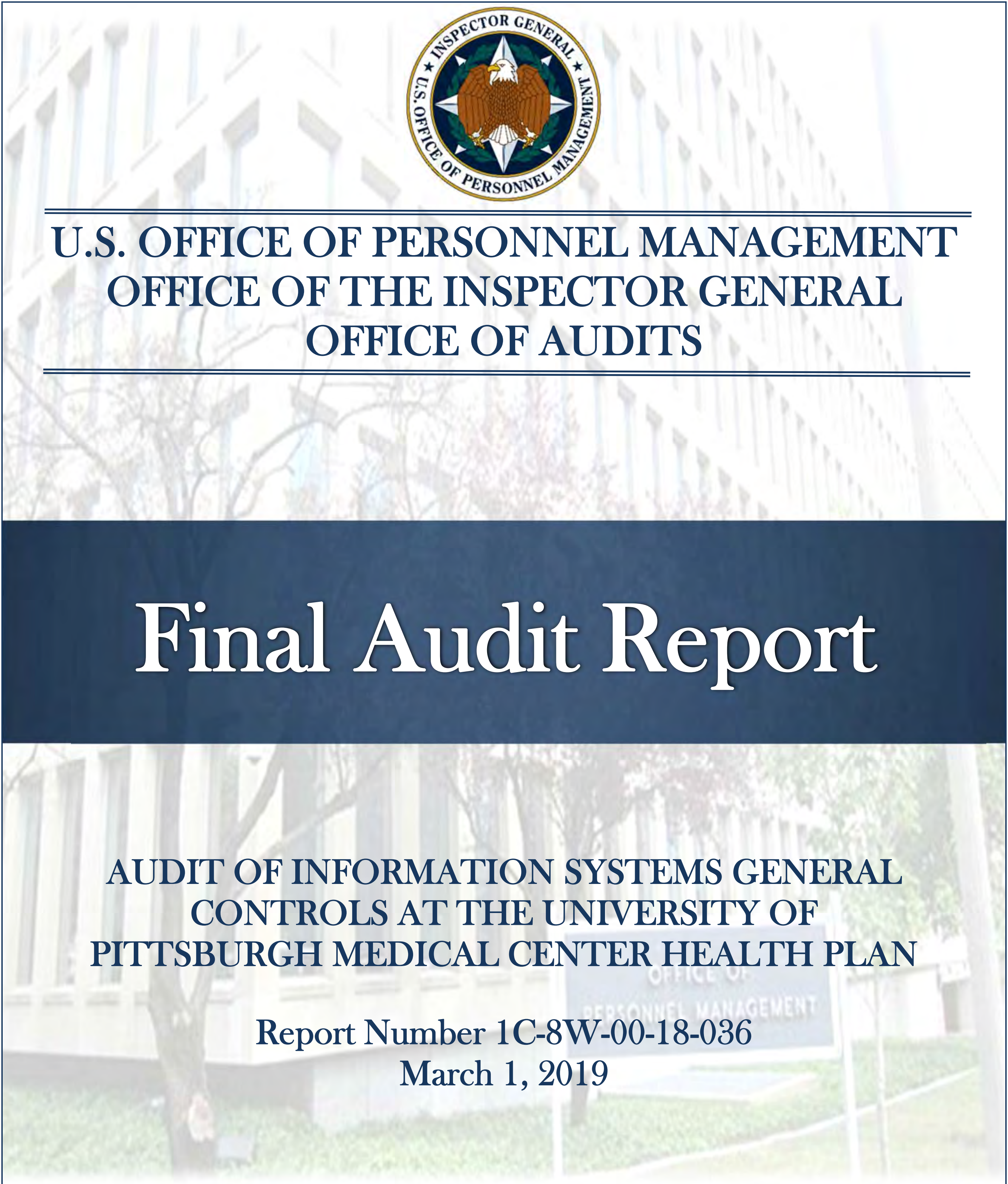

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL CONTROLS AT THE UNIVERSITY OF PITTSBURGH MEDICAL CENTER HEALTH PLAN

Report Number 1C-8W-00-18-036
March 1, 2019

EXECUTIVE SUMMARY

Audit of Information Systems General Controls at the University of Pittsburgh Medical Center Health Plan

Report No. 1C-8W-00-18-036 **March 1, 2019**

Why Did We Conduct The Audit?

