBSFL local system and the BCBSA's FEP Express system. This test was conducted at BCBSFL's Jacksonville, Florida facility with the assistance of BCBSFL personnel. The exercise involved developing a test plan that included realistic situations to present to BCBSFL personnel in the form of institutional and professional claims. All test scenarios were processed through the BCBSFL local claims processing system, and where appropriate, the FEP Express system. The test plan included expected results for each test case. 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.

1. Procedure to Diagnosis Inconsistency

Two test claims were processed where benefits were paid for a procedure associated with an inappropriate diagnosis.

The OIG entered a test claim into the BCBSFL local system with a procedure code for a [redacted] and a diagnosis of [redacted] A second test claim was entered with a procedure code for an [redacted] and a diagnosis of [redacted] Despite the procedures/diagnosis inconsistencies, the claims processed through the local system without encountering any edits and were sent to FEP Express. FEP Express also processed and paid these claims without suspending the claims or triggering any edits.

This system weakness increases the risk that benefits are being paid for procedures associated with a diagnosis that may not warrant such treatment. This issue has been documented in past OIG audits of BCBS plans.

Recommendation 3

We recommend that the BCBSA make the appropriate system modifications to FEP Express to ensure that claims with procedure/diagnosis inconsistencies are flagged for review.

BCBSFL Response:

"BCBSFL disagrees with this recommendation. BCBSFL has implemented and maintains detective system controls to ensure claims with diagnosis inconsistencies are reviewed prior to processing. The Plan has a comprehensive medical policy program that applies necessary controls to ensure services are medically appropriate before approved to pay. However, these controls are not absolute but are intended to identify the common types of procedures that are not consistent with the diagnosis.

However, the FEP Director's Office is in the process of analyzing the feasibility of using existing commercial medical editing software to address this issue. The analysis will also consider implications across the system and how this process will impact Plans. The anticipated completion date for this project is late Second Quarter 2010."

OIG Reply:

We believe that comprehensive medical edit software is needed for FEP Express, as multiple OIG audits of BCBS Plans have detected many weaknesses in the system's medical edit capabilities (including three found during this audit). As part of the audit resolution process, we recommend that the BCBSA provide the RBO documentation detailing its efforts in implementing commercial medical editing software.

2. Provider Invalid for Procedure

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

The OIG entered a test claim for professional services into the BCBSFL local system with a [redacted] performed by an [redacted] This procedure would generally be performed by an [redacted] Despite the provider/procedure inconsistency, the claim was processed by the BCBSFL local system and FEP Express without encountering any edits.

A second test claim for professional services entered into the BCBSFL local system indicated that a [redacted] was performed by an [redacted] This procedure would generally be performed by a [redacted] Despite the provider/procedure inconsistency, the claim was processed by the BCBSFL local system and FEP Express without encountering any edits.

This system weakness increases the risk that providers are being paid for services outside the scope of their license.

Recommendation 4

We recommend that the BCBSA make the appropriate system modifications to FEP Express to ensure that medical providers are not paid for services outside the scope of their license.

BCBSFL Response:

"BCBSFL disagrees with this recommendation, given that the Plan has implemented and maintains appropriate system controls to ensure that medical providers are not paid for services outside the scope of their license on a post payment basis. Most physicians declare a specialty and often receive board certification, but with additional training and or experience in other specialty areas, can through the life of the practice change their practice specialty to a subset or other areas of interest. Therefore, it is impossible to limit a physician when they study in all areas of medicine.

The claim form may indicate one specialty however, some providers have multiple specialties. Edits exist to keep limited license practitioners such as podiatrists from performing medical services outside their scope of practice and controls are in place which helps ensure that medical providers are paid only for services within the scope of their license. In addition, the Plan does have pre-payment edits in place to identify providers rendering services outside of the scope licensure. Also, the Plan does have post-payment review processes conducted by its Special Investigation Unit and Utilization Review areas to identify abnormal billing practices.

However, the FEP Director's Office is in the process of analyzing the feasibility of using existing commercial medical editing software to address this issue. The analysis will also consider implications across the system and how this process will impact Plans. The anticipated completion date for this project is late Second Quarter 2010."

OIG Reply:

We acknowledge the fact that certain providers may be capable of providing a broad range of medical services. However, the inconsistency in this test claim was so extreme that we would expect the system to detect it and suspend the claim for further review. Although the BCBSA searches for these inconsistencies on a post-payment basis, the implementation of preventive controls in the form of medical edit software is more effective and less costly. Post-payment reviews should complement rather than replace preventive controls.

