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

Final Audit Report

Subject:

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT AETNA INC.

Report No. 1C-22-00-12-065

Date: March 18, 2013

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 2900, 2867, 2914 & 1766

AETNA INC.

PLAN CODES 22 / JN / 2X / JC / HF / JR / 2U
WQ / C3 / HY / P1 / P3 / UB

HARTFORD, CONNECTICUT

Report No. 1C-22-00-12-065

Date: 03/18/13

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 2900, 2867, 2914 & 1766

AETNA INC.

PLAN CODES 22 / JN / 2X / JC / HF / JR / 2U

WQ / C3 / HY / P1 / P3 / UB

HARTFORD, CONNECTICUT

Report No. 1C-22-00-12-065

Date: 03/18/13

This final report discusses the results of our audit of general and application controls over the information systems at Aetna Inc. (Aetna or Plan). Aetna has two separate plans that service federal employees: a Health Maintenance Organization plan (HMO) referred to as "Open Access" and an individual practice plan with a consumer driven health plan option and a high deductible health plan option referred to as the "HealthFund."

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for Aetna, as well as the various processes and information technology (IT) systems used to support these applications. We documented controls in place and opportunities for improvement in each of the areas below.

Security Management

Aetna has established a series of IT policies and procedures to create an awareness of IT security at the Plan. We also verified that Aetna has adequate human resources policies related to the security aspects of hiring, training, transferring, and terminating employees.

Access Controls

Aetna has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. We also noted various controls over physical access to the data centers, as well as the method for encrypting emails containing sensitive information.

Network Security

Aetna has developed thorough network security policies and procedures around its entire operating environment. We also noted numerous hardening controls around the internal network and that Aetna conducts routine configuration reviews. Aetna's incident response policies and procedures are comprehensive and utilize software packages for incident correlation.

Configuration Management

Aetna has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes. However, we noted several weaknesses in Aetna's configuration management program related to system configuration auditing and vulnerability scanning methodology. Aetna is working to implement the necessary changes for the identified vulnerabilities.

Contingency Planning

We reviewed Aetna's business continuity plans and concluded that they contained the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis.

Claims Adjudication

Aetna has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in Aetna's claims application controls.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that Aetna is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Contents

I. Introduction

This draft 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) claims by Aetna Inc. (Aetna or Plan).

The audit was conducted pursuant to FEHBP contracts CS 2900, CS 2867, CS 2914, and CS 1766; 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.

Background

The FEHBP was established by the Federal Employees Health Benefits Act (the 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 second audit of Aetna's general and application controls. The first audit was conducted in 2001, and all recommendations from that audit were closed prior to the start of the current audit. We also reviewed Aetna's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All Aetna 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.

Objectives

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

- Security management;
- Access controls;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to Aetna's claims processing systems; and,
- HIPAA compliance.

Scope

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 Aetna'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 Aetna'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.

Aetna has two separate plans that service federal employees: a Health Maintenance Organization plan (HMO) referred to as "Open Access" and an individual practice plan with a consumer driven health plan option and a high deductible health plan option referred to as the "HealthFund."

The scope of this audit centered on the information systems used by Aetna to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. Two separate systems are used to process claims at Aetna: [redacted] system adjudicates claims for the Open Access plan and the [redacted] adjudicates claims for the HealthFund. The business processes reviewed are primarily located in Aetna's Hartford, Connecticut facilities.

The on-site portion of this audit was performed in July and August of 2012. 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 Aetna as of September 2012.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Aetna. 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.

Methodology

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed Aetna's business structure and environment;
- Performed a risk assessment of Aetna'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 to evaluating Aetna's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- 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;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and,
- HIPAA Act of 1996.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether Aetna's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Aetna was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

II. 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 Aetna's overall IT security controls. We evaluated Aetna's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Aetna has implemented a series of formal policies and procedures that comprise its security management program. Aetna's Information Security Committee is responsible for creating, reviewing, editing, and disseminating IT security policies. Aetna has also developed a thorough risk management methodology, and has procedures to document, track, and mitigate or accept identified risks. We also reviewed Aetna's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Aetna 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 Aetna's headquarters building and its data centers. We also examined the logical controls protecting sensitive data on Aetna's network environment and claims processing 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 revoking access to data centers for terminated employees;
- Procedures for removing Windows/network access for terminated employees; and,
- Controls to monitor and filter email and Internet activity.

