



---

**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 SelectHealth**

**Report Number 1C-SF-00-21-005  
September 13, 2021**

# Executive Summary

Audit of the Information Systems General and Application Controls at SelectHealth

Report No. 1C-SF-00-21-005

September 13, 2021

## Why Did We Conduct the Audit?

SelectHealth 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 SelectHealth's information technology (IT) environment.

## Why Did We Audit?

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

- SelectHealth is not adequately [REDACTED] [REDACTED] are not established for [REDACTED] in SelectHealth's IT [REDACTED] to business reasons.
- SelectHealth has adequate logical access controls. However, [REDACTED]
- SelectHealth does not have a formally documented [REDACTED] process in place. Additionally, adequate [REDACTED]
- SelectHealth has adequate event monitoring and incident response controls.
- SelectHealth has multiple areas for improvement related to [REDACTED]
- SelectHealth has adequate controls over contingency planning.
- SelectHealth has adequate controls over its application change control process.

# Abbreviations

<b>CFR</b>	<b>Code of Federal Regulations</b>
<b>FEHBP</b>	<b>Federal Employees Health Benefits Program</b>
<b>FISCAM</b>	<b>Federal Information System Controls Audit Manual</b>
<b>GAO</b>	<b>U.S. Government Accountability Office</b>
<b>IMH</b>	<b>Intermountain Healthcare</b>
<b>IT</b>	<b>Information Technology</b>
<b>NIST SP</b>	<b>National Institute of Standards and Technology Special Publication</b>
<b>OIG</b>	<b>Office of the Inspector General</b>
<b>OPM</b>	<b>U.S. Office of Personnel Management</b>

# Table of Contents

<b>Executive Summary</b> .....	i
<b>Abbreviations</b> .....	ii
<b>I. Background</b> .....	1
<b>II. Objectives, Scope, and Methodology</b> .....	2
<b>III. Audit Findings and Recommendations</b> .....	4
<b>A. Security Management</b> .....	4
1. Entity Segmentation.....	4
2. Risk Acceptance.....	5
<b>B. Access Controls</b> .....	6
1. Physical Access Audit Log Reviews .....	7
2. Physical Access Appropriateness Reviews.....	8
<b>C. Network Security</b> .....	8
1. Firewall Configuration Reviews .....	9
2. Internal Network Segmentation .....	10
3. Vulnerabilities Identified by OIG Scans.....	11
<b>D. Security Event Monitoring and Incident Response</b> .....	12
<b>E. Configuration Management</b> .....	12
1. Security Configuration Standards .....	13
2. Security Configuration Auditing.....	14
3. System Lifecycle Management.....	15
4. Patch Management.....	16
<b>F. Contingency Planning</b> .....	17
<b>G. Application Change Control</b> .....	17

**Appendix:** SelectHealth’s July 6, 2021, response to the draft audit report issued May 5, 2021

**Report Fraud, Waste, and Mismangement**

# 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 SelectHealth.

The audit was conducted pursuant to FEHBP contract CS 2925; 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.

SelectHealth is a subsidiary of Intermountain Healthcare (IMH), which offers a wide range of health care products and services in addition to its FEHBP line of business. IMH is an integrated organization with two distinct entities related to the FEHBP: healthcare delivery (IMH) and a health plan (SelectHealth) organization. This was our initial audit of general and application controls at SelectHealth.

All SelectHealth 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 make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit were greatly appreciated.

# II. Objectives, Scope, and Methodology

## Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in SelectHealth's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to SelectHealth'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 SelectHealth'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 SelectHealth'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 SelectHealth to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Murray, Utah.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general and application controls in place over SelectHealth's information systems. The findings, recommendation, and conclusions outlined in this report are based on the status of information system general and application controls in place at SelectHealth as of March 2021.

In conducting our audit, we relied to varying degrees on computer-generated data provided by SelectHealth. Due to time constraints, we did not verify the reliability of the data used to

complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

We used judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of SelectHealth’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 SelectHealth’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 evaluate SelectHealth’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;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-39, Managing Information Security Risk.

## **Compliance with Laws and Regulations**

In conducting the audit, we performed tests to determine whether SelectHealth’s practices were consistent with applicable standards. While generally compliant with respect to the items tested, SelectHealth was not in complete compliance with all standards, as described in section III of this report.

# III. Audit Findings and Recommendations

## A. Security Management

The security management component of this audit involved an examination of the policies and procedures that serve as the foundation of SelectHealth’s overall IT security program. We evaluated SelectHealth’s ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.



