



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

Final Audit Report

**AUDIT OF THE INFORMATION SYSTEMS
GENERAL AND APPLICATION CONTROLS
AT CAPITAL BLUECROSS**

**Report Number 1A-10-36-20-032
February 21, 2021**

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Capital BlueCross

Report No. 1A-10-36-20-032

February 21, 2021

Why Did We Conduct The Audit?

Capital BlueCross (CBC) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in CBC's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by CBC to process and store data related to medical encounters and insurance claims for FEHBP members.

What Did We Find?

Our audit of CBC's IT security controls determined that:

- CBC has adequate controls over security management.
- CBC has adequate logical and physical access controls.
- CBC has controls in place related to network security, such as encryption to protect sensitive data and data loss prevention. However, controls could be improved related to [REDACTED]
[REDACTED]
- CBC maintains approved security configuration standards. However, it does not [REDACTED]
[REDACTED] Furthermore, CBC's network environment [REDACTED]
[REDACTED]
- CBC has adequate controls over contingency planning.
- CBC has adequate controls over its claims adjudication process.



Michael R. Esser
*Assistant Inspector General
for Audits*

ABBREVIATIONS

CBC	Capital BlueCross
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information Systems Controls Audit Manual
GAO	U.S. Government Accountability Office
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	i
ABBREVIATIONS	ii
I. BACKGROUND	1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	2
III. AUDIT FINDINGS AND RECOMMENDATIONS	4
A. SECURITY MANAGEMENT	4
B. ACCESS CONTROLS	4
C. NETWORK SECURITY	5
1. Firewall Configuration Reviews	5
2. Internal Network Segmentation	6
3. Vulnerability Scanning	7
4. Vulnerabilities Identified by OIG Scans	7
D. CONFIGURATION MANAGEMENT	9
1. Security Configuration Auditing.....	9
2. System Lifecycle Management.....	10
E. CONTINGENCY PLANNING	11
F. CLAIMS ADJUDICATION	11
1. Application Change Control	11
2. Claims Processing System	12
3. Debarment and Suspension.....	12
APPENDIX: CBC’s December 19, 2020, response to the draft audit report, issued October 22, 2020.	
REPORT FRAUD, WASTE, AND MISMANAGEMENT	

I. BACKGROUND

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) data by Capital BlueCross (CBC).

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

The FEHBP was established by the Federal Employees Health Benefits 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, or comprehensive medical services.

This was our initial audit of general and application controls at CBC. All CBC personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

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

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to CBC's claims processing system.

SCOPE AND METHODOLOGY

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 CBC's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of CBC'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 CBC to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Harrisburg, Pennsylvania.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews with CBC subject matter experts, documentation reviews, and remote testing of the general and application controls in place over CBC's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at CBC as of July 2020.

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

In conducting this audit we:

- Performed a risk assessment of CBC's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM);
- Gathered documentation and conducted interviews;
- Reviewed CBC's business structure and environment; 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 CBC's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;
- National Institute of Standards and Technology Special Publication (NIST SP) 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy; and
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

COMPLIANCE WITH LAWS AND REGULATIONS

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

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

CBC has adequate controls over security management.

CBC has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. CBC also has implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that CBC has not implemented adequate controls related to security management.

B. ACCESS CONTROLS

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

We examined the physical access controls at CBC's facilities and data center. We also examined the logical access controls protecting sensitive data on CBC's network environment and claims processing applications.

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

- Procedures for appropriately granting and removing physical access to facilities and data centers;
- Procedures for appropriately granting and removing logical access to applications and software resources; and
- Routine access reviews for logical and physical access.

Nothing came to our attention to indicate that CBC has not implemented adequate access controls.

C. NETWORK SECURITY

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

CBC has adequate data loss prevention controls.

We evaluated CBC's network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public network connections;
- Encryption to protect sensitive data at rest; and
- Data loss prevention controls.

However, we noted the following opportunities for improvement related to CBC's network security controls.