Nothing came to our attention to indicate that Aetna has not implemented adequate controls related to 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.

Aetna has documented thorough and complete network infrastructure diagrams. Aetna has implemented a comprehensive firewall architecture in its network, and conducts routine configuration reviews of these devices. Aetna's incident response policies and procedures are comprehensive, and they have utilized software packages for incident correlation.

Nothing came to our attention to indicate that Aetna does not have an adequate network security program.

D. Configuration Management

Aetna uses two claims adjudication applications to process FEHBP claims: [redacted] for the Open Access plan and [redacted] for the HealthFund. These applications are housed in a mainframe environment. We evaluated Aetna's management of the configuration of the mainframes and the supporting [redacted] environment and determined that the following controls were in place:

- Documented and approved server and workstation builds;
- Controls for monitoring privileged user activity on the operating platform; and,
- Thorough change management procedures for system software and hardware.

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

1. Routine System Configuration Auditing

Aetna maintains an approved baseline configuration for its mainframe security software. In the fieldwork phase of our audit, we found that routine compliance auditing was not a formal process and was not documented within Aetna's security policies and procedures. Since then, Aetna has implemented a formal process for routine mainframe system configuration auditing and has documented the procedures within an approved security policy.

Aetna utilizes an approved standard build for all [redacted] Before a [redacted] is moved from the test environment to production, a one-time review is conducted to ensure configuration settings are compliant with the approved build. However, there is currently no ongoing/routine compliance check to ensure [redacted] onfigurations continue to remain in compliance with approved build sheets after [redacted] implementation.

NIST SP 800-53 Revision 3 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures. FISCAM also requires that current configuration information be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system.

Failure to routinely monitor the system configuration increases the risk the system may not meet security and performance requirements defined in the established documentation.

Recommendation 1

We recommend that Aetna implement a methodology to routinely monitor the configuration of [redacted] to the approved build documentation.

Aetna Response:

"Aetna will implement a methodology that includes:

- ***Establish configuration baselines***
- ***Schedule scans to determine deviation from baseline***
- ***Establish a risk based approach for remediation of configuration deviations***

Closure ETA: Management has presented an issue closure plan by 01/31/2013. [redacted]

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's Healthcare and Insurance Office (HIO) with evidence that configuration baselines have been established, scans have been conducted, and deviations have been remediated.

2. Vulnerability Scanning

a. Full-scope Vulnerability Scanning

Aetna conducts periodic vulnerability scans on its information systems using automated tools, and contracts a third party vendor to conduct external scans. Aetna scans several specific [redacted] on a weekly basis, but only scans the remainder [redacted] on an informal ad hoc basis. Aetna's network infrastructure is large and we understand that it may be unreasonable for Aetna to frequently scan its entire environment. However, we were not able to independently confirm whether [redacted] had ever been subject to previous vulnerability scans.

[redacted]

Recommendation 2

We recommend that Aetna implement a process to conduct routine vulnerability scans on its entire [redacted] environment.

Aetna Response:

"Aetna currently utilizes a risk based approach in support of completing vulnerability assessments by focusing its scanning resources to high risk environments. As a result, these environments are scanned with significant rigor by both Aetna and externally contracted partners. Currently, Aetna's internal trusted network is subjected to annual and ad hoc assessments that scan [redacted] ***and provide results with remediation advice to the system owners responsible for remediation.***

To evolve Aetna's strategic vulnerability management program in 2012, the investment of deploying a scanning technology framework across the enterprise was achieved. Aetna's strategic vision of its vulnerability management program further evolved in 2012 due to the integration effort of the scanning infrastructure into the IT GRC (Governance, Risk and Compliance) tool. Integrating vulnerability scan results into the IT GRC tool will provide increased risk management oversight for remediation and prioritization. This new vulnerability management program will establish a strategic foundation for findings management and remediation workflow by providing data to assess and deploy timely patches across the enterprise... This accomplishment will allow for the management of more frequent scanning and drive timely implementation of system patches.