SelectHealth and IMH have developed adequate IT security policies and procedures. SelectHealth has also developed an adequate risk management methodology that includes internal risk assessments conducted by SelectHealth and external risk assessments conducted by third parties. SelectHealth creates remediation plans to address weaknesses identified in its risk assessments.

However, we noted the following opportunities for improvement related to SelectHealth’s security management program.

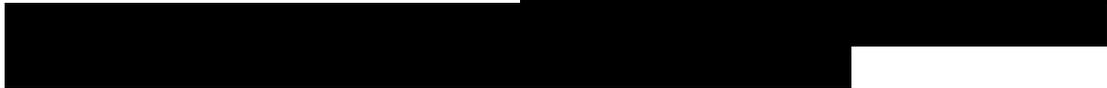
### 1. Entity Segmentation

As mentioned above, IMH, the parent company of SelectHealth, provides healthcare services to FEHPB members.



Without the use of a [redacted], the current [redacted] presents the risk [redacted]

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



NIST SP 800-53, Revision 4, states that the information system “[redacted]



## Recommendation 1

We recommend that SelectHealth implement firewall protection between its sensitive resources and network connections with IMH.

### SelectHealth's Response:

*"SelectHealth is currently evaluating*

[REDACTED]

### OIG Comments:

We acknowledge that

[REDACTED]

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

## 2. Risk Acceptance

As part of our audit, we received a complete inventory of servers in SelectHealth and

[REDACTED] was in place at the enterprise-level.

These systems

[REDACTED] business purposes. However, no evidence was provided to demonstrate that a

[REDACTED]

NIST SP 800-53, Revision 4, states that "The organization ... Provides justification and documents approval for

[REDACTED]

Furthermore, NIST SP 800-39, states that "

[REDACTED]

Additionally, NIST SP 800-39, states that [REDACTED]

Failure to [REDACTED]

## Recommendation 2

We recommend that SelectHealth [REDACTED]

### SelectHealth's Response:

*“SelectHealth has formalized, documented and is managing risk acceptance within our enterprise tracking system with [REDACTED] in our environment.”*

### OIG Comments:

We acknowledge that SelectHealth has an enterprise-level risk acceptance process. During the audit, we were provided a demonstration via video conference of this acceptance process. However, we were not provided evidence of the specific risk acceptances for the [REDACTED] we identified during this audit. We recommend that SelectHealth provide evidence to OPM's Healthcare and Insurance Office, Audit Resolution Group, that it has documented risk acceptances for the [REDACTED] we identified.

## 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 SelectHealth's facilities and data centers. We also examined the logical access controls protecting sensitive data on SelectHealth's network environment and applications.

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

- Procedures for appropriately granting and removing physical access to facilities and data centers;

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

However, we noted the following opportunities for improvement related to SelectHealth’s physical access controls.

## 1. Physical Access Audit Log Reviews

SelectHealth maintains a formal procedure requiring routine enterprise-wide physical access audits for secure data areas. However, SelectHealth does not routinely review physical access audit logs generated from badge readers for suspicious activity to secure areas such as the data centers and paper claim storage area.

NIST SP 800-53, Revision 4 states that, “The organization ... Maintains physical access audit logs for [critical entry points] ... Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof.”

Furthermore, NIST SP 800-53, Revision 4, states that, “The organization ... Reviews physical access logs [within a defined frequency] and upon occurrence of [defined events].”

Failure to review physical access audit logs increases the risk that individuals could gain unauthorized entry to secure areas without detection.

### Recommendation 3

We recommend that SelectHealth update its current procedures to include a routine process to review physical access audit logs to all secure areas within its facilities.

#### SelectHealth’s Response:

*“SelectHealth has updated current procedures to include a routine review process of physical access audit logs to secure areas within our facilities.”*

#### OIG Comments:

In response to the draft audit report, SelectHealth provided updated procedures that include a process to review physical access logs to secure areas. The intent of this recommendation has been addressed. No further action is required.

## 2. Physical Access Appropriateness Reviews

As noted above, SelectHealth maintains a formal procedure requiring routine enterprise-wide physical access audits for secure data areas, which includes the data center. However, this procedure does not apply to the secure area in which paper claims containing FEHBP member Personally Identifiable Information and Protected Health Information are stored. During the audit, we were informed that SelectHealth does not conduct routine physical access reviews for appropriateness to this secure area.

