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 AETNA

Report Number 1C-22-00-19-020
March 4, 2020

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Aetna

Report No. 1C-22-00-19-020 **March 4, 2020**

Why Did We Conduct The Audit?

Aetna 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 Aetna's information technology (IT) environment.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of Aetna's IT security controls determined:

- Aetna has implemented a series of formal policies and control standards to govern its security management program. Aetna requires these policies and control standards to be reviewed at least annually. However, during our fieldwork Aetna could not provide evidence demonstrating that all policies and control standards were reviewed annually.
- Aetna has adequate controls over granting, removing, and monitoring access to facilities, network resources, and applications.
- [redacted]
- System configuration is controlled according to documented policies, procedures, and standards.
- Aetna has an adequate contingency planning process in place to respond to and recover from unexpected disruptions.
- Aetna has adequate policies and procedures in place related to claims adjudication.

ABBREVIATIONS

ACAS	**Automated Claims Adjudication System**
CFR	**Code of Federal Regulations**
EPDB	**Enterprise Provider Database**
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

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 Aetna.

The audit was conducted pursuant to FEHBP contracts CS 1766, CS 2900, CS 2938, CS 2867, CS 2914, CS 1948-A, and CS 2839; 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 third audit of general and application controls at Aetna. The previous audits of general and application controls at Aetna were conducted in 2000 and 2012. Final Audit Report No. 1C-JN-00-01-007 was issued on November 1, 2001, and Final Audit Report No. 1C-22-00-12-065 was issued on March 18, 2013. All recommendations from these previous audits have been closed.

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 Aetna's 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 Aetna'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 Aetna'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 Aetna'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 Aetna to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Hartford, Connecticut.

The onsite portion of this audit was performed in May and September of 2019. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at Aetna as of September 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Aetna. 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 Aetna'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 Aetna'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 Aetna's control structure. These criteria include, but are not limited to, the following publications:

- GAO's FISCAM; and

- National Institute of Standards and Technology Special Publication (NIST SP) 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy.

COMPLIANCE WITH LAWS AND REGULATIONS

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

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

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

1. IT Security Policy Review

Aetna has implemented a series of formal policies and control standards that govern its security management program. Aetna requires that each policy and control standard be reviewed at least annually or whenever significant changes are made. However, during our review we identified a number of policies and control standards that were not subject to a routine review.

FISCAM states that policies "should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use."

Furthermore, FISCAM states that "Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied."

Recommendation 1

We recommend that Aetna follow its process to review and update all IT security policies and control standards on a routine basis.

Aetna's Response:

"The Plan disagrees with the Draft Report's contention that not all policies and control standards are reviewed on a routine basis. The Plan agrees that due to a misconfiguration, certain control standards were not reviewed during an annual assessment because they were missing a date/notification that would prompt such a review. Aetna identified the cause of the configuration issue and subsequently corrected the affected control standards so they would notify the Policy Administrator for the need to conduct an annual review. This issue has been remediated."

OIG Comments:

In response to the draft audit report, Aetna provided evidence that the configuration issue preventing the notification prompting a policy review has been remediated; the Policy Administrator will now be notified of the need to conduct the annual policy review. No further action is required.

B. ACCESS CONTROLS

Aetna has adequate logical and physical 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 Aetna's facilities and data center. We also examined the logical access controls protecting sensitive data on Aetna's network environment and 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; and

- Procedures for appropriately granting and adjusting logical access to applications and software resources.

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

C. NETWORK SECURITY

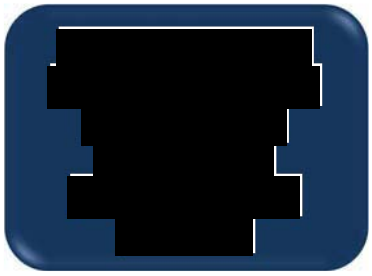
Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. We evaluated Aetna's network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Network access controls to prevent unauthorized devices from connecting to the internal network; and
- Documented policies and procedures to identify and respond to information security incidents.

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

1. [redacted]



[redacted]

[redacted]

Recommendation 2

[redacted]

Aetna's Response:

[redacted]

[redacted]

OIG Comments:

[redacted]

As a part of the audit resolution process, we recommend that Aetna provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence that it has fully implemented this recommendation.