1. Firewall Configuration Reviews

CBC maintains documented firewall configurations based on established IT security best practices. Firewalls are hardened to these best practices and any deviations are documented and tracked through the change management process. However,

NIST SP 800-41, Revision 1, states that "Policy rules may need to be updated as new threats are identified and requirements change, such as when new applications or hosts are implemented within the network, and should also be reviewed periodically to ensure they remain in compliance with security policy."

Furthermore, NIST SP 800-41, Revision 1, states that "It is important to review the firewall policy often. Such a review can uncover rules that are no longer needed as well as new policy requirements that need to be added to the firewall."

[REDACTED]

Recommendation 1

We recommend that CBC perform [REDACTED]

CBC's Response:

“CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by March 31, 2021.”

OIG Comment:

As a part of the audit resolution process, please provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence that CBC has fully implemented this recommendation. This statement also applies to subsequent recommendations in this audit report that CBC agrees to implement.

2. Internal Network Segmentation

CBC uses firewalls to control connections with systems outside of its network as well as between public-facing applications and the internal network. However, [REDACTED]



[REDACTED] CBC has previously identified this gap and a project is currently ongoing to address this issue.

NIST SP 800-41, Revision 1, advises that “Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. [REDACTED]

[REDACTED]

Recommendation 2

We recommend that CBC complete its project to [REDACTED]
[REDACTED]

CBC's Response:

“CBC agrees with the recommendation and plans to implement this by December 31, 2020.”

3. Vulnerability Scanning

CBC conducts authenticated vulnerability scans on most of its network environment on a routine basis. Additionally, CBC utilizes a vendor to conduct annual penetration testing of its web applications. However, as part of this audit we reviewed a sample of historical vulnerability scan results to verify that CBC is following its vulnerability scanning process.
[REDACTED]

NIST SP 800-53, Revision 4, states that the organization should implement privileged access authorization for vulnerability scanning activities.
[REDACTED]

Recommendation 3

We recommend [REDACTED]
[REDACTED]

CBC's Response:

“CBC agrees with the recommendation and plans to implement this by December 31, 2020.”

4. Vulnerabilities Identified by OIG Scans

CBC conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. The specific vulnerabilities that we identified were provided to CBC in the form of an audit inquiry, but will not be detailed in this report. CBC responded to our audit inquiry that it was aware of

the majority of the vulnerabilities and those vulnerabilities were also identified in historical scan results that were provided. However, [REDACTED]

NIST SP 800-53, Revision 4, states that organizations should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

Furthermore, FISCAM 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.”

[REDACTED]

Recommendation 4

We recommend [REDACTED]

CBC’s Response:

“CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.”

Recommendation 5

We recommend [REDACTED]

CBC’s Response:

“CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.”

D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. CBC employs a team of technical personnel who manage system software configuration for the organization. We evaluated CBC's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented system change control process;
- An established system build and hardening process; and
- An established patch management process.

However, we noted the following opportunities for improvement related to CBC's configuration management.

1. Security Configuration Auditing

CBC maintains approved security configuration standards based on established IT security best practices for current workstation and server operating systems in its network environment. Prior to systems being deployed, security configurations are applied in accordance with the approved configuration standards and reviewed for compliance using an automated tool. However, [REDACTED]



NIST SP 800-53, Revision 4, states that an organization should monitor and control "changes to the configuration settings in accordance with organizational policies and procedures."

FISCAM requires the "Current configuration information [to] be routinely monitored for accuracy. Monitoring should address the ... baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

[REDACTED]

Recommendation 6

We recommend [REDACTED]

CBC's Response:

“CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by June 30, 2021.”

2. System Lifecycle Management

CBC maintains policies and procedures related to system lifecycle management that require unsupported systems to be removed from the network. If unsupported systems cannot be removed, a formal risk assessment must be conducted to identify mitigating controls. [REDACTED]

NIST SP 800-53, Revision 4, recommends that organizations replace “information system components when support for the components is no longer available from the developer, vendor, or manufacturer” NIST SP 800-53, Revision 4, also states that “Unsupported components ... provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components.”