The University of Pittsburgh Medical Center (UPMC) Health Plan 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 UPMC Health Plan's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by UPMC Health Plan to process and store data related to insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of UPMC Health Plan determined that:

- UPMC Health Plan has established an adequate security management program.
- UPMC Health Plan could improve its network security posture by implementing [redacted] Furthermore, vulnerability scanning could be improved by using [redacted]
- UPMC Health Plan has established an adequate security event monitoring and incident response program.
- UPMC does not maintain documented [redacted]
- UPMC does not effectively [redacted] network environment on a routine basis.

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**
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**
UPMC	**University of Pittsburgh Medical Center**

TABLE OF CONTENTS

I. BACKGROUND

This final audit 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 the University of Pittsburgh Medical Center (UPMC) Health Plan.

The audit was conducted pursuant to FEHBP contracts CS 2856; 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.

UPMC Health Plan is a subsidiary of UPMC, which offers a wide range of health care products and services in addition to its FEHBP line of business. This was our first audit of UPMC Health Plan's information technology (IT) general security controls. All UPMC Health Plan personnel that worked with the auditors were helpful and open to ideas and suggestions. 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 UPMC Health Plan's IT environments. We accomplished these objectives by reviewing the following areas:

- Security Management;
- Network Security;
- Security Event Monitoring and 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 UPMC Health Plan'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 UPMC Health Plan'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 UPMC Health Plan to process medical insurance claims and/or store the data of FEHBP members. UPMC manages many of the information technology resources and processes supporting UPMC Health Plan. Therefore, the IT operations of UPMC were considered to be within the scope of this audit. The business processes reviewed are primarily located in Pittsburgh, Pennsylvania.

The onsite portion of this audit was performed in June 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 controls in place at UPMC Health Plan and UPMC as of July 2018.

In conducting our audit, we relied to varying degrees on computer-generated data provided by UPMC Health Plan. 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 review we:

- Gathered documentation and conducted interviews;

- Reviewed UPMC Health Plan's business structure and environment;

- Performed a risk assessment of UPMC Health Plan'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 UPMC Health Plan'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 800-41, 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 UPMC Health Plan's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, UPMC Health Plan 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 UPMC Health Plan's overall IT security program. We evaluated UPMC Health Plan's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

UPMC Health Plan has implemented an adequate security management program.

UPMC Health Plan's parent company, UPMC, has implemented a series of formal policies and procedures that govern the security management program for UPMC Health Plan. UPMC 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 UPMC does not have an adequate security management program.

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. UPMC manages the technical environment that supports UPMC Health Plan's claims adjudication process; we therefore evaluated UPMC's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A documented incident response program.

The following sections document several opportunities for improvement related to UPMC's network security controls.

1. Internal Network Segmentation

Firewalls are used at ingress and egress locations on UPMC Health Plan’s network in order to control network traffic from external connections and vendors. A demilitarized zone is established to segregate externally accessible systems in UPMC Health Plan’s network. However, no [redacted]

UPMC Health Plan does not have [redacted]

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 segregate user and server network segments increases the risk that a system could be compromised and allow unauthorized access to sensitive servers and data.

Recommendation 1

We recommend that UPMC Health Plan [redacted]

UPMC Health Plan’s Response:

[redacted]

OIG Comments:

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

2. Network Access Control

UPMC Health Plan [redacted] This issue is compounded by [redacted] However, UPMC Health Plan has a project in place to install technical tools to address this issue.

NIST SP 800-53, Revision 4, states that an information system should uniquely identify and authenticate devices before establishing a network connection. Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

Recommendation 2

We recommend that UPMC Health Plan implement [redacted]

UPMC Health Plan's Response:

"UPMC will deploy [redacted] ***The*** [redacted] ***system will prevent*** [redacted]

3. Credentialed Vulnerability Scanning

UPMC performs vulnerability scanning on all company network devices including those operated by UPMC Health Plan. UPMC stated that it conducts vulnerability scanning on a routine basis using [redacted] on most systems in its network environment. Our review of historical scan reports confirmed that [redacted]

UPMC does not use [redacted]

NIST SP 800-53, Revision 4, states that the organization should implement privileged access authorization for vulnerability scanning activities. "Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning."