Aetna will implement a methodology that includes:

- ***Aetna has continued to expand its vulnerability management program to other environments with the solution in place as of 1/31/201[3].***
- ***To complete the migration of its strategic vulnerability management program, Aetna is scheduled to include all [redacted] within the Internal Trusted network [redacted]"***

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's HIO with evidence that vulnerability scans are routinely conducted on the entire [redacted] environment.

b. System Patching

Aetna has documented patch management policies and procedures. However, the results of our [redacted]

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." [redacted] Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously."

Although the servers we scanned are protected by firewalls and other threat mitigation technologies, [redacted] sensitive information could be stolen.

Recommendation 3

We recommend that Aetna implement a methodology to ensure that [redacted]

Aetna Response:

"Aetna will continue to evolve its enterprise vulnerability management program, enabling more stringent oversight and communication with system owners on vulnerability findings and remediation expectations.

Aetna will implement a methodology that includes:

- ***Review of current [redacted] patching process to identify gaps***
- ***Refinement of [redacted] patching process***
- ***Post-implementation scan to ensure successful completion of upgrades***

[redacted]

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's HIO with evidence of its improved methodology to ensure that [redacted] are installed with appropriate [redacted].

c. Noncurrent Software

The results of our vulnerability scans indicated that [redacted] s contained noncurrent software applications that were no longer supported by the vendors and may have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 4

We recommend that Aetna implement a methodology to ensure that only current and supported versions of system software are installed on the [redacted]

Aetna Response:

"Aetna will implement a methodology that includes:

- ***Review of current [redacted] software patching process to identify gaps***
- ***Refinement of [redacted] software patching process***
- ***Schedule of scans***
- ***Establish a risk based approach for remediation of non-current and unsupported software***

Closure ETA: Management has submitted an issue closure plan by 01/31/2013. Closure target date was presented as part of the closure plan."

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's HIO with evidence of its improved methodology to ensure that only current and supported versions of system software are installed on the [redacted]

d. Unnecessary Applications

The results of our vulnerability scans indicated that [redacted] contained third-party applications [redacted] that were not likely essential to the functionality of that server.

NIST SP 800-53 Revision 3 states that the organization should configure the information system to provide only essential capabilities. An organization should also review the information system to identify and eliminate unnecessary functions.

Installing unnecessary software to an information system can increase the amount of exposed vulnerabilities and methods an intruder can use to gain unauthorized access to the system.

Recommendation 5

We recommend that Aetna review its current system configuration to ensure that only necessary software is installed on its [redacted]

Aetna Response:

"Aetna will implement a methodology that includes:

- ***Schedule of scans to identify unnecessary software installations***
- ***Establish a risk based approach for removal of unnecessary software.***

Closure ETA: Management has presented an issue closure plan by 01/31/2013. Closure target date was presented as part of the closure plan."

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's HIO with evidence of its improved methodology to ensure that only necessary software is installed on its [redacted]

E. Contingency Planning

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

- Disaster response plan;
- Business continuity plan for data center operations;
- Business continuity plans for claims processing operations and claims support;
- Disaster recovery plan tests conducted in conjunction with the alternate data center; and,

- Emergency response procedures and training.

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems." Aetna 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 Aetna 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 Aetna's claims adjudication process.

1. Application Configuration Management

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

Aetna 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:

- Aetna has adopted practices that allow modifications to be tracked throughout the change process;
- Code, unit, system, and quality testing are all conducted in accordance with industry standards; and,
- Aetna 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 Aetna 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 Aetna's claims processing systems. We determined that Aetna has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail room are tracked to ensure timely processing;
- Claims are monitored as they are processed through the systems 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 Aetna has not implemented adequate controls over the claims processing system.

3. Enrollment

We evaluated Aetna's procedures for managing its database of member enrollment data. Electronic enrollment data is processed weekly and paper files are processed daily. Aetna has a reconciliation process to ensure all data that was sent to the plan was received and processed.

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

4. Debarment

Aetna has adequate procedures for updating its claim processing systems with debarred provider information and routinely audits its debarment database for accuracy.

Aetna downloads the OPM OIG debarment list every month and compares the data to its provider database. Debarred providers that are a direct match to the debarment list are automatically terminated from the provider database. A manual review is conducted for all partial matches to ensure that all debarred providers are appropriately terminated.

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

5. Special Investigations and Fraud

We evaluated the Aetna policies and procedures governing special investigations and fraud. We determined that Aetna has substantial policies and procedures in place to detect, manage, and report fraud.

