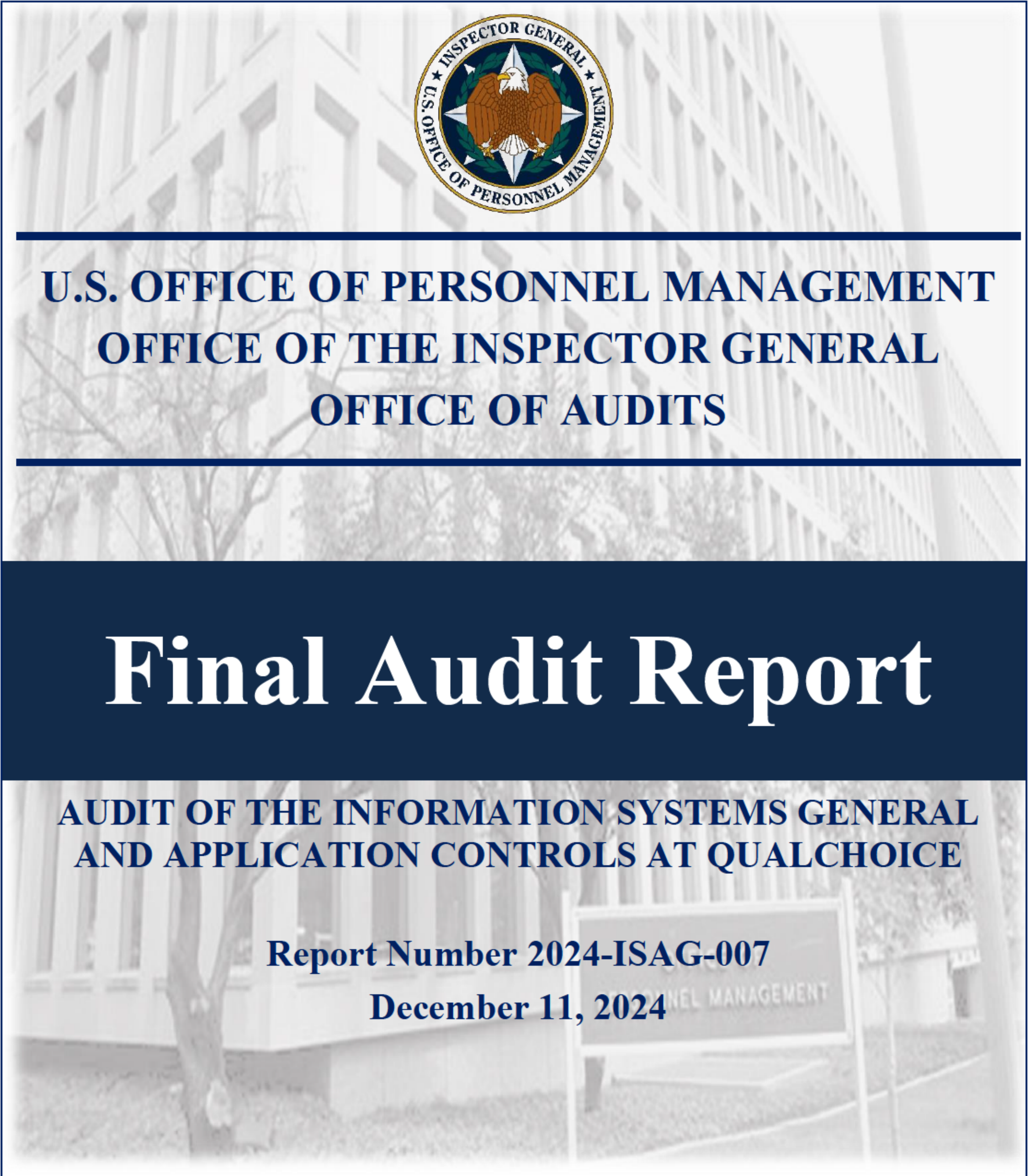

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT QUALCHOICE

Report Number 2024-ISAG-007
December 11, 2024

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at QualChoice.

Report No. 2024-ISAG-007 **December 11, 2024**

Why Did We Conduct the Audit?

QualChoice is contracted by the U.S. Office of Personnel Management to provide health insurance benefits for federal employees, annuitants, and their dependents as part of the Federal Employees Health Benefits Program (FEHBP).

The objective of this audit was to determine if QualChoice has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

What Did We Audit?