Failure to perform [redacted]

Recommendation 3

We recommend that UPMC [redacted] in its network environment [redacted]

UPMC Health Plan's Response:

"UPMC currently performs authenticated scanning on [redacted] of Health Plan servers. UPMC will apply [redacted]

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.

UPMC has an adequate monitoring and incident response program.

Our review found the following controls in place:

- Security event monitoring throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

Nothing came to our attention to indicate that UPMC does not have an adequate security event monitoring or incident response program.

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. UPMC employs a team of technical personnel who manage system software configuration for the organization. We evaluated UPMC'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 process.

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

1. Security Configuration Standards

UPMC does not [redacted]

UPMC maintains a standard build process for most of the operating systems in its network environment. However, UPMC does not [redacted] In addition, system owners have the authority to deviate from the standard build process if necessary [redacted]

NIST SP 800-53, Revision 4, states that an organization should establish and document “configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements … .”

Furthermore, NIST SP 800-53, Revision 4, states that the organization “Identifies, documents, and approves any deviations from established configuration settings … .”

Failure to establish approved system configuration settings increases the risk that the system may not be configured in a secure manner.

Recommendation 4

We recommend that UPMC document approved security configuration standards for all operating system platforms and databases deployed in its technical environment. Furthermore, we recommend that UPMC implement a process to document and track [redacted]

UPMC Health Plan’s Response:

“UPMC will develop [redacted] ***will be implemented*** [redacted]

2. Security Configuration Auditing

UPMC performs annual configuration reviews on most of its servers using an automated tool that maintains high-level system configurations. However, this review does not focus on security configuration settings that are typically included in a security configuration audit.

As noted above, UPMC does not have documented approved [redacted] Without approved [redacted]

UPMC does not [redacted]

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the 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 5

We recommend that UPMC improve its [redacted]

Note – this recommendation cannot be implemented until [redacted]

UPMC Health Plan's Response:

[redacted] ***UPMC will develop scan templates and processes to routinely audit the server*** [redacted]

APPENDIX

UPMC Health Plan
Quality Assurance & Operational Integrity Department
U.S. Steel Tower 600 Grant Street
5th Floor
Pittsburgh, PA 15219

December 10, 2018

[redacted], Auditor-in-Charge
Information Systems Audit Group
U.S. Office of Personnel Management
Office of the Inspector General

Reference: OPM Draft IT Report - Information Systems General Controls
University of Pittsburgh Medical Center Health Plan (UPMCHP)
Audit Report No.1C-8W-00-18-036

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

A. SECURITY MANAGEMENT

No recommendation noted.

B. NETWORK SECURITY

Recommendation 1
We recommend that UPMC Health Plan [redacted]

Plan Response
UPMC will [redacted]

Recommendation 2
We recommend that UPMC Health Plan implement [redacted]

Plan Response

UPMC will deploy [redacted] using [redacted] The [redacted]

Recommendation 3

We recommend that UPMC conduct [redacted] in its network environment [redacted]

Plan Response

UPMC currently perform authenticated scanning on [redacted] of Health Plan servers. UPMC will apply [redacted]

C. SECURITY EVENT MONITORING AND INCEIDENT RESPONSE

No recommendation noted.

D. CONFIGURATION MANAGEMENT

Recommendation 4

We recommend that UPMC [redacted] Furthermore, we recommend that UPMC implement a process to document and track [redacted]

Plan Response

UPMC will develop [redacted] will be implemented [redacted]

Recommendation 5

We recommend that UPMC improve its [redacted] Note -this recommendation cannot be implemented until the controls from Recommendation [redacted]

Plan Response

[redacted] PMC will develop scan templates and processes to routinely audit [redacted]

We appreciate the opportunity to provide our responses and request that our comments be included in their entirety and are made part of the final report.
Please contact me with question or if additional information is required.

[redacted]

[redacted]
Vice President, IT Payer Applications
UPMC Health Plan, UPMC

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