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 UNITEDHEALTHCARE

Report Number 1C-JP-00-032
January 24, 2017

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at UnitedHealthcare

Report No. 1C-JP-00-16-032 **January 24, 2017**

Why Did We Conduct the Audit?

UnitedHealthcare (UHC) 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 UHC's information technology (IT) environment.

What Did We Audit?

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

- UHC has established an adequate security management program.
- UHC has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information.
- UHC has implemented an incident response and network security program. UHC has also implemented preventative controls at the network perimeter and performs security event monitoring throughout its network. However, UHC does not perform credentialed vulnerability scans on all systems in its network environment.
- UHC has developed formal configuration management policies and baselines for its operating platforms. Furthermore, UHC has a documented change control process for the documented baseline configurations. However, the vulnerability scans that we performed as part of this audit detected isolated instances of servers that were not configured in full compliance with the established baselines.
- UHC's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. UHC also tests these plans on a routine basis.
- UHC has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Security Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
UHC	**UnitedHealthcare**

TABLE OF CONTENTS

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 UnitedHealthcare (UHC).

The audit was conducted pursuant to FEHBP contracts CS 2947, CS 2908, CS 1937, and CS 1935; 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 UHC's information technology (IT) general and application controls. All UHC 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 was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OJBECTIVES

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

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation management;
- Contingency planning; and
- Application controls specific to UHC'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 UHC's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of UHC'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 UHC to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Plymouth, Minnesota.

UHC is a subsidiary of UnitedHealth Group which offers a wide range of insurance products and services. Another subsidiary of UnitedHealth Group, Optum, manages data center operations

and information security for all UnitedHealth Group subsidiaries. The operations of Optum were considered within the scope of this audit.

The onsite portion of this audit was performed in March and April of 2016. 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 UHC as of April 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by UHC. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed UHC's business structure and environment;
- Performed a risk assessment of UHC's information systems environment and applications, and prepared an audit program based on the assessment and the 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 for evaluating UHC'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;

- 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, An Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- 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 UHC's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, UHC 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 are the foundation of UHC's overall IT security controls. We evaluated UHC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

UHC maintains a series of thorough IT security policies and procedures.

UHC has implemented a series of formal policies and procedures that comprise its security management program. UHC has developed an adequate risk management methodology, and creates remediation plans to address weaknesses identified in its risk assessments. We also reviewed UHC's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that UHC 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 of UHC's facilities and data centers located in [redacted] and [redacted], Minnesota. We also examined the logical controls protecting sensitive data in UHC's network environment and applications.

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

- Procedures for appropriately granting physical access to facilities and data centers;
- Procedures for appropriately granting, adjusting, and removing logical access;
- Routine audits of user's information system access; and

- Adequate physical and environmental controls at the data centers.

Nothing came to our attention to indicate that UHC has not implemented adequate physical and logical access controls.

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 UHC network security program and 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 thorough incident response program.

UHC performs routine automated scans on its network environment to detect vulnerabilities. However, we were told that UHC does not perform all scans with the system privileges necessary to conduct a thorough review. UHC has a corporate initiative to implement credentialed access for all server vulnerability scans and expects to complete this program by the end of 2016.

UHC does not conduct authenticated vulnerability scanning on all systems in its technical environment.

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

Failure to perform vulnerability scanning with sufficient access increases the risk that system flaws go undetected, leaving the organization exposed to security threats.

Recommendation 1

We recommend that UHC implement a process to routinely conduct *credentialed* vulnerability scans on all systems in its network environment.

UHC Response:

"UnitedHealth Group acknowledges OIG's recommendation. As discussed during the onsite review, UnitedHealth Group will continue executing existing and reasonable efforts to expand credentialed vulnerability scans on the remainder of our network environment where privileged access is reasoned appropriate. We will be more than happy to discuss additional details should OIG wish to discuss further."

OIG Comment:

As a part of the audit resolution process, we recommend that UHC provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when UHC has fully implemented this recommendation. This statement applies to the subsequent recommendation in this audit report that UHC agreed to implement.

D. CONFIGURATION MANAGEMENT

Configuration management consists of the policies and procedures used to ensure systems are configured according to approved risk-based configuration controls. We evaluated the UHC's configuration management program and observed the following controls in place:

- Standard configuration baselines;
- A thorough change management process; and
- Routine configuration compliance audits.

As part of this audit we performed credentialed vulnerability and configuration compliance assessments on a sample of servers in the UHC network. The results of our vulnerability and compliance scans indicate that several servers contain insecure configurations. We also detected isolated instances of servers that were not in compliance with established configuration baselines. The specific vulnerabilities that we identified were provided to UHC in the form of an audit inquiry, but will not be detailed in this report. UHC told us that it was aware of and already has remediation plans in place for the majority of vulnerabilities that we identified and has created remediation plans for the newly discovered vulnerabilities.

NIST SP 800-53, Revision 4, states that organizations must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate

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

Recommendation 2

We recommend that UHC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scanning audit inquiry provided directly to UHC.

UHC Response:

"UnitedHealth Group acknowledges OIG's recommendation. As discussed during the onsite, UnitedHealth Group will continue executing existing and reasonable risk mitigation efforts to address the potential weaknesses identified. We will be more than happy to discuss additional details should OIG wish to discuss further."