NIST SP 800-53, Revision 4, states that “Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid.”

Furthermore, FISCAM states that “Management should regularly review the list of persons authorized to have physical access to sensitive facilities, including contractors and other third parties.”

Failure to review the appropriateness of physical access to all secure areas increases the risk that an individual could gain inappropriate physical access to sensitive information.

### **Recommendation 4**

We recommend that SelectHealth update its current procedures to include a routine process to review physical access lists for appropriateness to all secure areas within its facilities.

#### **SelectHealth’s Response:**

*“SelectHealth has updated current procedures to include a routine review process of physical access lists for appropriateness to secure areas within our facilities.”*

#### **OIG Comments:**

In response to the draft audit report, SelectHealth provided updated procedures that include a routine process to review physical access lists for appropriateness to all secure areas within its facilities. The intent of this recommendation has been addressed. No further action is required.

## 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 SelectHealth’s controls related to network design, data protection,

and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during the audit.

We observed the following controls in place:

- Endpoint security controls;
- Policies and procedures to protect sensitive data at rest; and
- Network access controls to prevent unauthorized devices on the internal network.

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

### 1. Firewall Configuration Reviews

SelectHealth uses a security tool to maintain and manage approved firewall rules. The security tool creates a record and alerts SelectHealth personnel when rules are changed or added. Additionally, SelectHealth conducts annual configuration reviews comparing the approved firewall settings, managed by the security tool, to the settings actually configured on the firewalls. However,



[Redacted]

NIST SP 800-41, Revision 1, states that [Redacted]

Furthermore, NIST SP 800-41, Revision 1, states that [Redacted]

[Redacted]

#### Recommendation 5

We recommend that SelectHealth implement policies and procedures to formalize the process of performing routine audits of its [Redacted]

**SelectHealth’s Response:**

*“SelectHealth has implemented and further improved policies and procedures to formalize the process of performing routine audits of its [REDACTED] [REDACTED]”*

**OIG Comments:**

In response to the draft audit report, SelectHealth provided an updated policy that mandates routine firewall audits. However, the intent of this recommendation was to also [REDACTED]

[REDACTED] Additionally, we would like to see detailed guidance for [REDACTED]. We recommend SelectHealth implement procedures that provide more granular guidance for performing routine audits.

**2. Internal Network Segmentation**

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

[REDACTED]

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

[REDACTED]

[REDACTED]

**Recommendation 6**

We recommend that SelectHealth [REDACTED]

**SelectHealth’s Response:**

*“SelectHealth is currently [REDACTED] [REDACTED]”*

[REDACTED]

**OIG Comments:**

SelectHealth’s response is the same as the one given in response to recommendation 1.

[REDACTED]

**3. Vulnerabilities Identified by OIG Scans**

SelectHealth conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of 142 servers from a universe of 616. The sample selection included a variety of system functionality and operating systems across production, test, and development. The judgmental sample was drawn from systems that store and/or process Federal member data, as well as other systems in the same general control environment that contain Federal member data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

[REDACTED]

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

Failure to [REDACTED]

**Recommendation 7**

We recommend that SelectHealth [REDACTED]

**SelectHealth’s Response:**

*“Since the audit, SelectHealth has increased dedicated personal with sole responsibility and accountability of vulnerability management and has [REDACTED]. We have further matured tools and monitoring to help with the lifecycle management and regular [REDACTED]*

### **OIG Comments:**

In response to the draft audit report, SelectHealth provided updated procedures for server patching and software updates. We encourage SelectHealth to continue to mature its vulnerability management process. Please provide OPM's Healthcare and Insurance Office, Audit Resolution Group [REDACTED]

## **D. Security Event Monitoring and Incident Response**

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

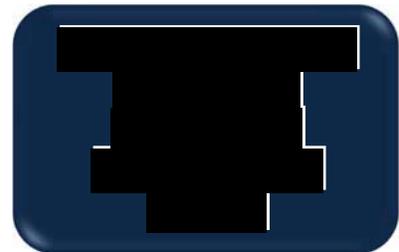
Our review of SelectHealth's security event monitoring and incident response programs identified the following controls in place:

- Security event monitoring throughout the network;
- Documented incident response procedures; and
- Incident reporting and notification procedures.

Nothing came to our attention to indicate that SelectHealth has not implemented adequate security event monitoring and incident response controls.