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. Aetna employs a team of technical personnel who manage system software configuration for the organization. We evaluated Aetna's management of the configuration of its computer servers and databases. Our review found the following controls in place:

- Documented and approved configuration standards including an exception process for deviations;
- Documented system change control process; and
- Established patch management process.

Nothing came to our attention to indicate that Aetna has not implemented adequate controls over the configuration management program.

E. CONTINGENCY PLANNING

Aetna has adequate contingency planning controls in place.

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

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

Nothing came to our attention to indicate that Aetna has not implemented adequate controls over the contingency planning process.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting Aetna's claims adjudication process. Aetna adjudicates claims using an internally developed claims processing application called the Automated Claims Adjudication System (ACAS). We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

1. Application Change Control

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

Aetna has implemented policies and procedures related to application configuration management, and also 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 Aetna has not implemented adequate controls over the application configuration management process.

2. Claims Processing System

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

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

- 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.

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

3. Enrollment

We evaluated Aetna's procedures for managing its member enrollment database. Enrollment information is received either electronically or in paper format, and loaded into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

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

4. Debarment

Aetna has documented procedures for reviewing provider files for debarments and suspensions. Aetna downloads the OPM OIG debarment list and performs an automated comparison with provider records maintained in Aetna's Enterprise Provider Database (EPDB). Aetna's EPDB is the source of record for provider information and is connected to ACAS. Positive matches from the debarment list are identified and flagged within the EPDB. If a debarred provider submits a claim, the claims processing application will suspend the claim for review by a claims processor. Aetna adheres to the OPM OIG debarment 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 Aetna has not implemented adequate controls over the debarment process.

151 Farmington Ave.
Hartford, CT 06156

[redacted]

VIA EMAIL: [redacted]@opm.gov

January 28, 2020

Mr. [redacted]
Auditor In Charge
Information Systems Audit Group
U.S. Office of Personnel Management
Office of the Inspector General
1900 E Street NW, Room 6400
Washington, DC 20415

Re: Information Technology Audit
Draft Report No. 1C-22-00-19-020

Dear Mr. [redacted]:

Thank you for the opportunity to respond to the above referenced draft audit report dated December 4, 2019. After a careful review of this draft report, we agree with the majority of the draft report's findings and recommendations. [redacted]

We look forward to continuing to work with the OIG in the coming weeks to address and resolve any and all concerns outlined in the draft report prior to OIG issuing their final audit report. After you have had a chance to review our response, please feel free to contact me to discuss our next steps.

Sincerely,

[redacted]

cc: [redacted]

Response to Draft Report dated December 4, 2019

Information Technology Audit of Aetna
Hartford, Connecticut

Report No.
1C-22-00-19-020

Aetna submits the following comments to the above-referenced draft report ("Draft Report") issued by the Office of Personnel Management ("OPM") Office of the Inspector General ("OIG") in connection with the OIG's Information Technology audit of the Aetna Federal Employees Health Benefits Program ("FEHBP").

Background

The Plan's compliance must be assessed pursuant to 5 U.S.C. Chapter 89, and 5 Code of Federal Regulations (CFR) Chapter 1, part 890, as well as all FEHBP contracts with Aetna.

Plan's Specific Responses to Draft Report's Findings and Recommendations

The following is the Plan's response to the Draft Report's preliminary findings and recommendations.

Background

The Draft Report indicates that the audit was conducted pursuant to FEHBP contract CS 1766. The Plan disagrees. The audit should have been conducted pursuant to FEHBP contracts CS 1766, CS 2900, CS 2938, CS 2867, CS 2914, CS 1948-A and CS 2839.

Security Management

The Plan disagrees with the Draft Report's contention that not all policies and control standards are reviewed on a routine basis. The Plan agrees that due to a misconfiguration, certain control standards were not reviewed during an annual assessment because they were missing a date/ notification that would prompt such a review. Aetna identified the cause of the configuration issue and subsequently corrected the affected control standards so they would notify the Policy Administrator for the need to conduct an annual review. This issue has been remediated.

[redacted]

The Plan agrees with the Draft Report regarding:

- Access Controls,
- Configuration Management
- Contingency Planning,
- Claims Adjudication

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