The scope of this audit included all QualChoice information systems operating in the general control environment where FEHBP data is processed and stored as of July 2024.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of QualChoice's information systems general and application controls determined that:

- QualChoice has implemented adequate enterprise security controls.
- QualChoice has implemented adequate logical access controls.
- QualChoice could improve its physical access controls by [redacted]
- QualChoice has implemented adequate data center controls.
- QualChoice could improve its network security controls by [redacted].
- Our testing identified that some QualChoice systems are missing security patches, have known exploited vulnerabilities, and unsupported software.
- QualChoice has implemented adequate security event monitoring and incident response controls.
- QualChoice has implemented adequate configuration management controls.
- QualChoice has implemented adequate contingency planning controls.
- QualChoice has implemented adequate system development lifecycle controls.

ABBREVIATIONS

Centene	Centene Corporation
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information Systems Controls Audit Manual
GAGAS	Generally Accepted Government Auditing Standards
GAO	U.S. Government Accountability Office
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management
SP	Special Publication

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

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

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. ENTERPRISE SECURITY 5

B. LOGICAL ACCESS 5

C. PHYSICAL ACCESS 6

1. [redacted] 6

D. DATA CENTER 7

E. NETWORK SECURITY 7

1. [redacted] 8

2. OIG Vulnerability Scan Results 9

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE 10

G. CONFIGURATION MANAGEMENT 10

H. CONTINGENCY PLANNING 11

I. SYSTEM DEVELOPMENT LIFECYCLE 11

APPENDIX: QualChoice's October 16, 2024, response to the draft audit report issued August 16, 2024

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of QualChoice's general and application controls over its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data is processed and stored as of July 2024.

The FEHBP was established by the Federal Employees Health Benefits Act (Public Law 86-382), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and their dependents. Health insurance coverage is made available through contracts with various health insurance carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

The provisions of the Federal Employees Health Benefits Act are implemented by the U.S. Office of Personnel Management (OPM) through regulations that are codified in Title 5, Chapter 1, Part 890 of the Code of Federal Regulations (CFR).

FEHBP contracts include provisions stating that an authorized representative of the Contracting Office may use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (or its current equivalent) requirements as a benchmark for conducting audits of a health insurance carrier's information systems and may recommend that the carrier adopt a best practice drawn from NIST SP 800-53 (or its current equivalent) to information systems that directly process FEHBP data and all other information systems in the same general IT environment.

The audit was conducted pursuant to QualChoice's FEHBP contract CS 2921; 5 U.S.C. Chapter 89; and 5 CFR Chapter 1, Part 890. The audit was performed by OPM's Office of the Inspector General (OIG), as established and authorized by the Inspector General Act of 1978, as amended.

QualChoice is a subsidiary of the Centene Corporation (Centene), which offers a wide range of health care products and services in addition to its FEHBP line of business. Additionally, QualChoice inherits some policies and procedures and IT controls from Centene.

This was our initial audit of the information systems general and application controls at QualChoice. All QualChoice and Centene 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 were greatly appreciated.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine if QualChoice has implemented adequate general and application controls over its information systems to protect the confidentiality, integrity, and availability of FEHBP data.

SCOPE AND METHODOLOGY

This audit was a performance audit conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of this audit included all QualChoice information systems operating in the general IT control environment where FEHBP data is processed and stored as of July 2024.

Due to resource limitations, we were not able to assess QualChoice's entire information systems control environment. Therefore, the scope of our work was limited to high-risk areas identified during the planning phase of our audit. Accordingly, we performed a risk assessment of QualChoice's information systems environment and applications during the planning phase of the audit to develop an understanding of QualChoice's internal controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the internal controls were properly designed, placed in operation, and effective.

Our audit program was based on procedures contained in the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) and NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

NIST SP 800-53, Revision 5, controls were selected for testing based on risk, applicability, and over-all impact to the organization's IT security posture. These controls have been organized into the following audit sections:

- Enterprise Security;
- Logical Access;
- Physical Access;
- Data Center;
- Network Security;

- Security Event Monitoring and Incident Response;
- Configuration Management;
- Contingency Planning; and
- System Development Lifecycle.

For each of our audit sections, FISCAM identifies critical elements that represent tasks essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns.

NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP 800-53, Revision 5. We used these potential assessment methods and artifacts, where appropriate, to evaluate QualChoice's internal controls. This includes interviews, observations, control tests, and inspection of computer-generated data and various documents, including IT and other related organizational policies and procedures.

When our objective involved the assessment of computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable. However, due to time constraints, we did not verify the reliability of data used to complete some of our audit steps when we determined that the evidence was adequate to achieve our audit objectives.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. Where appropriate, control tests utilized judgmental sampling methods. Results of judgmentally selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

All audit work was completed remotely. The remote work performed included staff interviews, documentation reviews, and testing of the general and application controls in place over QualChoice's information systems. The business processes reviewed are primarily located in Little Rock, Arkansas.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at QualChoice as of July 2, 2024.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether QualChoice's information system general and application controls were consistent with applicable standards. Various laws, regulations, and industry standards were used as a guide to evaluate QualChoice's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;
- NIST SP 800-41, Revision 1;
- NIST SP 800-53, Revision 5; and
- QualChoice and Centene's policies and procedures.

While generally compliant with respect to the items tested, QualChoice was not in compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. ENTERPRISE SECURITY

QualChoice has implemented adequate enterprise security controls.

Enterprise security controls include the policies, procedures, and techniques that serve as the foundation of QualChoice's overall IT security program. As discussed above in the "Background" section of this report, QualChoice is a subsidiary of Centene. As a subsidiary, QualChoice adheres to many of Centene's IT security policies and procedures in its overall IT security program that were included in the scope of this audit. We evaluated QualChoice's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

- Documented IT security policies and procedures;
- Routine information security risk assessments; and
- Routine security awareness training.

Nothing came to our attention to indicate that QualChoice has not implemented adequate enterprise security controls.

B. LOGICAL ACCESS

QualChoice provisions logical access based on a least privilege methodology.

Logical access controls include the policies, procedures, and techniques used to detect and prevent unauthorized logical access to information systems or modification, loss, and disclosure of sensitive data. We evaluated the logical access controls protecting sensitive data on QualChoice's network environment and applications supporting the FEHBP claims processing business function.

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

- Routine user access reviews;
- Multifactor authentication for remote user network access; and
- Least privilege methodology for granting access to systems and applications.

Nothing came to our attention to indicate that QualChoice has not implemented adequate logical access controls.

C. PHYSICAL ACCESS

Physical access controls include the policies, procedures, and techniques used to prevent or detect unauthorized physical access to facilities which contain information systems and sensitive data. We evaluated the controls protecting physical access to QualChoice's facilities and data centers.

QualChoice does not [redacted]

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

- Physical access to the headquarters facility is controlled using a badge access system;
- Policies and procedures for granting, adjusting, and removing physical access; and
- Physical access is granted based on least privilege.

However, we identified the following opportunity for improvement related to QualChoice's physical access controls.

1. [redacted]

During our audit we were informed that [redacted]. However, we did not receive any evidence in response to our information request demonstrating that [redacted]

NIST SP 800-53, Revision 5, [redacted]

[redacted]

Recommendation 1

We recommend that QualChoice [redacted]

QualChoice's Response:

"QualChoice will [redacted]

OIG Comment:

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

D. DATA CENTER

Data center controls include the policies, procedures, and techniques used to protect information systems from environmental damage and provide network resiliency. QualChoice utilizes a third-party vendor to host its primary data center and a different third-party vendor to provide a mobile back-up data center trailer on demand. We evaluated the controls for QualChoice's primary and back-up data centers.

QualChoice has implemented adequate data center controls.

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

- Fire detection and suppression systems in place;
- Environmental controls maintain appropriate temperature and humidity; and
- Multiple telecommunication services provide network redundancy.

Nothing came to our attention to indicate that QualChoice has not implemented adequate data center controls.

E. NETWORK SECURITY

Network security controls include the policies, procedures, and techniques used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated QualChoice's controls related to network design, data protection, and systems monitoring.

QualChoice does not have [redacted]

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

- Perimeter controls secure connections to external network connections;

- Technical controls to secure endpoint devices; and
- Network access controls to prevent non-company devices from connecting to the internal network.