## **E. Configuration Management**

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. SelectHealth employs a team of technical personnel who manage system software configuration for the organization. We evaluated SelectHealth's management of the configuration of its computer servers and databases.



We observed the following controls in place:

- Documented system change control process;
- Adequate tracking of change management documentation; and

- Policy governing software installation.

However, we noted the following opportunities for improvement related to SelectHealth’s configuration management controls.

## 1. Security Configuration Standards

[REDACTED] SelectHealth has a server hardening procedure that describes the use of documented security configuration standards and has documented security configuration standards for some of its systems. However, [REDACTED]

Security configuration standards are formally approved documents that list specific security settings for each operating system that an organization uses to configure its servers.

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

In addition, NIST SP 800-53, Revision 4, states that [REDACTED]

### Recommendation 8

We recommend that SelectHealth develop, document, and maintain approved security configuration standards for [REDACTED] deployed in its IT environment.

#### SelectHealth’s Response:

*“SelectHealth has developed, documented and maintained approved security configuration standards [REDACTED].”*

**OIG Comments:**

In response to the draft audit report, SelectHealth provided documented security configuration standards for the remaining [REDACTED]. The intent of this recommendation has been addressed. No further action is required.

**2. Security Configuration Auditing**

As noted above, SelectHealth [REDACTED]

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

FISCAM requires, “Current [REDACTED] stem.”

Failure to perform [REDACTED]

**Recommendation 9**

We recommend that SelectHealth [REDACTED] to ensure compliance with approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 8 are in place.

**SelectHealth’s Response:**

*“SelectHealth has [REDACTED] to ensure compliance with approved configuration standards.*

**OIG Comments:**

In response to the draft audit report, SelectHealth provided a document titled “Server Security Configuration Standards” that describes the process for applying security configurations to servers. However, the intent of this recommendation is to ensure

SelectHealth routinely compares [REDACTED]  
[REDACTED]  
Please provide OPM's Healthcare and Insurance  
Office, Audit Resolution Group [REDACTED]  
[REDACTED] have been completed.

### 3. System Lifecycle Management

SelectHealth does not have documented policies or procedures related to system lifecycle  
[REDACTED]  
[REDACTED]  
[REDACTED]. SelectHealth informed  
us that it was aware of the [REDACTED]  
[REDACTED]  
Furthermore, while the remediation plan  
addresses the [REDACTED] currently in SelectHealth's [REDACTED]  
[REDACTED]

NIST SP 800-53, Revision 4, advises that the organization [REDACTED]  
[REDACTED]  
NIST SP 800-53, Revision 4, also states that  
[REDACTED]  
[REDACTED]

Failure to [REDACTED]  
[REDACTED]

#### Recommendation 10

We recommend that SelectHealth [REDACTED]  
[REDACTED]

#### SelectHealth's Response:

*"SelectHealth has [REDACTED]  
[REDACTED] If it is  
determined that the software is still needed, we will follow our established risk  
management process."*

**OIG Comments:**

Please provide OPM’s Healthcare and Insurance Office, Audit Resolution Group evidence demonstrating that [REDACTED]

**Recommendation 11**

We recommend that SelectHealth [REDACTED]

**SelectHealth’s Response:**

*“SelectHealth has [REDACTED]*

**4. Patch Management**

SelectHealth has established a proactive patch testing and installation schedule for [REDACTED] its operating systems. [REDACTED], newly released patches are identified during routine vulnerability scanning and then scheduled for installation based on criticality on an ad-hoc basis. SelectHealth [REDACTED]

[REDACTED] SelectHealth provided a proposal to address the issue that defines a structured patching schedule for all of its operating systems and approval to acquire additional personnel.

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

Failure to define a [REDACTED]

**Recommendation 12**

We recommend that SelectHealth [REDACTED]

**SelectHealth’s Response:**

“*SelectHealth has* [REDACTED]

**OIG Comments:**

In response to the draft audit report, SelectHealth provided evidence demonstrating the [REDACTED] The intent of this recommendation has been addressed. No further action is required.

**F. 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 SelectHealth’s contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur.

**SelectHealth has adequate controls over contingency planning.**

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

- Environmental controls to minimize disruptions;
- Documented contingency plans; and
- Documented contingency plan tests.

Nothing came to our attention to indicate that SelectHealth has not implemented adequate contingency planning controls.

**G. Application Change Control**

We evaluated the policies and procedures governing SelectHealth’s application development and change control process.

