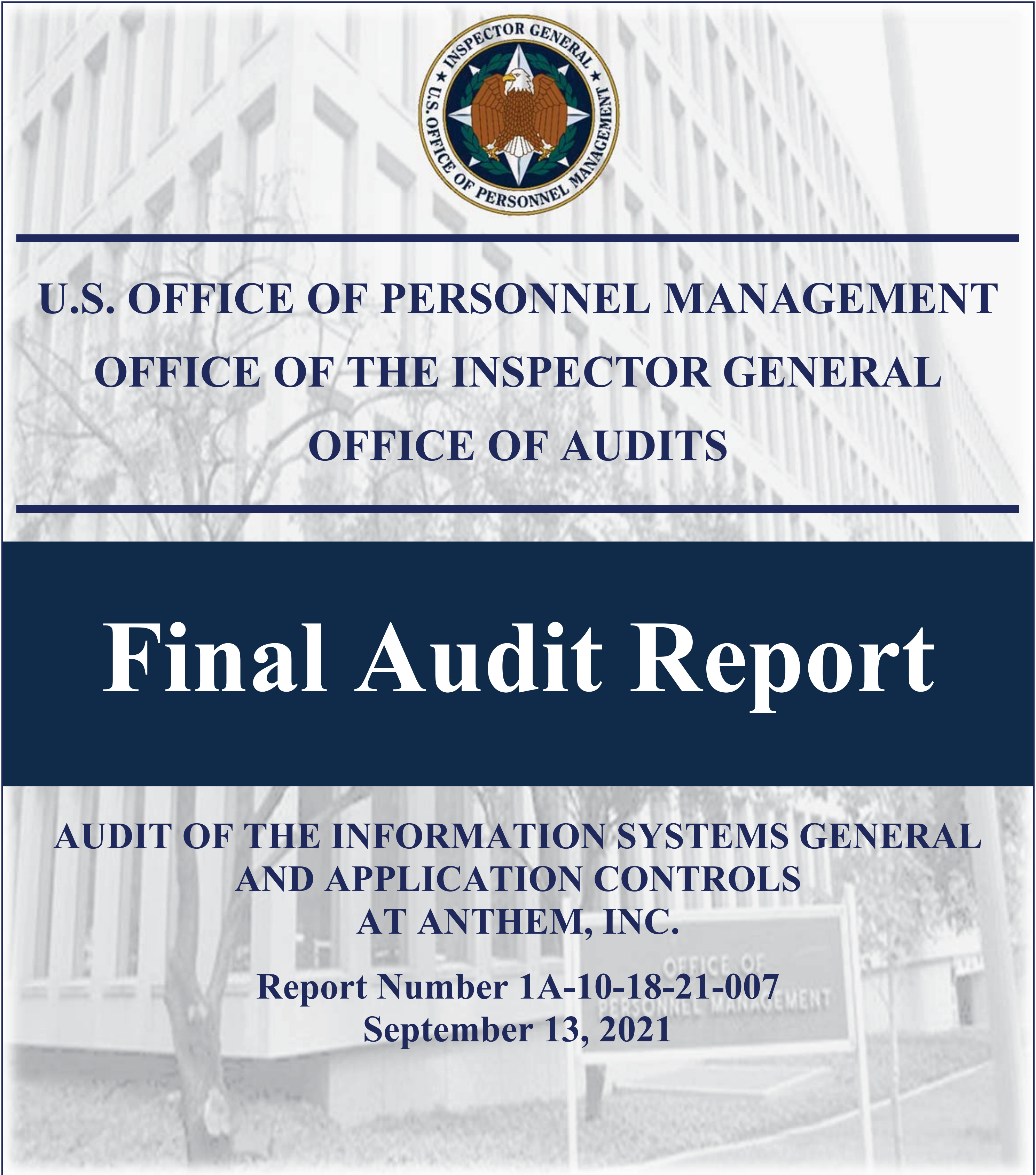

U.S. OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF THE INSPECTOR GENERAL

OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT ANTHEM, INC.

Report Number 1A-10-18-21-007
September 13, 2021

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Anthem, Inc.

Report No. 1A-10-18-21-007 **September 13, 2021**

Why Did We Conduct the Audit?

Anthem, Inc. (Anthem) 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 Anthem's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Anthem 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 Anthem's IT security controls determined that:

- Anthem has adequate controls over security management.
- Anthem has adequate logical and physical access controls.
- Our vulnerability and compliance scan exercise identified technical weaknesses in Anthem's network environment.
- Anthem has adequate event monitoring and incident response controls.
- Anthem has adequate controls over its configuration management program.
- Anthem has adequate controls over contingency planning.
- Anthem has adequate controls over its application change control process.

