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

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT KAISER FOUNDATION HEALTH PLAN, INC., NORTHERN AND SOUTHERN CALIFORNIA REGIONS

Report Number 1C-59-00-19-005
July 23, 2019

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Kaiser Foundation Health Plan, Inc., Northern California and Southern California Regions

Report No. 1C-59-00-19-005 **July 23, 2019**

Why Did We Conduct The Audit?

Kaiser Foundation Health Plan, Inc., Northern California and Southern California Regions (Kaiser of CA) 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 Kaiser of CA's information technology (IT) environment.

What Did We Audit?

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

- The Plan has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.
- Access controls appear to be appropriately provisioned, enforced, and reviewed.
- Kaiser of CA is working to strengthen [redacted].
- Kaiser of CA does not currently have [redacted].
- System configuration is controlled according to documented policies, procedures, and standards.
- Kaiser of CA has an adequate service continuity process to respond to and recover from unexpected disruptions.
- Kaiser of CA follows a standardized application development and change control process.
- Proper controls have been implemented to protect sensitive data throughout the claims adjudication process.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
COBIT	**Control Objectives for Information and Related Technologies**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
Kaiser of CA	**Kaiser Foundation Health Plan, Inc., Northern California and Southern California Regions**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
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 Kaiser Foundation Health Plan, Inc., Northern California and Southern California Regions (Kaiser of CA).

The audit was conducted pursuant to FEHBP contracts CS 1044-A and CS 1044-B; 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 second audit of the information technology (IT) general and application controls at Kaiser of CA. The previous audit resulted in Report No. 1C-59-00-09-002, dated June 18, 2009. All findings from the previous audit have been resolved.

All Kaiser of CA 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 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 Kaiser of CA's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to Kaiser of CA'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 Kaiser of CA'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 Kaiser of CA'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 Kaiser of CA to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed covered the Northern and Southern California regions and are primarily located in [redacted] and [redacted] as well as [redacted].

The onsite portion of this audit was performed in October and November of 2018. We completed additional audit work before and after the on-site visit 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 Kaiser of CA as of February 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Kaiser of CA. 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:

- Gathered documentation and conducted interviews;
- Reviewed Kaiser of CA's business structure and environment;
- Performed a risk assessment of Kaiser of CA'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); 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 Kaiser of CA's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Control Objectives for Information and Related Technologies (COBIT) 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

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

Kaiser of CA has implemented a series of formal policies and procedures that govern its security management program. The Plan has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Kaiser of CA has also implemented adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Kaiser of CA 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 Kaiser of CA's facilities and the datacenters. We also examined the logical access controls protecting sensitive data in Kaiser of CA's network environment and the Kaiser of CA claims processing applications.

Access controls appear to be appropriately provisioned, enforced, and reviewed.

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

- Procedures for appropriately managing logical and physical access to health plan facilities, datacenters, and information systems;
- Elevated access controls for high-risk privileged user accounts; and
- Routinely reviewing access rights for facilities, datacenters, and information systems.

Nothing came to our attention to indicate that Kaiser of CA has not implemented adequate controls regarding access controls.

C. NETWORK SECURITY

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. We evaluated Kaiser of CA's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans that we performed during this audit.

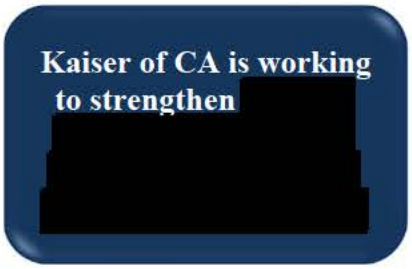
We observed the following controls in place:

- Documented firewall administration policies and procedures;
- Security event monitoring throughout the network; and
- A documented incident response program.

The following sections document opportunities for improvement related to Kaiser of CA's network security controls.

1. [redacted]

Kaiser of CA employs firewalls, intrusion prevention systems, virtual private networks, web application firewalls, and a demilitarized zone to secure connections between internal and external networks. However, there is limited [redacted]. Kaiser of CA previously identified this as an area for improvement and has a project in progress to remediate the weakness.



NIST SP 800-41, Revision 1, advises that, "[redacted]."

Failure to [redacted] increases the risk that a system could be compromised and allow unauthorized access to [redacted].

Recommendation 1

We recommend that Kaiser of CA complete its current project for the implementation of additional [redacted] systems.

Kaiser of CA Response:

"The Carrier agrees that [redacted] is an important control to [redacted] systems. The Carrier has implemented [redacted] /controls for internet facing systems, payment card systems, wireless networks, and voice systems. In addition, [redacted]. The Carrier agrees that additional [redacted] would further enhance the security of our network and continues to implement controls to further [redacted] from [redacted] systems."

OIG Comments:

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

2. [redacted]

Kaiser of CA does not have [redacted] controls to prevent [redacted] (e.g., [redacted]. However, Kaiser of CA does have a project in place to [redacted] to address this issue.

