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 Blue Cross and Blue Shield of Alabama

Report Number 2022-ISAG-006

August 22, 2022

Executive Summary

Audit of the Information Systems General and Application Controls at Blue Cross and Blue Shield of Alabama

Report No. 2022-ISAG-006 **August 22, 2022**

Why Did We Conduct the Audit?

Blue Cross and Blue Shield of Alabama (BCBSAL), plan codes 10 and 11, 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 BCBSAL's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSAL to process and store data related to medical encounters and insurance claims for FEHBP members as of March 2022.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- [redacted]
- BCBSAL has adequate physical and logical access controls in place.
- BCBSAL has adequate network security controls in place.
- BCBSAL's enterprise security event monitoring and incident response programs are adequate.
- [redacted]
- BCBSAL has adequate controls over its contingency planning program.
- BCBSAL has adequate application change control policies and procedures.

Abbreviations

BCBSAL	**Blue Cross and Blue Shield of Alabama**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System 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

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 Blue Cross and Blue Shield of Alabama (BCBSAL).

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, indemnity benefits, or comprehensive medical services.

This was our initial audit of the information technology (IT) general security and application controls at BCBSAL. All BCBSAL personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit were 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 BCBSAL's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to BCBSAL'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 BCBSAL'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 BCBSAL'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 BCBSAL to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Birmingham, Alabama.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of subject matter experts, documentation review, and remote testing of the general controls in place over BCBSAL'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 BCBSAL as of March 2022.

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

We used judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of BCBSAL's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's Federal Information System Controls Audit Manual;
- Gathered documentation and conducted interviews;
- Reviewed BCBSAL's business structure and environment; and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended.

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

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-39, Managing Information Security Risk.

Compliance with Laws and Regulations

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

BCBSAL has developed adequate IT security policies and procedures. BCBSAL has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

However, we noted the following opportunity for improvement related to BCBSAL's security management program.

1. Risk Response

During our audit, we found that BCBSAL [redacted] In response to this finding, BCBSAL developed [redacted]

NIST SP 800-53, Revision 5, control RA-7 states that the organization should respond to findings from security and privacy assessments, monitoring, and audits in accordance with risk tolerance. Responding to risk includes mitigating, accepting, sharing, or avoiding risk.

Furthermore, NIST SP 800-39, states that "Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance."

Additionally, NIST SP 800-39, states that "Explicit understanding and acceptance of the risk to an organization's operations and assets, individuals, other organizations … by senior leaders/executives (reflecting the organization's risk tolerance) are made in accordance with the organization's risk management strategy … ."

[redacted]

Recommendation 1:

We recommend that BCBSAL formally [redacted]

BCBSAL's Response:

"BCBSAL agrees with the recommendation and is working to implement the recommendation. The Plan has reviewed and updated its policy (Attachment 1), developed an implementation plan (Attachment 2) and developed forms to capture information for acceptance (Attachment 3)."

OIG Comments:

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

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 BCBSAL's facilities and data centers. We also examined the logical access controls protecting sensitive data on BCBSAL's network environment and applications.

We observed the following controls in place:

- Routine access audits performed for secure areas;
- Multi-factor authentication for privileged and remote access; and
- Routine reviews of logical access to critical systems.

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

C. Network Security

BCBSAL has adequate network security controls in place.

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. We evaluated BCBSAL's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during the audit.

We observed the following controls in place:

- Perimeter controls to secure connections to external networks;
- Technical controls to secure mobile devices; and
- Network access controls to prevent non-company devices from connecting to the network.

Nothing came to our attention to indicate that BCBSAL has not implemented adequate network security controls.

D. Security Event Monitoring and Incident Response

BCBSAL has an adequate event monitoring program.

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

We observed the following controls in place:

- Security event monitoring throughout the network;
- Policies and standards for security event monitoring; and
- A documented incident response program.

Nothing came to our attention to indicate that BCBSAL has not implemented adequate security event monitoring and incident response controls.

E. 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. BCBSAL employs a team of technical personnel who manage system software configuration for the organization. We evaluated BCBSAL's management of the configuration of its computer servers and databases.

We observed the following controls in place:

- Documented security configuration standards;
- Adequate change management separation of duty controls; and
- An established patch management process.

However, we noted the following opportunity for improvement related to [redacted]

1. Vulnerabilities Identified by OIG Scans

BCBSAL conducted credentialed vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. We judgmentally selected a sample of [redacted] servers from a universe of [redacted]. The sample included a variety of system functionality and operating systems across production, test, and development environments. The sample was drawn from systems that store and/or process Federal member data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The specific vulnerabilities that we identified were provided to BCBSAL in the form of an audit inquiry but will not be detailed in this report. [redacted]

NIST SP 800-53, Revision 5, control RA-5 states that organizations should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

Failure to remediate vulnerabilities in a timely manner increases the risk that threat actors could exploit system weaknesses for malicious purposes.

Recommendation 2:

We recommend that BCBSAL remediate [redacted]

BCBSAL's Response:

"BCBSAL agrees with the recommendation and plans to complete implementation. The Plan has remediated all but one item identified in in [sic] the audit inquiry. Refer to Attachment 4 for evidence of remediation."

F. Contingency Planning

BCBSAL has adequate controls over contingency planning.

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

We observed the following controls in place:

- Environmental controls to minimize disruptions;
- Documented contingency plans; and
- Adequate contingency plan testing.

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

G. Application Change Control

We evaluated the policies and procedures governing BCBSAL's application development and change control process.

BCBSAL has implemented policies and procedures related to application configuration management and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications.

We observed the following controls in place:

- Documented application change management policies and procedures;
- An adequate application change review and approval process; and
- Adequate developer testing and evaluation.

Nothing came to our attention to indicate that adequate controls have not been implemented over the application change control 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

May 17, 2022

Matthew Antunez, 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
Blue Cross Blue Shield of Alabama (BCBSAL)
Audit Report Number 2022-ISAG-006
(Dated March 16, 2022)

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

A. Security Management

Risk Response

Recommendation 1:

We recommend that BCBSAL formally [redacted]

Plan Response:

BCBSAL agrees with the recommendation and is working to implement the recommendation. The Plan has reviewed and updated its policy (**Attachment 1**), developed an implementation plan (**Attachment 2**) and developed forms to capture information for acceptance (**Attachment 3**).

B. Access Controls

No recommendation noted.

C. Network Security

No recommendation noted.

D. Security Event Monitoring and Incident Response

No recommendation noted.

E. Configuration Management

Vulnerability Management

Recommendation 2:

We recommend that BCBSAL remediate [redacted]

Plan Response:

BCBSAL agrees with the recommendation and plans to complete implementation. The Plan has remediated all but one item identified in in the audit inquiry. Refer to **Attachment 4** for evidence of remediation.

F. Contingency Planning

No recommendation noted.

G. Application Change Control

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]

Sincerely,

[redacted]

[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: https://oig.opm.gov

By Phone: Toll Free Number: (877) 499-7295

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