We believe that comprehensive medical edit software is needed for FEP Express, as multiple OIG audits of BCBS Plans have detected many weaknesses in the system's medical edit capabilities (including three found during this audit). As part of the audit resolution process, we recommend that BCBSFL provide OPM's RBO documentation detailing its efforts in implementing commercial medical editing software.

3. OBRA90 PRICER Updates

BCBSFL OBRA90 claims are being processed with an outdated version of the 2009 CMS PRICER program.

The OIG entered seven test claims that are subject to OBRA90 pricing into the BCBSFL local system. The local system sent the claims to FEP Express where they were processed and priced. The auditors priced each claim with the CMS Inpatient PC PRICER program and compared the Medicare Diagnosis Related Group (DRG) amount produced by the PRICER to the amount produced in the test case.

In three of the seven test claims, the Medicare DRG amount produced by the October 26, 2009 version of the PRICER did not match the amount produced in the test case. The auditors priced these claims again using an older version of the 2009 CMS PRICER program, and in each case the Medicare DRG amount matched that from the test case. The OIG believes that this indicates that FEP Express is processing OBRA90 claims with

an outdated version of the CMS PRICER. As a result, BCBSFL has incorrectly priced some of the OBRA90 claims processed after January 1, 2009.

Recommendation 5 (Draft Audit Report Recommendation 6)

We recommend that the BCBSA implement the appropriate system modifications to FEP Express to ensure that OBRA90 claims are priced with the correct version of the CMS PRICER and adjust all OBRA90 claims that were incorrectly priced.

BCBSFL Response:

"BCBSA agrees with this recommendation as the FEP Operations Center's OPM approved OBRA '90 Mainframe Pricer is the official mechanism used to price all FEP claims meeting the OBRA '90 requirements and not the responsibility of BCBSFL.

In the past, OPM provided FEP with any updates to the OBRA '90 Pricer. Recently, FEP began obtaining the updates directly from CMS. When the first updates were received, it was discovered that the type of tape used by CMS was no longer supported by the FEP Data Center. In order to use the CMS tapes, the Operations Center had to find a vendor to convert them into an alternative tape format for usage in the FEP claims system Mainframe OBRA '90 Pricer. This process resulted in a delay in implementing the CMS updates. All updates received first and second quarters 2009 were updated by July 17, 2009, and re-pricing of the impacted OBRA '90 claims will occur prior to year-end 2010. Attachment A is a schedule of when the updates were received from the various sources and the dates that the changes were implemented into the FEP Mainframe OBRA '90 Pricer Mainframe software. There was a delay in the April 4, 2009 update to the OBRA '90 Pricer.

This delay could account for the different pricing generated during the claims testing process."

OIG Reply:

As part of the audit resolution process, we recommend that the BCBSA provide OPM's RBO with documentation demonstrating that the impacted claims have been appropriately re-priced.

F. Health Insurance Portability and Accountability Act

The OIG reviewed BCBSFL's efforts to maintain compliance with the security, privacy, and national provider identifier standards of HIPAA. Nothing came to our attention that caused us to believe that BCBSFL is not in compliance with the various requirements of these HIPAA regulations.

BCBSFL has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. BCBSFL has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. The documents related to the HIPAA privacy and security rules are readily

available to all BCBSFL employees via the company's intranet. BCBSFL employees receive privacy and security-related training during new hire orientation, as well as periodic subsequent training as needed.

In addition, the OIG documented that BCBSFL has adopted the national provider identifier as the standard unique health identifier for health care providers, as required by HIPAA.

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], IT Auditor
- [redacted] IT Auditor
- [redacted] IT Auditor

Appendix

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

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

February 3, 2010

[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
Florida Blue Cross Blue Shield
Audit Report Number 1A-10-41-09-063

Dear Mr. [redacted]

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

A. ACCESS CONTROLS

1. Authentication Controls for Scanning and Data Verification Application

Recommendation 1

OIG recommended that Affiliated Computer Services (ACS) and Blue Cross Blue Shield of Florida (BCBSFL) continue its efforts to ensure that the authentication controls for all applications that process FEP's data that meet the requirements of BCBSFL's Authentication Security Standard.

