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 Medical Mutual of Ohio

Report Number 1C-UX-00-18-019
January 24, 2019

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Medical Mutual of Ohio

Report No. 1C-UX-00-18-019 **January 24, 2019**

Why Did We Conduct The Audit?

Medical Mutual of Ohio 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 Medical Mutual's information technology (IT) environment.

What Did We Audit?

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

- Medical Mutual has an adequate security management program.
- Local privileged authentication controls could be improved [redacted]
- Physical access to [redacted] could be strengthened.
- Medical Mutual's internal network [redacted]
- Technical controls to [redacted] are not in place.
- Medical Mutual has [redacted]
- Our vulnerability scans [redacted]
- Medical Mutual [redacted]
- Medical Mutual has [redacted]
- Adequate controls to continue operations are in place related to contingency planning.
- Medical Mutual has not developed policies and procedures to handle debarred providers.

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**
Medical Mutual	**Medical Mutual of Ohio**
NIST SP	**National Institute of Standards and Technology 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

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. SECURITY MANAGEMENT 5

B. ACCESS CONTROLS 5

1. Privileged User Authentication 6
2. Physical Access Controls at the Primary Data Center 7

C. NETWORK SECURITY 8

1. Internal Network Segmentation 8
2. Network Access Controls 9
3. Vulnerability Scanning 9
4. OIG Vulnerability Scanning 10

D. CONFIGURATION MANAGEMENT 11

1. Configuration Management Policy 11
2. Security Configuration Standards 12
3. Security Configuration Auditing 13
4. System Lifecycle Management 14

E. CONTINGENCY PLANNING 14

F. CLAIMS ADJUDICATION 15

1. Application Configuration Management 15
2. Claims Processing System 16
3. Enrollment 16
4. Debarment 16

APPENDIX: Medical Mutual's September 28, 2018, response to the draft audit report issued July 31, 2018.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

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 Medical Mutual of Ohio (Medical Mutual).

The audit was conducted pursuant to FEHBP contract CS 1182; 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 Medical Mutual's information technology (IT) general and application controls.

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 Medical Mutual'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 Medical Mutual'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 Medical Mutual'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 Medical Mutual'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 Medical Mutual to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Cleveland, Ohio.

The onsite portion of this audit was performed in April and May 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 Medical Mutual as of June 2018. In conducting our audit, we relied to varying degrees on computer-generated data provided by

Medical Mutual. 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 Medical Mutual's business structure and environment;
- Performed a risk assessment of Medical Mutual'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 Medical Mutual'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, Appendix III;
- 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) 800-30, 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 Medical Mutual's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Medical Mutual 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 Medical Mutual's overall IT security program. We evaluated Medical Mutual's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Medical Mutual 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. Medical Mutual has also implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Medical Mutual 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 Medical Mutual's facilities and data center located in Cleveland, Ohio. We also examined the logical access controls protecting sensitive data in Medical Mutual's network environment and applications.

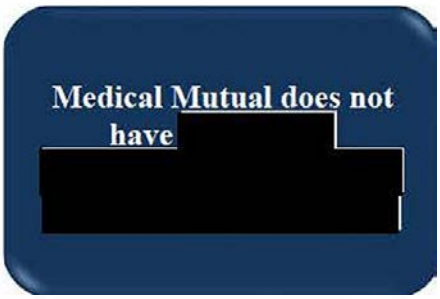
The access controls observed during this audit include, but were not limited to:

- Procedures for appropriately granting and removing physical access to facilities and the datacenter;
- Procedures for appropriately granting and adjusting logical access to applications and software resources; and
- Robust environmental controls within the primary data center;

The following sections document opportunities for improvement related to Medical Mutual's physical and logical access controls.

1. Privileged User Authentication

Medical Mutual information systems require two-factor authentication for access from outside the network. [redacted]



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

[redacted]

Recommendation 1

We recommend that Medical Mutual implement [redacted]

Medical Mutual's Response:

"Medical Mutual is in the process of expanding the capacity and capability of the existing [redacted]

OIG Comments:

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

2. Physical Access Controls at Primary Data Center

Access to the main entrance of the plan's data center facility is controlled by a security guard and turnstiles. [redacted] While this facility houses only Medical Mutual employees, not all of the employees who work in the building are authorized to [redacted]

- [redacted]
- [redacted]

NIST SP 800-53, Revision 4, provides guidance for [redacted]

Recommendation 2

We recommend that Medical Mutual implement [redacted]

Medical Mutual's Response:

"Medical Mutual is in the process of [redacted]

Recommendation 3

We recommend that Medical Mutual implement [redacted]

Medical Mutual's Response:

"Medical Mutual is in the process [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 the Medical Mutual network security program and reviewed the results of several automated vulnerability scans performed during this audit.