E. CONTINGENCY PLANNING

We reviewed the following elements of UHC's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur:

UHC maintains and routinely tests its disaster recovery and business continuity plans.

- Disaster recovery plan;
- Business continuity plan;
- Disaster recovery plan tests;
- Business continuity 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." UHC 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 UHC 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 the UHC claims adjudication process.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of UHC's claims processing systems.

UHC has implemented policies and procedures related to application configuration management, and has also adopted a thorough system development life cycle methodology that IT personnel follow during software modifications. We observed the following controls related to testing and approvals of software modifications:

- UHC has implemented practices that allow modifications to be tracked throughout the change process;
- Unit, system, and user acceptance testing are all conducted in accordance with a documented testing strategy; and
- UHC uses a business unit independent from the software developers to move the code between development and production environments to ensure adequate segregation of duties.

Nothing came to our attention to indicate that UHC has not implemented adequate controls related to the application configuration management process.

2. Claims Processing System

We evaluated the input, processing, and output controls associated with UHC's claims processing system. We determined that UHC has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail processing facilities are 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 UHC has not implemented adequate controls over its claims processing systems.

3. Enrollment

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

We do not have any concerns regarding UHC's enrollment policies and procedures.

4. Debarment

We reviewed UHC's process for reviewing provider files for debarments and suspensions. UHC downloads the OPM OIG debarment list monthly and compares the list to recently paid claims; any potential matches are reviewed and confirmed. Debarred providers are then suspended in the system. Any claim submitted by a debarred provider is flagged by UHC to adjudicate through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial.

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

APPENDIX

August 10, 2016

[redacted]
Auditor-In-Charge
Information Systems Audit Group
United States Office of Personnel Management
Washington, DC 20415

Dear [redacted]:

Thank you for the opportunity to review and respond to the Office of the Inspector General at the U.S. Office of Personnel Management report, which outlines the results of the security assessment and site visit to UnitedHealth Group in March and April, 2016. UnitedHealth Group believes the report accurately reflects the processes and controls reviewed and in place to secure and protect the Federal Employees Health Benefits Program's data. UnitedHealth Group's responses to the recommendations noted in the report are contained in the attached.

UnitedHealth Group understands the responsibility it has to protect confidential and proprietary information and to maintain availability and integrity of information systems and assets. This commitment is integral to the relationships we have with all of our customers, regulators and vendors alike.

UnitedHealth Group appreciates the opportunity to review our processes and controls to ensure the data entrusted to UnitedHealth Group is appropriately protected. We also appreciate the diligence and expertise of the individuals from the U.S. Office of Personnel Management that performed the site review. It was a pleasure working with the examination team.

We look forward to continuing to support the U.S. Office of Personnel Management with their assessment needs. Should you require any additional information, please reach out to myself or your UnitedHealthcare Representative.

Regards,

[redacted]

[redacted], *CRISC*
Sr. Director, Audit, Risk Management & Compliance UnitedHealth Group, Optum Finance
[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 UHC network security program and 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 thorough incident response program.

UHC performs routine automated scans on its network environment to detect vulnerabilities. However, we were told that UHC does not perform all scans with the system privileges necessary to conduct a thorough review. UHC has a corporate initiative to implement credentialed access for all server vulnerability scans and expects to complete this program by the end of 2016.

NIST SP 800-53, Revision 4, states that organizations should implement privileged access authorization for vulnerability scanning activities. Privileged access authorization facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning. Failure to perform vulnerability scanning with sufficient access increases the risk that system flaws go undetected leaving the organization exposed to security threats.

Recommendation 1

We recommend that UHC implement a process to routinely conduct *credentialed* vulnerability scans on all systems in its network environment.

UnitedHealth Group acknowledges OIG's recommendation. As discussed during the onsite review, UnitedHealth Group will continue executing existing and reasonable efforts to expand credentialed vulnerability scans on the remainder of our network environment where privileged access is reasoned appropriate. We will be more than happy to discuss additional details should OIG wish to discuss further.

D. Configuration Management

Configuration management consists of the policies and procedures used to ensure systems are configured according to approved risk-based configuration controls. We evaluated the UHC's configuration management program and observed the following controls in place:

- Standard configuration baselines;
- A thorough change management process; and
- Routine configuration compliance audits.

As part of this audit we performed credentialed vulnerability and configuration compliance assessments on a sample of servers in the UHC network. The results of our vulnerability and compliance scans indicate that several servers contain insecure configurations. We also detected isolated instances of servers that were not in compliance with established configuration baselines. The specific vulnerabilities that we identified were provided to UHC in the form of an audit inquiry, but will not be detailed in this report. UHC told us that it was aware of and has remediation plans in place for the majority of vulnerabilities that we identified and has created remediation plans for any newly discovered vulnerabilities.

NIST SP 800-53, Revision 4, states that organizations must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 2

We recommend that UHC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scanning audit inquiry provided directly to UHC.

UnitedHealth Group acknowledges OIG's recommendation. As discussed during the onsite, UnitedHealth Group will continue executing existing and reasonable risk mitigation efforts to address the potential weaknesses identified. We will be more than happy to discuss additional details should OIG wish to discuss further.

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