BCBSFL Response to Recommendation 1

BCBSFL agrees with this recommendation. The ACS CISO Policy and Governance team recognizes the risks associated with non-compliance with password policy at the application level and is monitoring remediation efforts across the enterprise. One such effort involves the WebDE application in use within the BCBSFL operations. WebDE based data entry application does not adhere to the ACS Information Security Standard's password policy requirements for password complexity. WebDE is one of several legacy applications in use at ACS which does not adhere to this policy and is part of a temporary exception granted by the ACS Security Governance Committee. The exception was granted on the basis of existing mitigating controls and a commitment by the application developers to research, pilot, and deploy a new authentication mechanism for these applications by using a federated solution to front end the applications.

The mitigating controls protecting access to the WebDE application include the inability of users to launch the web application from an outside system or network. The application can only be initiated from an active directory authenticated session on the production or administration domain. Additionally, use of the application requires membership within an active directory security group of authorized WebDE users. Therefore, access to the application is controlled through a fully compliant windows domain authentication process and is role based through the security group designation. The WebDE application is entirely an internally hosted application. Access to the web site is restricted to only hosts on the production and administrative networks by perimeter firewalls and the use of restricted routing to the application server.

The ACS Security Engineering team is deploying a federated solution from the Novell Identity Management product line to provide front-end authentication to several internal ACS applications. This product is to be piloted in an ACS business unit using the WebDE application and should be rolled out to all WebDE instances over the course of next year. The pilot process began in September 2009 and is expected to be completed by the end of the calendar year. On December 16, 2009, this policy was amended for clarification regarding the ACS pilot group. ACS WebDE team had pre-determined groups they would utilize during the pilot phase. This pilot group does not include any of the BCBSFL SBU's. ACS anticipates the successful completion of the pilot phase by the end of the first quarter of 2010. Barring unforeseen technical issues, BCBSFL hopes to implement this solution within the SBU's by the end of Second Quarter of 2010.

2. Secure Transmission of Electronic Data

Recommendation 2

OIG recommended that BCBSFL make the appropriate changes to its email filter settings to ensure that all social security numbers and other sensitive data are blocked from being transmitted in an insecure manner.

BCBSFL Response to Recommendation 2

BCBSFL is in the process of performing an analysis of current traffic patterns and preliminary results indicate that the recommended change in the email filter would result in primarily capturing and encrypting non-privacy related emails that include zip codes, addresses and phone numbers. However, the Plan will finalize its analysis of the results by April 30, 2010 and make appropriate enhancements as required to mitigate risks.

B. APPLICATION CONTROLS

1. Procedure to Diagnosis Inconsistency

Recommendation 3

OIG recommended that BCBSFL make the appropriate system modifications to ensure that claims with procedure/diagnosis inconsistencies are flagged for review.

BCBSFL Response to Recommendation 3

BCBSFL disagrees with this recommendation. BCBSFL has implemented and maintains detective system controls to ensure claims with diagnosis inconsistencies are reviewed prior to processing. The Plan has a comprehensive medical policy program that applies necessary controls to ensure services are medically appropriate before approved to pay. However, these controls are not absolute but are intended to identify the *common types* of procedures that are not consisted with the diagnosis.

However, the FEP Director's Office is in the process of analyzing the feasibility of using existing commercial medical editing software to address this issue. The analysis will also consider implications across the system and how this process will impact Plans. The anticipated completion date for this project is late Second Quarter 2010.

2. **Provider Invalid for Procedure**

Recommendation 4

OIG recommended that BCBSFL make the appropriate system modifications to ensure that medical providers are not paid for services outside the scope of their license.

BCBSFL Response to Recommendation 4

BCBSFL disagrees with this recommendation, given that the Plan has implemented and maintains appropriate system controls to ensure that medical providers are not paid for services outside the scope of their license on a post payment basis. Most physicians declare a specialty and often receive board certification, but with additional training and or experience in other specialty areas, can through the life of the practice change their practice specialty to a subset or other areas of interest. Therefore, it is impossible to limit a physician when they study in all areas of medicine.

The claim form may indicate one specialty however, some providers have multiple specialties. Edits exist to keep limited license practitioners such as podiatrists from performing medical services outside their scope of practice and controls are in place which helps ensure that medical providers are paid only for services within the scope of their license. In addition, the Plan does have pre-payment edits in place to identify providers rendering services outside of the scope licensure. Also, the Plan does have post-payment review processes conducted by its Special Investigation Unit and Utilization Review areas to identify abnormal billing practices.

