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 HEALTH NET OF CALIFORNIA

Report Number 1C-LB-00-18-007
December 10, 2018

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Health Net of California

Report No. 1C-LB-00-18-007 **December 10, 2018**

Why Did We Conduct The Audit?

Health Net of California (Health Net) is a subsidiary of Centene Corporation (Centene) and 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 Health Net's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Health Net to process and store data related to medical encounters and insurance claims for FEHBP members. The audit also included general IT controls managed by Health Net's parent company, Centene.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of Health Net and Centene determined that:

- Centene has implemented an adequate risk assessment methodology.
- [redacted] controls to Centene information systems could be improved by requiring [redacted].
- Physical access controls could be improved to prevent unauthorized access to [redacted].
- Centene could improve its network security posture by implementing [redacted] controls.
- Centene does not have [redacted] In addition, Centene is not [redacted] of [redacted].
- Centene maintains adequate disaster recovery and business continuity plans to minimize interruptions to Health Net operations.
- The security of Centene's [redacted] could be improved by implementing [redacted].

ABBREVIATIONS

Centene	**Centene Corporation**
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**
Health Net	**Health Net of California**
IT	**Information Technology**
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**
PHI	**Protected Health Information**

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. [redacted] 6
2. [redacted] 6
3. [redacted] 7

C. NETWORK SECURITY 8
1. [redacted] 8

D. CONFIGURATION MANAGEMENT 9
1. [redacted] 9
2. [redacted] 10

E. CONTINGENCY PLANNING 11

F. CLAIMS ADJUDICATION 12
1. Application Configuration Management 12
2. Claims Processing System 13
3. Enrollment 15
4. Debarment 15

APPENDIX: Health Net's October 3, 2018, response to the draft audit report, issued August 3, 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 Health Net of California (Health Net).

The audit was conducted pursuant to FEHBP contract CS 2002; 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.

Health Net was recently acquired by Centene Corporation (Centene), which offers a wide range of health care products and services in addition to its FEHB line of business. This was our first audit of Centene and Health Net's information technology (IT) general and application controls.

During the fieldwork phase of this audit, we issued a flash audit alert to bring immediate attention to audit obstruction by Health Net (Report No. 1C-LB-00-18-023). The Plan initially refused to provide specific audit artifacts or allow us to perform our standard vulnerability and configuration compliance scanning test work. The alert included two recommendations that we believed were urgent in nature. We requested the OPM Director to require Health Net to comply with our requests. Health Net subsequently provided the requested documentation and allowed us to perform vulnerability and configuration compliance testing. Both recommendations have been closed.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVE

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Health Net'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 Health Net'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 Health Net'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 Health Net'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 Health Net to process medical insurance claims and/or store the data of FEHBP members. Centene manages many of the information technology resources and processes supporting Health Net. Therefore, the IT operations of Centene were considered to be within the scope of this audit. The business processes reviewed are primarily located in [redacted] and [redacted].

The onsite portion of this audit was performed in January and 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 and application controls in place at Centene and Health Net as of July 2018.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Health Net. 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 Health Net's business structure and environment;
- Performed a risk assessment of Health Net'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 Health Net'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: The NIST Handbook;
- 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 Health Net's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Health Net 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 Health Net's overall IT security program. We evaluated Health Net's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Health Net's parent company, Centene, has implemented a series of formal policies and procedures that govern the security management program for Health Net. Centene has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Centene has also implemented adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Centene has implemented an adequate risk management methodology.

Nothing came to our attention to indicate that Centene 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 Centene's facilities and datacenters. We also examined the logical access controls protecting sensitive data in Centene's network environment and the Health Net claims processing applications.

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

- An electronic badging system implemented to control access to facilities;
- Procedures for appropriately granting and adjusting logical access to applications and software resources; and
- Routinely reviewing user access.

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

1. [redacted]

Centene information systems require two-factor authentication for access from outside the network. [redacted] via [redacted]). The use of [redacted].

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

Recommendation 1

We recommend that Centene implement [redacted].

Centene Response:

"Centene uses [redacted]. is used [redacted]. Centene is in the process of increasing [redacted]."

OIG Comment:

As part of the audit resolution process, we recommend that Centene 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 Centene agrees to implement.

2. [redacted]

[redacted]

[redacted]. Furthermore, [redacted].

We expect all FEHBP contractors to require [redacted]).

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

Recommendation 2

We recommend that Centene [redacted].

Centene Response:

"Centene has [redacted] ***"***

3. [redacted]

Centene has documented policies and procedures for disabling physical and logical access when employees and contractors [redacted]. We were also told that Centene performs periodic reviews of existing access to certain key business information systems and facilities. These reviews are not specifically focused [redacted].

In order to verify the effectiveness of the access removal process, we requested information to perform both [redacted]

[redacted]

[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. Centene manages the technical environment that supports Health Net's claims adjudication process; we therefore evaluated Centene'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 section documents an opportunity for improvement related to Centene's network security controls.

1) [redacted]

Firewalls are used at ingress and egress locations on Centene's network in order to control network traffic from external connections and vendors. Additional virtual firewalls are implemented on the internal network to segregate certain high-risk systems including a demilitarized zone that contains externally accessible systems in Centene's network.

[redacted].

[redacted]

[redacted]

Failure to [redacted]

Recommendation 3

We recommend that Centene [redacted].

