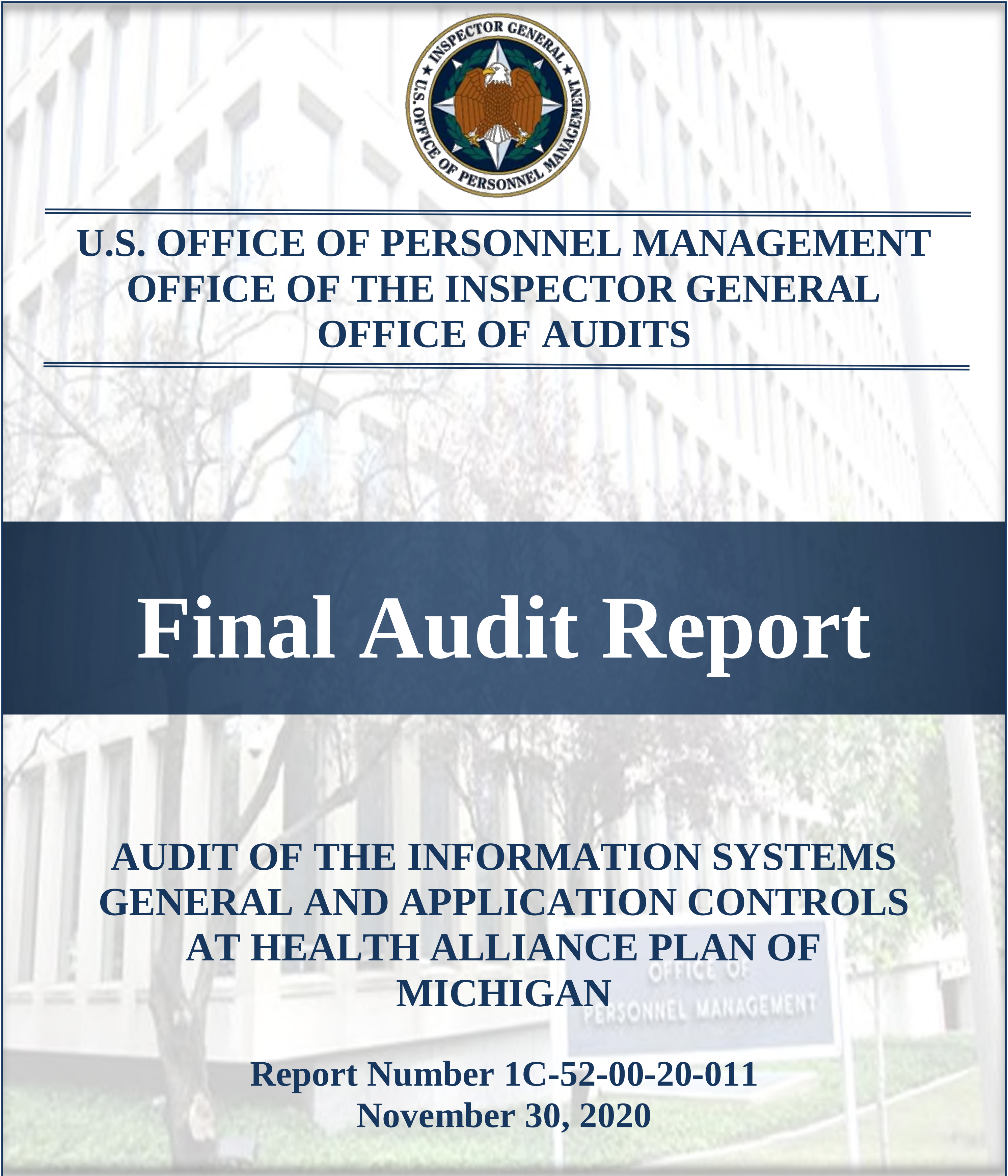


U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT HEALTH ALLIANCE PLAN OF MICHIGAN

Report Number 1C-52-00-20-011
November 30, 2020

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Health Alliance Plan of Michigan

Report No. 1C-52-00-20-011 **November 30, 2020**

Why Did We Conduct The Audit?

The Health Alliance Plan of Michigan (HAP) 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 confidentiality, integrity, and availability of FEHBP data processed and maintained in HAP's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by HAP to process and store data related to medical encounters and insurance claims for FEHBP members as of April 2020.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- [redacted]
- [redacted]
- HAP utilizes HFHS network connection guidance; however, it does not have a formal firewall policy and does not perform routine firewall configuration audits.
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- HAP has conducted disaster recovery plan tests; however, a business continuity plan test has not been conducted.
- HAP has adequate controls over the application configuration management process.