However, the FEP Director's Office is in the process of analyzing the feasibility of using existing commercial medical editing software to address this issue. The analysis will also consider implications across the system and how this process will impact Plans. The anticipated completion date for this project is late Second Quarter 2010.

3.

******Text redacted: not relevant to final audit report******

Text redacted: not relevant to final audit report

4. OBRA '90 Pricer Updates

Recommendation 6

OIG recommended that BCBSFL implement the appropriate system modifications to ensure that OBRA '90 claims are priced with the correct version of the CMS PRICER, and adjust all OBRA '90 claims that were incorrectly priced.

BCBSFL Response to Recommendation 6

BCBSA agrees with this recommendation as the FEP Operations Center's OPM approved OBRA '90 Mainframe Pricer is the official mechanism used to price all FEP claims meeting the OBRA '90 requirements and not the responsibility of BCBSFL.

In the past, OPM provided FEP with any updates to the OBRA '90 Pricer. Recently, FEP began obtaining the updates directly from CMS. When the first updates were received, it was discovered that the type of tape used by CMS was no longer supported by the FEP Data Center. In order to use the CMS tapes, the Operations Center had to find a vendor to convert them into an alternative tape format for usage in the FEP claims system Mainframe OBRA '90 Pricer. This process resulted in a delay in implementing the CMS updates. All updates received first and second quarters 2009 were updated by July 17, 2009, and re-pricing of the impacted OBRA '90 claims will occur prior to year-end 2010. Attachment A is a schedule of when the updates were received from the various sources and the dates that the changes were implemented into the FEP Mainframe OBRA '90 Pricer Mainframe software. There was a delay in the April 4, 2009 update to the OBRA '90 Pricer. This delay could account for the different pricing generated during the claims testing process.

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

cc: [redacted]

Attachment – A

Text redacted: not relevant to final audit report

Attachment - B

OBRA '90

Updates for OBRA '90 And Implementation Dates

HISTORY OF OBRA90 SOFTWARE RECEIVED FROM OPM/CMS						
DATE RECEIVED FROM OPM/CMS	SOFTWARE RECEIVED	NEW/ UPDATES	QUARTERLY UPDATES FOUND ON CMS WEBSITE FOR	DATE INSTALLED IN PRODUCTION	Problem/ Comments	TT#
Nov-04	Medicare Code Editor Software: Version 21.0 October 1, 2004; CMS Diagnosis Related Groups Software: Version 22.0 October 1, 2004; Provider Specific Files including	New: Yearly Software		1/1/2005		21210
14-Mar-05	Provider Specific Files including Pricer Software-ver D05.0 (PSF0105), PPS050	UPDATES: Provider file updates only	Provider data submitted thru Sep 30 2004 & also Provider data submitted thru Dec 31 2004	4/8/2005		29375
14-Apr-05	Provider Specific Files including Pricer Software-ver D05.1 (PSF0105), PPS051	UPDATES: Pricer Modules - PPCAL046, PPCAL051, PPDRV041 & PPDRV051; PPSPROV - Provider Data files for 2005; PPSCBSA - Wage		6/11/2005		34823
17-May-05	Provider Specific Files including Pricer Software-ver D05.1 (PSF0405), PPS051	UPDATES: PPSPROV - Provider Data files for 2005	Provider data submitted thru Mar 31 2005	6/11/2005		34823
24-Aug-05	Provider Specific Files including Pricer Software-ver D05.1 (PSF0705), PPS051	UPDATES: PPSPROV - Provider Data files for 2005	Provider data submitted thru Jun 30 2005	10/15/2005		51377
13-Oct-05	Medicare Code Editor Software: Version 22.0 October 1, 2005; CMS Diagnosis Related Groups Software: Version 23.0 October 1, 2005; Provider Specific Files including	New: Yearly Software		1/1/2006		39456