NIST SP 800-53, Revision 4, states that an [redacted]

Recommendation 2

We recommend that Kaiser of CA complete its current project to implement [redacted]

Kaiser of CA Response:

"The Carrier has implemented controls such as [redacted] controls to prevent [redacted]. The Carrier agrees that additional [redacted] controls would further enhance the security of our network and continues to implement [redacted] controls to prevent [redacted]."

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. We evaluated Kaiser of CA's policies and procedures that govern its configuration management program. We also reviewed the results of configuration compliance scans to validate the effectiveness of the security management program.

System configuration is controlled according to documented policies, procedures, and standards.

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 Kaiser of CA has not implemented adequate controls regarding its configuration management program.

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 Kaiser of CA's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to Kaiser of CA business operations when disruptive events occur:

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems."

Nothing came to our attention to indicate that Kaiser of CA 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 Kaiser of CA's claims adjudication process. Kaiser of CA prices and adjudicates claims using a locally operated claims processing application. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control over Kaiser of CA's claims processing systems.

The Plan 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:

- Policies and procedures that allow modifications to be tracked throughout the change 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 adequate controls have not been implemented over the application configuration management process.

2. Claims Processing System

We evaluated the business process controls associated with Kaiser of CA's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

Proper controls have been implemented to protect sensitive data throughout the claims adjudication process.

We determined that Kaiser of CA 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.

Nothing came to our attention to indicate that Kaiser of CA has not implemented adequate controls over its claims processing system.

3. Enrollment

We evaluated Kaiser of CA's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and is either manually or automatically 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 Kaiser of CA has not implemented adequate controls over the enrollment process.

4. Debarment

Kaiser of CA has documented procedures for reviewing the provider file for debarments and suspensions. Kaiser of CA's processing guides are based on the OPM/OIG "Guidelines for

Implementation of Federal Employees Health Benefits Program (FEHBP) Debarment and Suspension Orders." The Kaiser of CA IT department downloads the OPM OIG debarment list and performs an automated comparison with their provider records. Kaiser of CA's National Compliance Office verifies positive matches and takes appropriate action on a case-by-case basis. Kaiser of CA 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 Kaiser of CA has not implemented adequate controls over the debarment process.

APPENDIX

KAISER PERMANENTE®

May 15, 2019

Via Email ([redacted]@opm.gov)

Mr. [redacted]
Auditor-in-Charge
Information Systems Audit Group
U.S. Office of Personnel Management
Office of the Inspector General
1900 E Street N.W., Room 6400
Washington, D.C. 20415

Re: Draft Audit Report No. 1C-59-00-19-005 Information Systems General and Application at Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions

Dear Mr. [redacted]:

This letter responds to your correspondence of March 18, 2019, which enclosed a Draft of a Proposed Report (Draft Report) based on ". . . the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions (Kaiser)." Draft Report, p. 1. This response addresses recommendations in the Draft Report. Where appropriate, it also outlines corrective actions that have been taken or will be taken by Kaiser based on the recommendations.

As used in this report, "Kaiser" or the "Carrier" refers to Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions.

As you requested, we are submitting a copy of this document electronically.

I. RESPONSE TO DRAFT REPORT FINDINGS

Kaiser generally applauds the many positive observations and findings in the Draft Report, and views these as affirmation of the significant expenditures of time, effort and resources that Kaiser has undertaken to develop, build, and secure its information technology environment. In several instances, the Draft Report has helped Kaiser identify opportunities to improve the programs, processes, systems and plans it already has in place.

With regard to the opportunities for improvement identified in the Draft Report, Kaiser already has addressed or is in the process of implementing plans to address these opportunities and has provided additional details in the discussion below. Continued development and implementation of these programs may depend on budgetary constraints. We would be pleased to provide any additional information that would help satisfy concerns noted in the Draft Report.

Recommendation 1 (C. Network Security; 1. [redacted]):

Carrier Response:

The Carrier agrees that [redacted] is an important control to [redacted] systems. The Carrier has implemented segmentation/controls for internet facing systems, payment card systems, wireless networks, and voice systems. In addition, [redacted]
The Carrier agrees that additional [redacted] would further enhance the security of our network and continues to implement controls to further [redacted] from [redacted] systems.

Recommendations 2 (B. Access Controls; 3. [redacted] Controls):

Carrier Response:

The Carrier has implemented controls such as [redacted] controls to prevent [redacted]. The Carrier agrees that additional [redacted] controls would further enhance the security of our network and continues to implement [redacted] controls to prevent [redacted].

III. CONCLUSION

We appreciate this opportunity to respond to the Draft Report and urge OPM to give due consideration to the information provided in this letter.

This response contains commercial and technical information that is proprietary and confidential to the Carrier. Disclosure of this information would cause substantial harm to the Carrier's competitive position. OPM is requested to treat this document as confidential. This material is exempt from disclosure under Section 552(b)(4) of Title 5 of the United States Code.

Please do not hesitate to contact me if you have any questions or need any additional information. You can reach me at [redacted]. Thank you.

Sincerely,

[redacted]

[redacted]
Vice President, FEHBP Line of Business

cc: [redacted]

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