Centene Response:

"[Centene] is in agreement with the OPM recommendation. Centene's [redacted]."

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. Centene employs an information system support team that manages system software configuration for the organization. We evaluated Centene'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.

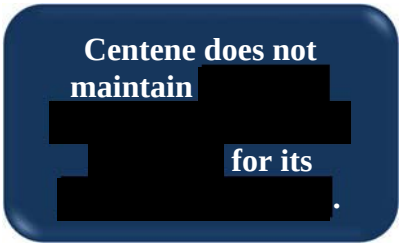
The sections below document areas for improvement related to Centene's configuration management controls.

1) [redacted]

[redacted]

Centene maintains a detailed [redacted]. Centene has implemented an

industry best practice [redacted].



Information systems that support the FEHB program [redacted].

[redacted]

Failure to [redacted].

Recommendation 4

We recommend that Centene [redacted]

Centene Response:

"Centene has implemented [redacted]

"

2) [redacted]

As noted above, Centene [redacted]

[redacted]

Recommendation 5

We recommend that Centene [redacted]

Centene Response:

"Centene has updated its policies and processes to require [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 Centene's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to Health Net business operations when disruptive events occur:

Centene maintains adequate disaster recovery and business continuity plans to minimize interruptions to Health Net operations.

- 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."

Nothing came to our attention to indicate that Centene has not implemented adequate controls over the contingency planning process.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting Health Net's claims adjudication process. Health Net prices and adjudicates claims using a locally operated claims processing application. Following the acquisition of Health Net, Centene informed us that it intends to [redacted]

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 Health Net's current claims processing systems.

Health Net's [redacted]. Centene has implemented policies and procedures related to application configuration management, and has also 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 Health Net's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that Health Net 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.

The sections below document areas for improvement related to Health Net's claims adjudication processes.

Mail Vendor Contract

Centene uses a vendor to pick up mail, including FEHBP claims, from the post office and deliver it to the mail processing facility. However, Centene does not have a formal agreement in place with the vendor that defines the responsibilities of and the services to be provided by the vendor. Centene is currently working to resolve this issue and has drafted a contract with the vendor. However, the contract is not yet formally approved.

NIST SP 800-53, Revision 4 states, "security requirements for external service providers including the security controls for external information systems are expressed in contracts or other formal agreements." Additionally, NIST SP 800-53, Revision 4 states, "Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements), organizations develop such agreements … ."

Failure to establish a contract with a vendor increases the risk that agreed-upon service standards regarding the handling of sensitive information are not met that could negatively impact business objectives and the FEHBP.

Recommendation 6

We recommend that Centene establish and approve a formal contract with the mail carrier vendor that defines requirements and responsibilities of the vendor's services.

Centene Response:

"A formal, executed agreement with the mail carrier vendor is in place."

OIG Comment:

In response to the draft audit report, Centene has provided evidence that a contract agreement with the mail vender has been completed; no further action is required.

[redacted]

According to Centene's "Physical Access Control" policy, restricted areas include areas that store or process records containing protected health information (PHI). However, during our interviews, we were told that the Centene [redacted]

The security [redacted] controls at Centene's [redacted] could be improved.

According to [redacted]

Recommendation 7

We recommend that Centene ensure [redacted]

Centene Response:

[redacted]

OIG Comment:

Centene should provide OPM's Healthcare and Insurance's Audit Resolution Group with evidence of the [redacted].

3) Enrollment

We evaluated Health Net's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and is either manually or automatically loaded into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

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

4) Debarment

Health Net has documented procedures for reviewing the provider file for debarments and suspensions. Health Net is notified by OPM OIG when an update to the debarment list is available. An automated comparison of the OPM OIG debarment list and providers within Health Net's claims processing system generates reports that will flag debarred providers. If an active provider is determined to be debarred, Health Net personnel will manually update the provider file within the claims processing system. Health Net adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

Nothing came to our attention to indicate that Health Net has not implemented adequate controls over the debarment process.

APPENDIX

Draft Audit Report Response Document
Report Number 1C-LB-00-18-007
Dated August 3, 2018
October 3, 2018

[redacted]
U.S. Office of Personnel Management
Office of the Inspector General
Theodore Roosevelt Building
1900 E St. NW Room 6400
Washington, DC 20415-1100

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

Recommendation 1
We recommend that Centene implement [redacted].

Response 1
Centene uses [redacted] is used [redacted]. Centene is in the process of increasing [redacted].

Recommendation 2
We recommend Centene [redacted].

Response 2
Centene has [redacted].

Recommendation 3

We recommend that Centene [redacted].

Response 3

[Centene] is in agreement with the OPM recommendation. Centene's [redacted].

Recommendation 4

We recommend that Centene [redacted].

Response 4

Centene has implemented [redacted].

Recommendation 5

We recommend that Centene implement a process [redacted]

Response 5

Centene has updated its policies and processes to require [redacted].

Recommendation 6

We recommend that Centene establish and approve a formal contract with the mail carrier vendor that defines requirements and responsibilities of the vendor's services.

Response 6

A formal, executed agreement with the mail carrier vendor is in place.

Recommendation 7

We recommend that Centene ensure [redacted]

Response 7

[redacted]

We appreciate the opportunity to provide our response to each of the recommendations in this report.

Sincerely,

[redacted]

[redacted] CISA

Lead IT Auditor, Internal Controls and Compliance

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