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

# Final Audit Report

## AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT GEISINGER HEALTH PLAN

Report Number 1C-GG-00-20-026
March 9, 2021

# EXECUTIVE SUMMARY

*Audit of the Information Systems General Controls at Geisinger Health Plan*

**Report No. 1C-GG-00-20-026** **March 9, 2021**

**Why Did We Conduct The Audit?**

Geisinger Health Plan (GHP) 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 GHP's information technology (IT) environment.

**What Did We Audit?**

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

**What Did We Find?**

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

- GHP has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified during risk assessments.
- GHP has firewalls at the perimeter of its network to control traffic from external connections and vendors.
- GHP does not adequately segment all users from sensitive resources within the internal network.
- GHP has implemented controls to prevent non-authorized devices from connecting to its internal network.
- GHP has an established incident response program.
- GHP has documented and implemented a system change control process.
- GHP has established security configuration standards for all of its operating systems. However, GHP does not perform routine reviews of security configurations.

**Michael R. Esser**
**Assistant Inspector General for Audits**

# ABBREVIATIONS

| | |
|---|---|
| **CFR** | **Code of Federal Regulations** |
| **FEHBP** | **Federal Employees Health Benefits Program** |
| **FISCAM** | **Federal Information System Controls Audit Manual** |
| **GAO** | **U.S. Government Accountability Office** |
| **GHP** | **Geisinger Health Plan** |
| **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 controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Geisinger Health Plan (GHP).

The audit was conducted pursuant to FEHBP contract CS 2911; 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.

GHP is a subsidiary of Geisinger. Geisinger provides many centralized information technology (IT) related services to GHP. This was our first audit of the IT general security controls at GHP. All GHP 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 GHP's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Network security;
- Incident response; and
- Configuration management.

## 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 GHP'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 GHP'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 GHP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Danville, Pennsylvania.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews with GHP subject matter experts, documentation reviews, and remote testing of the general controls in place over GHP'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 GHP as of August 2020.

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

- GAO's FISCAM;

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

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

**Geisinger has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.**

GHP's parent company, Geisinger, has implemented a series of formal policies and procedures that govern the security management program for GHP. Geisinger has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

Nothing came to our attention to indicate that GHP has not implemented adequate controls related to security management.

## B. 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 GHP's controls related to network design, data protection, and systems monitoring.

GHP conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. The specific vulnerabilities that we identified were provided to GHP in the form of an audit inquiry, but will not be detailed in this report. GHP was aware of the vulnerabilities and had documented risk acceptances for the majority of identified vulnerabilities.

We also observed the following controls in place:

- Perimeter controls protecting network connections;
- Network access controls to prevent unauthorized devices on the internal network; and
- Web content filtering to protect against malicious websites.

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

## 1. Internal Network Segmentation

GHP uses firewalls to control connections with systems outside of its network. GHP also utilizes virtual local area networks and firewalls to segment high risk or non-standard devices from the rest of the network. However, GHP does not use firewalls to segment users from systems with sensitive information within the internal network.

**GHP does not use firewalls to segment users from systems with sensitive information within the internal network.**

NIST SP 800-41, Revision 1, advises that "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. Important internal systems should be placed behind internal firewalls."

Failure to adequately segregate user and server network segments increases the risk that a compromise of a user's system could allow access to sensitive servers and data.

### Recommendation 1

We recommend that GHP segregate its internal network in order to separate sensitive resources from user-controlled systems.

### GHP's Response:

***"Geisinger Health Plan appreciates the work OIG did on behalf of the Federal Employees Health Benefit Program (FEHBP). Geisinger is an Integrated Delivery Network and is uniquely positioned to provide care to our FEHBP members effectively and efficiently. Our integrated delivery network helps the Health Plan close care gaps via an integrated provider workflow; this is only possible using data sharing between the Payer and the provider organization.***

***Geisinger has taken a risk-based approach to network segmentation over the years. To that end we:***

- ***Assess applications and hardware against our security and technology standards to ensure compliance and manageability.***
- ***Segment and firewall devices that fail to meet standards but are required for business***

***and clinical operations.***

- ***Apply segmentation and firewalling to environments governed by special regulations, such as Payment Card Industry [(]PCI).***
- ***Utilize advanced endpoint protection software that identifies abnormal behavior and takes action to block nefarious activity.***
- ***Contract with a managed security service provider for 24x7x365 monitoring of all firewall and other critical IT infrastructure logs.***
- ***Manage administrative accounts using a privilege access management platform.***
- ***Utilize network intrusion prevention systems (IPS).***
- ***Utilize data loss prevention (DLP) to detect and block the unauthorized external transfer of confidential information.***

***Geisinger is utilizing a network review, commissioned with Gartner Research, to consider and potentially implement additional enhancements. At this time, due to business impact and high costs, further segmentation of the network is not planned. We continually monitor the cyber threat environment and will reconsider this option in the future."***

**OIG Comment:**

We acknowledge that GHP uses firewalls to segment devices that fail to meet security standards and environments governed by special regulations. Additionally, we acknowledge that GHP has implemented controls, such as endpoint protection, intrusion prevention systems, privilege access management controls, critical IT infrastructure log monitoring, and data loss prevention controls.

However, the purpose of this finding and recommendation is to highlight an area for improvement that we identified related to network segmentation controls. Network segmentation, and more specifically, separating users from sensitive resources, is an industry best practice that we observed during IT audits of FEHBP carriers. NIST stresses the importance of placing important internal systems behind firewalls and GHP appears to understand the importance of firewall-based segmentation considering it is used in several instances within the GHP network. Therefore, we continue to recommend that GHP segregate its internal network in order to separate sensitive resources from user-controlled systems.