[REDACTED]

Recommendation 7

We recommend [REDACTED]

CBC's Response:

“CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.”

E. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of CBC's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

CBC has adequately documented contingency plans.

- Data center environmental controls to minimize disruptions;
- Business continuity plan (e.g., people and business processes); and
- Disaster recovery plan (e.g., recovery of hardware and software infrastructure).

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

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting CBC's claims adjudication process. CBC adjudicates claims using a commercially available claims processing application called Facets and the BlueCross BlueShield Association's nationwide Federal Employee Program Direct system. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, and provider debarment and suspension.

1. Application Change Control

We evaluated the policies and procedures governing application development and change control over CBC's claims processing system.

CBC has implemented policies and procedures related to application configuration management, and has adopted a system development life cycle methodology that IT

personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

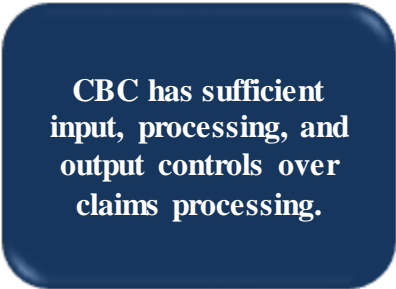
- Documented application change control process;
- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

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

2. Claims Processing System

We evaluated the business process controls associated with CBC's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that CBC has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;
- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and
- Claims scheduled for payment are actually paid.



CBC has sufficient input, processing, and output controls over claims processing.

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

3. Debarment and Suspension

CBC has documented procedures for reviewing provider files for debarments and suspensions. CBC downloads the OPM OIG debarment and suspension list and performs a comparison with provider records maintained in Facets. Positive matches from the debarment and suspension list are identified within Facets, and a notification letter is sent to members. If a debarred or suspended provider submits a claim, the claims processing

application will suspend the claim for review by a claims processor. CBC adheres to the OPM OIG debarment and suspension guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

Nothing came to our attention to indicate that CBC has not implemented adequate controls over the debarment and suspension process.

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

December 19, 2020

Christopher Bouchey, Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management (OPM)
1900 E Street, NW
Room 6400
Washington, D.C. 20415-1100

**Reference: OPM DRAFT IT AUDIT REPORT
Capital BlueCross (CBC)
Audit Report Number 1A-10-36-20-032
(Dated October 22, 2020)**

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

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

No recommendation noted.

C. NETWORK SECURITY

1. Firewall Configuration Reviews

Recommendation 1

We recommend that Capital BlueCross perform [REDACTED]

Plan Response

CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a

technical solution in place by March 31, 2021.

2. Internal Network Segmentation

Recommendation 2

We recommend that Capital BlueCross complete its project to [REDACTED]

Plan Response

CBC agrees with the recommendation and plans to implement this by December 31, 2020.

3. Vulnerability Scanning

Recommendation 3

We recommend [REDACTED]

Plan Response

CBC agrees with the recommendation and plans to implement this by December 31, 2020.

4. Vulnerabilities Identified by OIG Scans

Recommendation 4

We recommend [REDACTED]

Plan Response

CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.

Recommendation 5

We recommend [REDACTED]

Plan Response

CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.

D. CONFIGURATION MANAGEMENT

1. Secure Configuration Auditing

Recommendation 6

We recommend [REDACTED]

Plan Response

CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by June 30, 2021.

2. System Lifecycle Management

Recommendation 7

We recommend that [REDACTED]

Plan Response

CBC agrees with the recommendation and has already implemented enhancements. CBC will continue to monitor these items and expect to have a technical solution in place by September 30, 2021.

E. CONTINGENCY PLANNING

No recommendation noted.

F. CLAIMS ADJUDICATION

No recommendation noted.

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [REDACTED] or [REDACTED] at [REDACTED]

Sincerely,

[REDACTED]

Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
[REDACTED], FEP
[REDACTED], FEP



Report Fraud, Waste, and Mismanagement

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

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

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

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