20-Dec-05	Provider Specific Files including Pricer Software-ver D06.1 (PSF1005), PPS061	UPDATES: Pricer Modules - PPCAL061 & PPDRV061; PPSPROV - Provider Data files for		2/11/2006		58485
28-Feb-06	Provider Specific Files including Pricer Software-ver D06.2 (PSF0106), PPS062	UPDATES: Pricer Modules - PPCAL062, PPDRV062 & New CICS interface module PPOPN062; PPSPROV -		6/17/2006		63698
13-Jun-06	Provider Specific Files including Pricer Software-ver D06.2 (PSF0406), PPS062	UPDATES: PPSPROV - Provider Data files for 2006		07/07/2006 (08/12/2006)	Found 15 New Providers were added & 51 Old Providers were deleted	67022
25-Oct-06 21-Nov-06	Medicare Code Editor Software: Version 23.0 October 1, 2006; CMS Diagnosis Related Groups Software: Version 24.0 October 1, 2006; Provider Specific Files including Pricer Software-ver D07.2 (PSF0706), PPS072 along with Provider Specific Files including Pricer Software-ver D07.1 (PSF0706), PPS071 and Provider Specific Files	New: Yearly Software for 2007 & updates for 2007, 2006, 2005 & 2004.		1/2/2007		58479
7-Feb-07				3/2/2007	Problems found with some Utah & Arizona Providers that were dropped for the last quarter of 2006 PPS Provider files. Upon receiving an e-mail confirmation from Sarah Shirey @ CMS, the 2006	78423

30-Mar-07	Provider Specific Files including Pricer Software-ver D07.2 (PSF0107), PPS072	UPDATES: PPSPROV - Provider Data files for 2007		5/18/2007	Found 137 New Providers were added & 16 Old Providers were	81980
24-Jul-07	Provider Specific Files including Pricer Software-ver D07.2 (PSF0407), PPS072	UPDATES: PPSPROV - Provider Data files for 2007 & PPSCBSA - CBSA (Wage Index) file for 2007.		8/17/2007	Found 22 New Providers were added when compared to previous version of PPSPROV file. Also found 23 new CBSA (Wage Index)	88731
13-Sep-07 19-Nov-07	Medicare Code Editor Software: Version 24.0 October 1, 2007; Medicare Severity DRG Software (MS-DRG): Version 25.0 October 1, 2007; Provider Specific Files including Pricer Software-ver D08.4 (PSF0710), PPS084 along with updated 2007 Pricer	New: Yearly Software for 2008 & updates for 2007.		12/14/2007	Found 87 New Providers were added and 4 Old Providers were dropped when compared to 2007 version of PPSPROV file. Also found 447 new CBSA (Wage Index) records were added when compared to 2007 version of PPSCBSA file.	81983
21-Mar-08 14-Apr-08	Medicare Code Editor Software: Version 24.1 April 1, 2008; Medicare Severity DRG Software (MS-DRG): Version 25.1 April 1, 2008; Provider Specific Files including Pricer Software-ver D08.5 (PSF0801), PPS085.	Updates: Updated version of Editor, Grouper & Pricer software effective from 4/1/08 along with updated Provider Data files for 2008.		5/9/2008	Per documentation, a new discharge status 70 was added effective 4/1/08: Discharge/ transfer to another type of health care institution not defined elsewhere in the code list. Also, existing discharge status code 05 has a definition change effective 4/1/08: Discharged/ transferred	101511

N/A	N/A	Updates		8/16/2008	Defer claims that meet OBRA90 requirements (ie. Attempt all claims to	94186 (07BRD114)
11-Sep-08 10-Nov-08	Medicare Code Editor Software: Version 25.0 October 1, 2008; Medicare Severity DRG Software (MS-DRG): Version 26.0 October 1, 2008; Provider Specific Files including Pricer Software-ver D09.3 (PSF0807), PPS093.	New: Yearly Software for 2009.		1/2/2009	Found 38 New Providers were added and 1,336 Old Providers that were terminated in prior FYs, were dropped when compared to 2008 version of PPSPROV file. Also found 445 new CBSA (Wage Index)	98673 (OBRA90 Real Time Processing) 98087 (OBRA90 Year End software install)
N/A	N/A	Updates		4/4/2009	Modify OBRA90 Patient Discharge status (Set Pricer Review code	100775 (08BRD028)
03/06/2009 03/23/2009 06/08/2009	Provider Specific Files including Pricer Software-ver D09.6 (PSF0904), PPS096	UPDATES: Pricer Modules - PPCAL096, PPDRV096, PPOPN096 & PPCAL086; PPSPROV - Provider Data files for 2009.		7/18/2009	Needed to convert 3490 tapes from CMS to 3590 tapes as CareFirst does not support 3490 tapes anymore effective 02/20/2009. Found 3,214 New Providers were added when compared to	176024