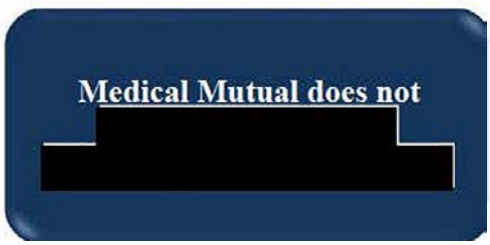
We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Security event monitoring throughout the network; and
- A documented incident response program.

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

1. Internal Network Segmentation

Medical Mutual uses a firewall to control connections with systems outside of its network [redacted]



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

Failure to [redacted] increases the risk that a compromise [redacted] could allow access to sensitive servers and data.

Recommendation 4

We recommend that Medical Mutual [redacted]

Medical Mutual's Response:

"Medical Mutual has purchased [redacted]

2. Network Access Controls

Medical Mutual [redacted]

Medical Mutual does not have [redacted]

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

Recommendation 5

We recommend that Medical Mutual implement [redacted]

Medical Mutual's Response:

"Medical Mutual will consider this as a future improvement."

3. Vulnerability Scanning

Medical Mutual has a high-level vulnerability assessment policy that requires penetration testing by a third party. We were also told that Medical Mutual employees conduct credentialed vulnerability scans on all systems in the network environment on a weekly basis. However our audit work [redacted] Our review of historical vulnerability scans indicated that several system [redacted] We also discovered that several systems [redacted]

NIST SP 800-53, Revision 4, states that the organization should scan for [redacted]

Recommendation 6

We recommend that Medical Mutual implement policies and procedures to routinely perform [redacted]

Medical Mutual's Response:

"Medical Mutual has supplied sufficient documentation to support the testing of mainframe security controls. In addition, Medical Mutual will document its policies and procedures to routinely [redacted]

OIG Comment

In response to the draft audit report, Medical Mutual has provided evidence that assessments on its mainframe are being performed. Medical Mutual should provide OPM's Healthcare and Insurance's Audit Resolution Group with evidence of the implementation of policies and procedures to [redacted]

4. OIG Vulnerability Scanning

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in Medical Mutual's network environment. The specific vulnerabilities that we identified were provided to Medical Mutual in the form of an audit inquiry, but will not be detailed in this report.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 7

We recommend that Medical Mutual remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

Medical Mutual's Response:

"As a component of the ongoing Vulnerability Management Program, the issues identified have been prioritized for remediation."

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 Medical Mutual's management of the configuration of its servers and databases. Our review found the following controls in place:

- System configuration changes are documented;
- A formal change approval process; and
- An adequate patch management process.

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

1. Configuration Management Policy

Medical Mutual [redacted]

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

[redacted]

[redacted]

Recommendation 8

We recommend that Medical Mutual document [redacted] that contains the elements recommended by NIST SP 800-53, Revision 4.

Medical Mutual's Response:

"Medical Mutual [redacted] NIST SP 800-53, Revision 4."

2. Security Configuration Standards

Medical Mutual configures its servers using a standard image for most operating systems. The images are developed internally and maintained by Medical Mutual personnel. However, Medical Mutual [redacted]

Medical Mutual does not have [redacted]

NIST SP 800-53, Revision 4, states that an organization should establish and document [redacted] ."

In addition, NIST SP 800-53, Revision 4, [redacted]

Failure to establish approved [redacted]

Recommendation 9

We recommend that Medical Mutual [redacted]

Medical Mutual's Response:

"Medical Mutual will [redacted]

3. Security Configuration Auditing

Medical Mutual [redacted]

NIST SP 800-53, Revision 4, [redacted]

FISCAM requires [redacted]

Failure to perform [redacted]

Recommendation 10

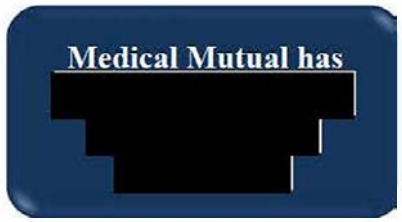
We recommend that Medical Mutual implement a process to [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 9 are in place.