ABBREVIATIONS

Anthem	**Anthem, Inc.**
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

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 Anthem, Inc. (Anthem).

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 third audit of the information technology (IT) general security controls at Anthem. The previous audits of general and application controls at Anthem were conducted in 2013 and 2016. Final Audit Report No. 1A-10-00-13-012 was issued on September 10, 2013, and Final Audit Report No. 1C-SG-00-16-007 was issued on August 15, 2016. All recommendations from the previous audits have been closed.

All Anthem 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 Anthem'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 Anthem'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 Anthem'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 Anthem'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 Anthem to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Richmond, Virginia.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely from the Washington, D.C. area. The remote work performed included teleconference interviews of subject matter experts, documentation reviews, and remote testing of the general and application controls in place over Anthem's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at Anthem as of March 2021.

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

To conduct our vulnerability and compliance scan exercise, we chose a sample of [redacted] servers from a universe of approximately [redacted]. The sample selection included a variety of system functionality and operating systems across production, test, development, and disaster recovery environments. The judgmental sample was drawn from systems that store, process, or forward federal member data, as well as other systems in the same general control environment that contain 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.

In conducting this audit, we:

- Performed a risk assessment of Anthem'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 Anthem'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 Anthem's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM; and

- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 5, 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 Anthem's practices were consistent with applicable standards. While generally compliant with respect to the items tested, Anthem was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATION

A. SECURITY MANAGEMENT

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

Anthem has an adequate risk management process.

Anthem has developed adequate IT security policies and procedures. Anthem has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Anthem has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

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

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 Anthem's facilities and data center. We also examined the logical access controls protecting sensitive data in Anthem's network environment and claims processing applications.

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

- Routine access audits for secure areas;
- Procedures for appropriately granting and removing physical access to facilities and datacenters; and
- Procedures for appropriately granting and adjusting logical access to applications and software resources.

Nothing came to our attention to indicate that Anthem has not implemented adequate controls over its access control processes.

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 Anthem'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:

- Encryption techniques are used to protect the confidentiality of transmitted data;
- A deny all, permit by exception firewall policy is in place; and
- Firewalls protect the internal network from external networks.

The following section documents an opportunity for improvement related to Anthem's network security controls.

1. Vulnerability Management

Anthem is addressing technical weaknesses in its IT environment.

Anthem conducted credentialed vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. The specific vulnerabilities that we identified were provided to Anthem in the form of an audit inquiry but will not be detailed in this report. Anthem was already aware of the identified technical weaknesses, had documented mitigation plans, and implemented compensating controls until the mitigation plans could be completed. Anthem should continue working to complete its mitigation plans for the vulnerabilities we identified.

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

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

Recommendation 1

We recommend that Anthem remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during audit fieldwork.

Anthem's Response:

"Anthem agrees with the recommendation and plans to complete implementation of this by December 31, 2021."

OIG Comments:

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

D. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

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.

Our review of Anthem's security event monitoring and incident response programs identified the following controls in place:

- Documented incident response plan;
- Strategic deployment of monitoring devices to detect attacks and collect essential information; and
- Intrusion detection and prevention mechanisms at the network perimeter.

Nothing came to our attention to indicate that Anthem 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. Anthem employs a team of technical personnel who manage system software configuration for the organization. We evaluated Anthem's management of the configuration of its computer servers and databases.

Anthem has adequate controls over its configuration management program.

We observed the following controls in place:

- Documented security configuration standards;

- Routine configuration compliance reviews;
- Documented and approved exception process; and
- An established patch management process.

Nothing came to our attention to indicate that Anthem has not implemented adequate controls regarding its configuration management program.

F. CONTINGENCY PLANNING

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

Anthem has adequate controls over contingency planning.

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

- Backups of system-level and user-level data contained in information systems;
- Alternate processing site with controls equivalent to the primary site and sufficient resources to transfer and resume operations; and
- Adequately documented contingency plan.

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

G. APPLICATION CHANGE CONTROL

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

Anthem 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 related to testing and approvals of software modifications:

- Documented application change control process;
- Application change control testing; 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 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

June 18, 2021

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
Anthem Blue Cross Blue Shield (Anthem)
Audit Report Number 1A-10-18-21-007
(Dated April 20, 2021)

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

Vulnerability Management

Recommendation 1

We recommend that Anthem remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during audit fieldwork.

Plan Response

Anthem agrees with the recommendation and plans to complete implementation of this by December 31, 2021.

D. SECURITY EVENT MONITORING AND INCIDENT

No recommendation noted.

E. CONFIGURATION MANAGEMENT

No recommendation noted.

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 (202) [redacted] or [redacted] at (202) [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