U.S. Office of Personnel Management

Office of the Inspector General

Office of Audits

Final Audit Report

Audit of the Information Systems General and Applications Controls at HealthPartners

Report Number 2022-ISAG-0027

March 20, 2023

Executive Summary

Audit of the Information Systems General and Application Controls at HealthPartners

Report No. 2022-ISAG-0027 **March 20, 2023**

Why Did We Conduct the Audit?

HealthPartners, plan code V3, 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 HealthPartners' information technology (IT) environment.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of HealthPartners' IT security controls determined that:

- HealthPartners [redacted].
- HealthPartners has adequate logical access controls in place.
- HealthPartners does not [redacted].
- Our vulnerability scanning exercise [redacted]
- HealthPartners' enterprise security event monitoring and incident response programs have adequate controls in place.
- Several of HealthPartners' [redacted].
- HealthPartners' contingency planning program has adequate controls in place.
- HealthPartners has adequate application change control policies and procedures.

Abbreviations

CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's 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 HealthPartners, plan code V3.

The audit was conducted pursuant to FEHBP contract CS 2875; 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 first audit of the information technology (IT) general and application security controls at HealthPartners. All HealthPartners 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 HealthPartners' 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 HealthPartners' 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 HealthPartners' 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 HealthPartners' 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 HealthPartners to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Bloomington, Minnesota.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general and application controls in place over HealthPartners' 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 HealthPartners as of October 2022.

In conducting our audit, we relied to varying degrees on computer-generated data provided by HealthPartners. 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 HealthPartners' 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 HealthPartners' 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 HealthPartners' 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 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy.

Compliance with Laws and Regulations

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

We observed the following controls in place:

- Policies and procedures that govern the security management program;
- A risk management methodology; and
- A process to create remediation plans to address weaknesses identified in risk assessments.

However, we noted the following opportunity for improvement related to HealthPartners' security management controls.

1. Role-Based Training

HealthPartners requires and provides annual IT security and privacy awareness training for all employees. Furthermore, HealthPartners provides role-based training specific to application developers. [redacted]

Recommendation 1:

We recommend that HealthPartners [redacted]

HealthPartners' Response:

"HealthPartners acknowledges [redacted]**."**

OIG Comments:

As stated above, we acknowledge that HealthPartners provides role-based training specific to application developers. [redacted].

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 HealthPartners' headquarters facility and data center. We also examined the logical access controls protecting sensitive data on HealthPartners' network environment and applications.

We observed the following controls in place:

- Procedures for appropriately granting and removing logical access to applications and software resources;
- Routine logical access reviews; and
- Routine secure area access reviews.

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

1. Data Center Physical Access

HealthPartners' primary data center is located within a building separate from its headquarters and other office buildings. Within the building, entrances to the data center areas are controlled and require multifactor authentication via access card and PIN. Not all employees that work in the building are authorized to access the data center areas where HealthPartners' sensitive information resides. [redacted]

Recommendation 2:

We recommend that HealthPartners [redacted]

HealthPartners' Response:

"HealthPartners acknowledges and has remediated. Evidence of remediation is included as an attachment with this response."

OIG Comments:

In response to the draft report, we received evidence [redacted]

[redacted].

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 HealthPartners' 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;
- Data loss prevention controls;
- 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.

[redacted].

1. Vulnerabilities Identified by OIG Scans

HealthPartners conducted credentialed vulnerability scans on a sample of servers and workstations in its network environment on our behalf. [redacted] The sample selection included a variety of system functionality and operating systems across production, test, and development environments. The judgmental sample was drawn from systems that store and/or process 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. [redacted].

[redacted]

[redacted]

Recommendation 3:

We recommend that HealthPartners [redacted]

HealthPartners' Response:

"HealthPartners acknowledges [redacted]***."***

OIG Comments:

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

2. Network Segmentation

HealthPartners uses firewalls to control connections outside of its network as well as between vendor managed systems, Payment Card Issuance systems, and external access systems.

[redacted]

[redacted]

[redacted]

Recommendation 4:

We recommend that HealthPartners [redacted].

HealthPartners' Response:

"HealthPartners acknowledges [redacted]."

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.

We observed the following controls in place:

- Controls to monitor security events throughout the network;
- Policies and standards for analyzing security events; and
- A documented incident response policy.

Nothing came to our attention to indicate that HealthPartners has not implemented adequate controls over 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. HealthPartners employs a team of technical personnel who manage system software configuration for the organization.

We observed the following controls in place:

- Documented configuration management policy; and
- Documented system change control process.

[redacted].

1. Security Configuration Settings

HealthPartners has approved security configuration settings for each operating system in its network environment. Additionally, HealthPartners has documented policies and procedures that require the implementation of these security configuration settings. Furthermore, HealthPartners conducts routine configuration scans of its servers to ensure compliance with the approved security configuration settings. However, in addition to our vulnerability scanning exercise discussed above we also conducted configuration compliance scans on the same judgmental sample of servers. Our compliance scans [redacted]

Recommendation 5:

We recommend that HealthPartners [redacted]

HealthPartners' Response:

"HealthPartners acknowledges [redacted]

F. Contingency Planning

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed HealthPartners' contingency planning documentation and processes to prevent or minimize interruptions to business operations if disruptive events were to occur.

HealthPartners has adequate controls over contingency planning.

We observed the following controls in place:

- Contingency plans including disaster recovery and business continuity plans;

- Contingency plan testing and follow-up; and
- Data center emergency response procedures.

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

G. Application Change Control

We evaluated HealthPartners' application development and change control process. HealthPartners 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:

- An adequately documented application change control process;
- Specialized training for developers; 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

HealthPartners
8170 33rd Avenue South
Bloomington, MN 55425

healthpartners.com

Mailing Address:
PO Box 1309
Minneapolis, MN 55440-1309

January 20, 2023

Julius Rios, 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: Draft Audit Report No. 2022-ISAG-0027 Information Systems General and Application Controls at HealthPartners

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

A. SECURITY MANAGEMENT

Role-Based Training

Recommendation 1
OIG recommends that HealthPartners [redacted]

Plan Response
HealthPartners acknowledges [redacted]

B. ACCESS CONTROLS

Data Center Physical Access

Recommendation 2
OIG recommends that HealthPartners [redacted]

Plan Response

HealthPartners acknowledges and has remediated. Evidence of remediation is included as an attachment with this response.

C. NETWORK SECURITY

Vulnerabilities Identified by OIG Scans

Recommendation 3

OIG recommends that HealthPartners [redacted]

Plan Response

HealthPartners acknowledges [redacted]

Network Segmentation

Recommendation 4

OIG recommends that HealthPartners [redacted]

Plan Response

HealthPartners acknowledges [redacted].

D. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

No recommendation noted.

E. CONFIGURATION MANAGEMENT

Security Configuration Settings

Recommendation 5

OIG recommends that HealthPartners [redacted]

Plan Response

HealthPartners acknowledges [redacted].

F. CONTINGENCY PLANNING

No recommendation noted.

G. APPLICATION CHANGE CONTROL

No recommendation noted.

Sincerely,

Josh M Goldman
IT Risk & Compliance
HealthPartners

Amy Mahan
Vice President
Major and National Accounts Health Solutions
HealthPartners

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/contact/hotline

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