ABBREVIATIONS

BCP	**Business Continuity Plan**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
HAP	**Health Alliance Plan of Michigan**
HFHS	**Henry Ford Health System**
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

Page

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 the Health Alliance Plan of Michigan (HAP).

The audit was conducted pursuant to FEHBP contract CS 1092; 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.

HAP is a subsidiary of the Henry Ford Health System (HFHS), which offers a wide range of health care products and services in addition to its FEHB line of business. This was our first audit of general and application controls at HAP. All HAP 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 HAP'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 HAP'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 HAP'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 HAP'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 HAP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Troy, Michigan.

The onsite portion of this audit was performed in February of 2020. 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 HAP as of April 2020.

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

- GAO's FISCAM;

- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, 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 HAP's practices were consistent with applicable standards. While generally compliant with respect to the items tested, HAP 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 HAP's overall IT security program. We evaluated HAP's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

HAP utilizes 39 of HFHS's enterprise security policies for guidance on IT security. HAP also has implemented HFHS human resources policies and procedures related to hiring, training, transferring, and terminating employees.

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

1. Entity Segmentation

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 1

[redacted]

HAP's Response:

[redacted]

[redacted]

[redacted]

OIG Comment:

[redacted]

[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 the HAP facility in Troy, Michigan and at the primary data center in Detroit, Michigan. We also examined the logical access controls protecting sensitive data in HAP's network environment and claims processing applications.

The access controls observed during this audit included, but were not limited to:

- Procedures for appropriately managing logical and physical access to health plan facilities, the data center, and information systems; and

- Multi-factor authentication for user remote access.

We noted the following opportunities for improvement related to HAP's physical and logical access management program.

1. Privileged User Authentication

[redacted]

[redacted]

Recommendation 2

[redacted]

HAP's Response:

"We concur. HAP management agrees and follows NIST guidelines for password complexity and leverages multi-factor authentication for user and privileged accounts requiring remote access. [redacted]

OIG Comment:

As a part of the audit resolution process, we recommend that HAP 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 HAP agrees to implement.

2. Primary Data Center Physical Access

HAP's primary data center is located within one of the organization's facilities in Detroit, Michigan. The facility also contains office suites for employees and customer service. HAP members have the ability to enter the building during customer service hours to pay bills and receive customer support.

HAP's primary data center does not have multi-factor authentication in place at entrances to the raised floor server room.

Access to the primary data center's server room is limited to a few personnel and controlled by a proximity card reader. However, we expect data centers of all FEHBP contractors to have the following controls that were not present at HAP's primary data center:

- Multi-factor authentication to enter the secure area (e.g., cipher lock or biometric device in addition to an access card); and

- A technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, two door "man traps," etc.).

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate data center access controls increases the risk that unauthorized individuals can gain physical access to server hardware and networking equipment. Direct physical access could allow someone to bypass logical access controls and take over sensitive systems.

Recommendation 3

We recommend that HAP implement multi-factor authentication and technical or physical controls to prevent or detect piggybacking at its primary data center.

HAP's Response:

"We do not concur. Ingress/egress controls to the primary datacenter include individually assigned access control cards, monitored cameras, security guards, and audit logs that are monitored. Access to the data center is limited to a very small number of technicians and piggybacking by unauthorized individuals would be impossible to occur or go undetected."

OIG Comment:

We acknowledge that HAP has several controls in place to protect access to its primary data center. However, the primary data center is located in a publicly accessible building where customers are able to pay bills. Furthermore, the building has offices with employees that do not have a business need to access the raised floor area. Multi-factor authentication and anti-piggy backing controls protecting the raised floor are industry standard controls that reduce the risk of threat actors, especially in this type of environment. We continue to recommend that the addition of multi-factor authentication and anti-piggybacking controls should be in place at HAP's primary data center to help protect sensitive resources.

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 HAP'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 network connections;
- Encryption to protect sensitive data at rest; and
- Documented incident response procedures and testing.

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

1. Firewall Policy

HAP utilizes HFHS's firewall-related policies such as the Transmission Security and Network Access Control Policies to control network connections. However, HAP does not have a formal firewall policy or standard that identifies and documents its approved firewall configurations. NIST SP 800-41, Revision 1, identifies key elements and details of a firewall policy including:

HAP does not have a formal firewall policy.

- "[H]ow firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies"; and
- Guidance on performing risk assessments to create a list of the types of traffic needed by the organization and categorize how they must be secured – including which types of traffic can traverse a firewall under what circumstances.