Medical Mutual's Response:

"Post implementation [redacted]

4. System Lifecycle Management

Our vulnerability scanning exercise and review of Medical Mutual's system inventory [redacted]



NIST SP 800-53, Revision 4, [redacted]

Failure to [redacted]

Recommendation 11

We recommend that Medical Mutual [redacted]

Medical Mutual's Response:

[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 Medical Mutual's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to Medical Mutual 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." Medical Mutual has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that Medical Mutual has not implemented adequate controls related to contingency planning.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting Medical Mutual's claims adjudication process. Medical Mutual prices and adjudicates claims using an internally developed 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 Medical Mutual's claims processing systems.

Medical Mutual has implemented policies and procedures related to application configuration management, and 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 approval 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 Medical Mutual's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that Medical Mutual 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 Medical Mutual has not implemented adequate controls related to the application configuration management process.

3. Enrollment

We evaluated Medical Mutual's procedures for managing its database of member enrollment data. Enrollment information is received electronically and is either manually or automatically loaded into the claims processing system. The plan sends quarterly submissions to OPM for enrollment reconciliation.

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

4. Debarment

Medical Mutual has recently implemented a debarment program, including a process to update the debarred provider list. This list is not incorporated into the claims processing system, but Medical Mutual performs a monthly review to detect and withhold any payments

to debarred providers. Medical Mutual told us that they follow guidelines for grace periods, notifications, and payments. However, Medical Mutual has not documented formal procedures related to debarment.

Recommendation 12

We recommend that Medical Mutual develop formal policies and procedures related to debarment in accordance with the OPM OIG Debarment Manual, as well as with Title 5, Code of Federal Regulations, Part 890.

Medical Mutual's Response:

"Medical Mutual will develop formal policies and procedures related to debarment in accordance with the OPM OIG Debarment Manual, as well as with Title 5, Code of Federal Regulations, Part 890."

APPENDIX

MEDICAL MUTUAL OF OHIO®

Medical Mutual'

Cleveland, Ohio 44115-135

MedMutu

September 28, 2018

Medical Mutual of Ohio (Medical Mutual)

Management responses to, the Office of the Inspector General at the U.S. Office of Personnel Management (OPM). audit of Federal Employees Health Benefits Program Contract CS 1182.

Report No. lC-UX-00-18-019

Recommendation 1

We recommend that Medical Mutual implement [redacted]

Medical Mutual Response

Medical Mutual is in the process of expanding the capacity and capability of the existing [redacted]

Recommendation 2

We recommend that Medical Mutual implement [redacted]

Medical Mutual Response

Medical Mutual is in the process of [redacted]

Recommendation 3

We recommend that Medical Mutual implement [redacted]

Medical Mutual Response

Medical Mutual is in the process of [redacted]

[redacted]

Recommendation 4

We recommend that Medical Mutual [redacted]

Medical Mutual Response

Medical Mutual has purchased [redacted]

Recommendation 5

We recommend that Medical Mutual implement [redacted]

Medical Mutual Response

Medical Mutual will consider this as a future improvement.

Recommendation 6

We recommend that Medical Mutual implement policies and procedures to routinely perform [redacted]

Medical Mutual Response

Medical Mutual has supplied sufficient documentation to support the testing of mainframe security controls. In addition Medical Mutual will document its policies and procedures to [redacted]

Recommendation 7

We recommend that Medical Mutual remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

Medical Mutual Response

As a component of the ongoing Vulnerability Management Program, the issues identified have been prioritized for remediation.

Recommendation 8

We recommend that Medical Mutual [redacted] that contains the elements recommended by NIST SP 800-53, Revision 4.

Medical Mutual Response

Medical Mutual will [redacted] NIST SP 800-53, Revision 4.

Recommendation 9
We recommend that Medical Mutual [redacted]

Medical Mutual Response
Medical Mutual will [redacted]

Recommendation 10
We recommend that Medical Mutual implement a process to [redacted] Note - This recommendation cannot be implemented until the controls from Recommendation 9 are in place.

Medical Mutual Response
Post implementation of [redacted]

Recommendation 11
We recommend that Medical Mutual [redacted]

Medical Mutual Response
Medical Mutual has [redacted]

Recommendation 12
We recommend that Medical Mutual develop formal policies and procedures related to debarment accordance with the OPM OIG Debarment Manual, as well as with Title 5, Code of Federal Regulations, Part 890.

Medical Mutual Response
Medical Mutual will develop formal policies and procedures related to debarment in accordance with the OPM OIG Debarment Manual, as well as with Title 5, Code of Federal Regulations, Part 890.

John S. Kish
Executive Vice President
Chief Information Officer

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