## C. 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 found the following controls in place:

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

We did not identify any opportunities for improvement related to GHP's security event monitoring and incident response controls.

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

- Documented configuration standards;
- A documented system change control process; and
- An established patch management process.

However, we noted the following opportunity for improvement related to GHP's configuration management.

### 1. Security Configuration Auditing

GHP maintains "Hardening Standards" that provide guidance for securely configuring its systems. Additionally, GHP maintains "Secure Configuration Guidelines" compiled from industry best practices that identify numerous security settings GHP has chosen to enforce on its systems.

**GHP does not routinely audit its system's security settings.**

New system builds are configured in accordance with these "Hardening Standards" and "Secure Configuration Guidelines" and are enforced by Group Policy and monitored through an endpoint protection tool. However, GHP does not routinely audit its system's security settings against its "Secure Configuration Guidelines" to ensure the actual settings on its systems are compliant with the approved settings.

NIST SP 800-53, Revision 4, advises that an organization should monitor and control "changes to configuration settings in accordance with organizational policies and procedures."

FISCAM requires "Current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement a configuration compliance auditing program increases the risk that servers are not configured appropriately and, left undetected, can create a potential gateway for unauthorized access or malicious activity.

**Recommendation 2**

We recommend that GHP implement a process to routinely audit all server configuration settings to ensure compliance with the approved security configuration standards.

**GHP's Response:**

***"Geisinger Health Plan leadership has reviewed this assessment and agrees with the observation noted in the form of recommendation. Geisinger will implement a Policy Compliance module that will perform automated security configuration assessments of all Geisinger Health Plan servers - this will help reduce risk and continuously comply with internal policies and external regulations.***

***This will not be used for workstations as they are managed by a group policy (GPO) setting and use a golden image approach (i.e. an enforceable and verifiable standard).***

***Due to the need to secure funding, realign staff priorities and minimize potential impact on infrastructure performance, Geisinger anticipates completion by 12/31/2021."***

**OIG Comment:**

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

# APPENDIX

James Michaels
Vice President
Geisinger Insurance Operations
100 North Academy Avenue
Danville, PA 17822
jgmichaels@geisinger.edu

December 16, 2020

Julius Rio
Auditor-In-Charge
Information Systems Audits Group
Via E-mail Julius.Rios@opm.gov

Dear Julius,
Please find attached the response to the audit you conducted on behalf of the Office of Personnel Management, Report No. 1C-GG-00-20-026 of Geisinger Insurance Operations (GIO) a.k.a. Geisinger Health Plan (GHP).

Please feel free to contact me at the e-mail or address above with any questions.

Sincerely,

James Michaels

cc:

Kurt Wrobel, President, Geisinger Health Plan
Keith Mcree, Chief of Compliance/Chief of Staff, Insurance Operations
Mark McCullough, Chief Financial and Operating Officer, Insurance Operations
John Kravitz, SVP/Chief Information Officer
Bhaskar Chowdhury, Associate Vice President, Information Technology, Insurance Operations


**Internal Network Segmentation: Recommendation**

We recommend that GHP segregate its internal network in order to separate sensitive resources from user-controlled systems.

***Management Response***

Geisinger Health Plan appreciates the work OIG did on behalf of the Federal Employees Health Benefit Program (FEHBP). Geisinger is an Integrated Delivery Network and is uniquely positioned to provide care to our FEHBP members effectively and efficiently. Our integrated delivery network helps the Health Plan close care gaps via an integrated provider workflow; this is only possible using data sharing between the Payer and the provider organization.

Geisinger has taken a risk-based approach to network segmentation over the years. To that end we:

- Assess applications and hardware against our security and technology standards to ensure compliance and manageability.
- Segment and firewall devices that fail to meet standards but are required for business and clinical operations.
- Apply segmentation and firewalling to environments governed by special regulations, such as Payment Card Industry {PCI).
- Utilize advanced endpoint protection software that identifies abnormal behavior and takes action to block nefarious activity.
- Contract with a managed security service provider for 24x7x365 monitoring of all firewall and other critical IT infrastructure logs.
- Manage administrative accounts using a privilege access management platform.
- Utilize network intrusion prevention systems (IPS).
- Utilize data loss prevention (DLP) to detect and block the unauthorized external transfer of confidential information.

Geisinger is utilizing a network review, commissioned with Gartner Research, to consider and potentially implement additional enhancements. At this time, due to business impact and high costs, further segmentation of the network is not planned. We continually monitor the cyber threat environment and will reconsider this option in the future.


**Security Configuration Auditing: Recommendation**

We recommend that GHP implement a process to routinely audit all server configuration settings to ensure compliance with the approved security configuration standards.

***Management Response***

Geisinger Health Plan leadership has reviewed this assessment and agrees with the observation noted in the form of recommendation. Geisinger will implement a Policy Compliance module that will perform automated security configuration assessments of all Geisinger Health Plan servers - this will help reduce risk and continuously comply with internal policies and external regulations.

This will not be used for workstations as they are managed by a group policy (GPO) setting and use a golden image approach (i.e. an enforceable and verifiable standard).

Due to the need to secure funding, realign staff priorities and minimize potential impact on infrastructure performance, Geisinger anticipates completion by 12/31/2021

# 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

Report No. 1C-GG-00-20-026