SelectHealth 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 approvals of software modifications:

- Documented system development lifecycle policy and process workflows;
- Documented application change management process; and

- Adequate documentation tracking throughout the application change management process.

Nothing came to our attention to indicate that SelectHealth has not implemented adequate controls over its application change control process.

# Appendix

SelectHealth, Inc.  
5381 South Green St.  
Salt Lake City, UT 84123

7/6/2021

Christopher Bouchey, Auditor-in-Charge  
Information Systems Audit Group  
U.S. Office of Personnel Management  
Office of the Inspector General

Reference: OPM-OIG Draft Audit Report – Information Systems General and Application Controls  
Audit Report No: 1C-SF-00-21-005

The following represents the response of SelectHealth Inc. to the recommendations included in the draft report

## A. Security Management

### 1. Entity Segmentation

#### *Recommendation 1*

We recommend that SelectHealth implement [REDACTED]

#### *Plan Response*

SelectHealth is currently evaluating [REDACTED]

### 2. Risk Acceptance

#### *Recommendation 2*

We recommend that SelectHealth [REDACTED]

#### *Plan Response*

SelectHealth has formalized, documented and is managing risk acceptance within our enterprise tracking system with [REDACTED] in our environment.

## **B. Access Controls**

### **1. Physical Access Audit Log Reviews**

#### *Recommendation 3*

We recommend that SelectHealth update its current procedures to include a routine process to review physical access audit logs to all secure areas within its facilities.

#### *Plan Response*

SelectHealth has updated current procedures to include a routine review process of physical access audit logs to secure areas within our facilities.

Note: refer to document for F3 and F4.

### **2. Physical Access Appropriateness Reviews**

#### *Recommendation 4*

We recommend that SelectHealth update its current procedures to include a routine process to review physical access lists for appropriateness to all secure areas within its facilities.

#### *Plan Response*

SelectHealth has updated current procedures to include a routine review process of physical access lists for appropriateness to secure areas within our facilities.

Note: refer to document for F3 and F4

## **C. Network Security**

### **1. Firewall Configuration Reviews**

#### *Recommendation 5*

We recommend that SelectHealth implement policies and procedures to formalize the process of performing routine audits of its current firewall configurations against its approved firewall settings.

#### *Plan Response*

SelectHealth has implemented and further improved policies and procedures to formalize the process of performing routine audits of its current firewall configurations against enterprise approved firewall settings.

Note: refer to document for F5.

## 2. Internal Network Segmentation

### *Recommendation 6*

We recommend that [REDACTED]

### *Plan Response*

SelectHealth is currently [REDACTED]

## 3. Vulnerabilities Identified by OIG Scans

### *Recommendation 7*

We recommend that SelectHealth [REDACTED]

### *Plan Response*

Since the audit, SelectHealth has increased dedicated personal with sole responsibility and accountability of vulnerability management and has [REDACTED]

[REDACTED] We have further matured tools and monitoring to help with the lifecycle management and regular [REDACTED]

Note: refer to document for F7

## D. Configuration Management

### 1. Security Configuration Standards

#### *Recommendation 8*

We recommend that SelectHealth develop, document, and maintain approved security configuration standards for [REDACTED] deployed in its IT environment.

#### *Plan Response*

SelectHealth has developed, documented and maintained approved security configuration standards for [REDACTED].

Note: refer to document for F8 and F9.

## 2. Security Configuration Auditing

### *Recommendation 9*

We recommend that SelectHealth [REDACTED] [REDACTED] to ensure compliance with approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 8 are in place.

### *Plan Response*

SelectHealth has [REDACTED] [REDACTED] to ensure compliance with approved configuration standards.

Note: refer to documentation for F8 and F9.

## 3. System Lifecycle Management

### *Recommendation 10*

We recommend that SelectHealth [REDACTED] [REDACTED]

### *Plan Response*

SelectHealth has [REDACTED] [REDACTED] If it is determined that the software is still needed, we will follow our established risk management process.

### *Recommendation 11*

We recommend that SelectHealth [REDACTED] [REDACTED]

### *Plan Response*

SelectHealth has [REDACTED] [REDACTED]

Note: Refer to document for F10 & F11.

## 4. Patch Management

### *Recommendation 12*

We recommend that SelectHealth [REDACTED] [REDACTED]

*Plan Response*

SelectHealth has [REDACTED]

Note: refer to document for F12.

Matt Christensen

Director, Payer Cybersecurity Intermountain Healthcare/SelectHealth





# 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