NIST SP 800-41, Revision 1, also states that a firewall policy should be documented and updated frequently.

Failure to develop and maintain a detailed firewall policy could lead to improper management of critical network connections.

Recommendation 4

We recommend that HAP develop and maintain a detailed firewall policy or standard to provide guidance for securely configuring firewalls.

HAP's Response:

"We concur. HAP effectively manages firewalls. We have appropriate perimeter controls protecting public network connections; encryption to protect sensitive data at rest; and documented incident response procedures and testing. HAP's firewall configuration is monitored and reviewed on a regular basis. A formal documented firewall policy and review process will be implemented by the 4th quarter 2020."

2. **Firewall Configuration Review**

[redacted]

[redacted]

[redacted]

Recommendation 5

[redacted]

HAP's Response:

[redacted]

3. Data Exfiltration

HAP has controls in place that categorically block malicious websites and prevent malicious content from being downloaded. [redacted]

[redacted]

[redacted]

Recommendation 6

[redacted]

HAP's Response:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

OIG Comment:

[redacted]

We recommend that HAP provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence when it has fully implemented this recommendation.

4. Internal Network Segmentation

HAP uses firewalls to control connections with systems outside of its network as well as between public-facing applications and the internal network. [redacted]

[redacted]

[redacted]

[redacted]

Recommendation 7

[redacted]

HAP's Response:

[redacted]

[redacted]

[redacted]

[redacted]

OIG Comment:

[redacted]

5. Network Access Control

[redacted]

[redacted]

Recommendation 8

[redacted]

HAP's Response:

"We concur. HAP understands the importance of network security and protecting sensitive resources from internal attacks and has implemented capabilities to secure and protect the data entrusted to us. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6. Vulnerability Scanning

HAP performs routine vulnerability scans on servers in its network environment. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 9

[redacted]

HAP's Response:

"We concur. HAP performs routine vulnerability scans on servers in its network and publicly facing systems within its DMZ and remediates findings. [redacted]

7. Vulnerabilities Identified by OIG Scans

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in HAP's network environment. [redacted]

[redacted]

[redacted]

Recommendation 10

[redacted]

HAP's Response:

"We concur. HAP performs routine vulnerability scans on servers in its network and publicly facing systems within its DMZ and remediates findings. [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. HAP employs a team of technical personnel who manage system software configuration for the organization. We evaluated HAP's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented system change control process; and

- Established patch management policy.

The sections below document areas for improvement related to HAP's configuration management controls.

1. Security Configuration Standards

Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers. HAP has documented policies that require the implementation of a security configuration standard. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 11

[redacted]

HAP's Response:

"We concur. HAP follows a standard process to install and setup new systems. [redacted]

2. **Security Configuration Auditing**

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 12

[redacted]

HAP's Response:

[redacted]

3. System Lifecycle Management

The Standards Handbook for HAP Information Systems Technology details the operating system software in use at HAP. Additionally, the Software Usage Policy issues guidance on end user software. [redacted]

[redacted]

[redacted]

Recommendation 13

[redacted]

HAP's Response:

"We concur. HAP agrees and recognizes the importance of keeping technology updated and supported. [redacted]

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 HAP'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); and
- Disaster recovery plan (e.g., recovery of hardware and software infrastructure).

However, we noted the following opportunity for improvement related to HAP's contingency planning.

1. Business Continuity Plan Testing

HAP's Business Continuity Plan Provider Operations standard states that its business continuity plan (BCP) should be tested annually. However, we were told that HAP has not conducted a BCP test since the BCP was put in place in 2019.

HAP has not performed a business continuity plan test.

FISCAM states that "Testing contingency plans is essential to determining whether they will function as intended in an emergency situation."

NIST SP 800-53, Revision 4, states that "The organization tests the contingency plan at the alternate processing site … To familiarize contingency personnel with the facility and available resources; and … To evaluate the capabilities of the alternate processing site to support contingency operations."

Failure to test the plan could increase the risk that unidentified gaps prolong recovery efforts.

Recommendation 14

We recommend that HAP routinely test its BCP, document the results, and use the results to update and improve its BCP.

HAP's Response:

"We do not concur. HAP performs Disaster Recovery testing at least once per year and as part of the process HAP ensures continuity and availability of applications and systems. HAP will continue to enhance our Business Continuity Program and the continuity testing that currently happens during Disaster Recovery testing. We recognize the importance of business continuity and plan to establish a separate test cycle in addition to what occurs during the Disaster Recovery process."