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

1. [redacted]

QualChoice uses a firewall to control connections with systems outside of its network as well as between public facing web applications and the internal network. [redacted]

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

[redacted]

<u>Recommendation 2</u>

We recommend that QualChoice implement [redacted]

<u>QualChoice's Response:</u>

"QualChoice will further increase its robust network security controls by [redacted]

2. OIG Vulnerability Scan Results

QualChoice performed credentialed vulnerability scans on all its servers and a sample of 20 out of 120 workstations in its network environment on our behalf. The server and workstation sample selection included a variety of system functionality and operating systems across the production, test, and development environments. 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. The specific vulnerabilities were documented in an audit inquiry and provided to QualChoice but will not be detailed in this report. Our analysis of the scan results identified missing patches, unsupported software, and some vulnerabilities listed in the Cybersecurity & Infrastructure Security Agency's known exploited vulnerabilities catalog. QualChoice was previously aware of the specific weaknesses identified in the results and is actively working to remediate the issues.

NIST SP 800-53, Revision 5, control SI-2, states that the organization "Install security-relevant software and firmware updates within [an organization-defined time period] of the release of the updates … ." Additionally, NIST SP 800-53, Revision 5, control RA-5 states that organizations should monitor, scan, and remediate legitimate vulnerabilities.

Furthermore, NIST SP 800-53, Revision 5, control SA-22, states that the organization "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer;" or acquire an alternative source for continued support.

Failure to remediate vulnerabilities in a timely fashion increases the risk that threat actors could exploit system weaknesses for malicious purposes.

Recommendation 3

We recommend that QualChoice remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

QualChoice's Response:

"QualChoice will remediate the specific technical weaknesses discovered during this audit. Compensating controls are in place to limit any potential impact."

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Security event monitoring controls include the policies, procedures, and techniques used for 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 controls include the policies, procedures, and techniques used to establish and implement an incident response plan which defines roles and responsibilities, response procedures, training, and reporting. We evaluated QualChoice's controls related to event log collection and security incident detection, response, and reporting.

QualChoice has implemented adequate controls related to security event monitoring and incident response.

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

- Controls to monitor security events throughout the network;
- Documented incident response plans and playbooks; and
- Routine incident response testing.

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

G. CONFIGURATION MANAGEMENT

Configuration management controls include the policies, procedures, and techniques used to develop, implement, and maintain secure, risk-based system configurations and ensure that systems are configured according to these standards. We evaluated QualChoice's configuration management of its end-user devices, servers, and databases.

QualChoice has implemented adequate controls related to configuration management.

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

- Established configuration management policy;
- Documented security configuration standards; and
- Routine security configuration compliance monitoring.

Nothing came to our attention to indicate that QualChoice has not implemented adequate configuration management controls.

H. CONTINGENCY PLANNING

Contingency planning controls include the policies, procedures, and techniques that ensure continuity and recovery of critical business operations and the protection of data in the event of a service impacting event. We evaluated QualChoice's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when service impacting events occur.

QualChoice has implemented adequate contingency planning controls.

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

- Documented disaster recovery and business continuity plans;
- Routine contingency plan testing; and
- Adequate data backup process.

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

I. SYSTEM DEVELOPMENT LIFECYCLE

System development lifecycle controls include the policies, procedures, and techniques related to the secure and controlled internal development of software supporting claims adjudication and sensitive web applications. We evaluated QualChoice's software development and change control policies and procedures and controls related to secure software development.

QualChoice has implemented adequate system development lifecycle controls.

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

- Documented application change management policies and procedures;
- Documented change requests are adequately tracked; and
- Established process for testing, approvals, and auditing application changes.

Nothing came to our attention to indicate that QualChoice has not implemented adequate system development lifecycle controls.

APPENDIX

QualChoice Health Insurance
1001 Technology Drive, Suite 401
Little Rock, AR 72223

October 16, 2024

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

Reference: OPM-OIG Draft Audit Report – Information Systems General and Application Controls at QualChoice

Audit Report No: 2024-ISAG-007

The following represents QualChoice's response to the recommendations included in the draft report.

PHYSICAL ACCESS

1. [redacted]

Recommendation 1
We recommend that QualChoice [redacted]

Plan Response
QualChoice will [redacted]

NETWORK SECURITY

1. [redacted]

Recommendation 2
We recommend that QualChoice [redacted]

Plan Response
QualChoice will further increase its robust network security controls by [redacted].

2. OIG Vulnerability Scan Results

Recommendation 3

We recommend that QualChoice remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

Plan Response

QualChoice will remediate the specific technical weaknesses discovered

Jeffrey Brinsfield
Vice President, Information Technology
QualChoice

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: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100