OIG Comment:

We agree that HAP performs adequate disaster recovery testing of its applications and systems. However business continuity plan testing helps to ensure business operations can continue during unexpected events. For example, a disruption at the Troy, Michigan HAP location would affect claims processing business operations but would not necessarily affect the critical applications and sensitive data located at the primary data center in Detroit, Michigan. The disaster recovery tests that HAP submitted as evidence did not test business operation recovery but instead tested the recovery of technology. We continue to recommend that HAP perform routine business continuity tests to reduce the risk of business operation disruptions.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting HAP's claims adjudication process. HAP adjudicates claims using a commercial off the shelf claims processing application called Facets. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

1. Claims Processing System

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

HAP has adequate controls in place over its claims processing system

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

2. Application Change Control

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

HAP 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 and system integration 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 HAP has not implemented adequate controls over the application configuration management process.

3. Enrollment

We evaluated HAP's procedures for managing its member enrollments. 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.

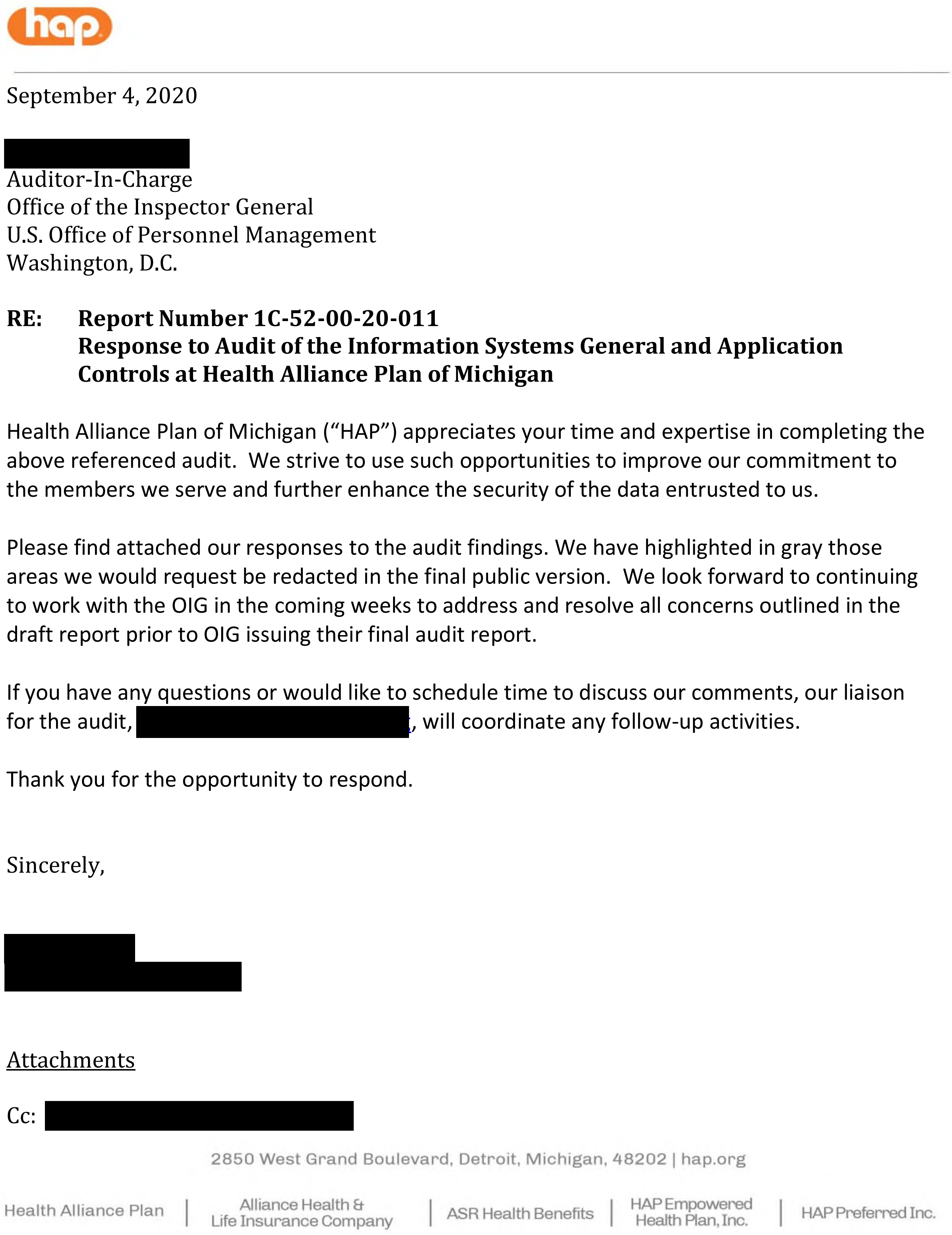
Nothing came to our attention to indicate that HAP has not implemented adequate controls over the enrollment process.

4. Debarment

HAP has documented procedures that require monitoring for debarred or suspended providers. HAP's Office of Compliance is responsible for monitoring debarments and sanctions. When the OPM debarment list is issued, HAP compares the list of debarred providers against its own providers. If a provider is debarred, HAP will update the provider record in Facets with a flag that blocks claims payment when detected by the program. HAP's policies state that it follows OPM's guidelines regarding payments to debarred providers.

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

APPENDIX



September 4, 2020

[redacted]
Auditor-In-Charge
Office of the Inspector General
U.S. Office of Personnel Management
Washington, D.C.

RE: Report Number 1C-52-00-20-011
Response to Audit of the Information Systems General and Application Controls at Health Alliance Plan of Michigan

Health Alliance Plan of Michigan ("HAP") appreciates your time and expertise in completing the above referenced audit. We strive to use such opportunities to improve our commitment to the members we serve and further enhance the security of the data entrusted to us.

Please find attached our responses to the audit findings. We have highlighted in gray those areas we would request be redacted in the final public version. We look forward to continuing to work with the OIG in the coming weeks to address and resolve all concerns outlined in the draft report prior to OIG issuing their final audit report.

If you have any questions or would like to schedule time to discuss our comments, our liaison for the audit, [redacted], will coordinate any follow-up activities.

Thank you for the opportunity to respond.

Sincerely,

[redacted]

Attachments

Cc: [redacted]

[redacted]
at Health Alliance Plan of Michigan

Recommendation 1 [redacted]

HAP Response:

[redacted]

Recommendation 2 [redacted]

HAP Response:

We concur. HAP management agrees and follows NIST guidelines for password complexity and leverages multi-factor authentication for user and privileged accounts requiring remote access. [redacted]

[redacted] and technical or physical controls to prevent or detect piggybacking at its primary datacenter.

HAP Response:
We do not concur. Ingress/egress controls to the primary datacenter include individually assigned access control cards, monitored cameras, security guards, and audit logs that are monitored. Access to the data center is limited to a very small number of technicians and piggybacking by unauthorized individuals would be impossible to occur or go undetected.

Recommendation 4: We recommend that HAP develop and maintain a detailed firewall policy or standard to provide guidance for securely configuring firewalls.

HAP Response:
We concur. HAP effectively manages firewalls. We have appropriate perimeter controls protecting public network connections; encryption to protect sensitive data at rest; and documented incident response procedures and testing. HAP's firewall configuration is monitored and reviewed on a regular basis. A formal documented firewall policy and review process will be implemented by the 4th quarter 2020.

Recommendation 5: [redacted]

HAP Response:
[redacted]

Recommendation 6: [redacted]

HAP Response:
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 7: [redacted]

HAP Response:

[redacted]

1. [redacted]

2. [redacted]

[redacted]

[redacted]

HAP Response:
We concur. HAP understands the importance of network security and protecting sensitive resources from internal attacks and has implemented capabilities to secure and protect the data entrusted to us. HAP has recently invested in two industry leading solutions to help [redacted]:

- [redacted]
- [redacted]

[redacted]

Recommendation 9: [redacted]

HAP Response:
We concur. HAP performs routine vulnerability scans on servers in its network and publicly facing systems within its DMZ and remediates findings. [redacted]

[redacted]

AP Response:
We concur. HAP performs routine vulnerability scans on servers in its network and publicly facing systems within its DMZ and remediates findings. [redacted]

Recommendation 11: [redacted]

HAP Response:
We concur. HAP follows a standard process to install and setup new systems. [redacted]

Recommendation 12: [redacted]

HAP Response:
[redacted]

Recommendation 13: [redacted]

[redacted]

We concur. HAP agrees and recognizes the importance of keeping technology updated and supported. [redacted]

[redacted]

Recommendation 14: We recommend that HAP routinely test its BCP, document the results, and use the results to update and improve its BCP.

HAP Response:
We do not concur. HAP performs Disaster Recovery testing at least once per year and as part of the process HAP ensures continuity and availability of applications and systems. HAP will continue to enhance our Business Continuity Program and the continuity testing that currently happens during Disaster Recovery testing.   We recognize the importance of business continuity and plan to establish a separate test cycle in addition to what occurs during the Disaster Recovery process.

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