Nothing came to our attention to indicate that Aetna has not implemented adequate controls over its special investigations and fraud unit.

6. Application Controls Testing

We conducted a test on Aetna's claims adjudication applications to validate the systems' processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which Aetna's systems adjudicated the claims. Test claims were submitted to the [redacted] system for the Open Access plan and [redacted] for the HealthFund.

Our test results indicate that both systems have controls and system edits in place to identify the following scenarios:

- Invalid members and providers;
- Member eligibility;
- Gender;
- Timely filing; and,
- Catastrophic maximum.

The sections below document opportunities for improvement related to Aetna's claims application controls.

a. Benefit Structure Inconsistency

We submitted test claims into [redacted] for [redacted]. The claims were processed and a $15 dollar copay was applied. However, according to the Aetna Open Access 2012 benefit brochure, the copay for [redacted] should be $35. Aetna confirmed that the copay amount was loaded into [redacted] incorrectly, but only for the state of Delaware, and has since corrected the error.

We also entered two test claims for a [redacted] within the same year. Both of these claims were processed and paid. However, the Aetna Open Access 2012 benefit brochure restricts coverage of [redacted] to one time per year.

Recommendation 6

We recommend that Aetna conduct a review of [redacted] settings to ensure the application properly reflects the benefits defined in the Aetna Open Access benefit brochure.

Aetna Response:

"Going forward, when Aetna is notified of a new state mandate the HMO Product Admin team will be sent a list of all groups with plans in that particular state. The team will scan the list for the federal plans and remove them from the list.

In the unlikely instance that a plan participant would receive more than one [redacted] in a year, due to system limitations, Aetna's HMO system does not have the ability to limit to this frequency. With the planned migration off of HMO to Aetna's strategic claim platform ([redacted] there is not anticipated investment in enhancements to the legacy platform."

OIG Reply:

We believe that the recommendation should remain open until Aetna provides OPM's HIO with evidence that the [redacted] has been updated to correct the deficiency or that the plan has successfully migrated all FEHBP claims processing activity to [redacted].

b. Provider/Procedure Inconsistency

We entered test claims for [redacted] performing a [redacted] into [redacted] and [redacted]. Despite the fact that a [redacted] r is not licensed to [redacted], the claim was processed without encountering any edits.

We also entered test claims for a [redacted] performing [redacted]. Again, the claims were inappropriately processed by the [redacted] and [redacted] systems without encountering any edits.

Aetna stated that its systems are not configured to compare the [redacted] to the [redacted] to identify inconsistencies. Aetna assumes that if a licensed

provider is billing a service, [redacted] and that they are indeed actively licensed in that state. Aetna's Special Investigations Unit is responsible for detecting instances of providers who are billing [redacted]. While we acknowledge that a medical doctor legally can perform any medical procedure [redacted]), the providers in our test claims were not medical doctors.

Although Aetna's SIU is tasked with detecting instances of providers billing outside the scope of their license, this process can be improved by utilizing preventive controls within the claims processing system.

Recommendation 7

We recommend that Aetna make the appropriate system modifications to prevent medically inconsistent claims from processing.

Aetna Response:

"Aetna has carefully reviewed this issue and based on a significantly extensive activity to implement such a solution for what would [be] considered a highly unlikely event, Aetna will continue to place reliance on the downstream SIU process."

OIG Reply:

We disagree with Aetna's position and continue to recommend that Aetna modify its claims processing system to prevent medically inconsistent claims from processing. We believe that preventive medical editing controls are much more efficient and effective than reactive controls, such as relying on the SIU to recoup inappropriately billed claims.

c. Procedure Code Billing Guidelines Not Enforced

We entered two separate test claims for [redacted] with multiple service dates within a span of 30 days. All of these services were paid without encountering edits in [redacted] However, according to the American Medical Association, this procedure code is only allowed to be billed once every 30 days. [redacted] was able to recognize the procedure code inconsistency and appropriately denied all but one claim line that occurred within the 30 day time span.

Recommendation 8

We recommend that Aetna make the appropriate system modification to enforce proper procedure code billing guidelines.

Aetna Response:

"A system enhancement was implemented November 10, 2012 which is now denying services for this scenario. Evidence has been provided to the OIG to demonstrate closure."

OIG Reply:

The evidence provided by Aetna in response to the draft audit report indicates that the Plan has made the appropriate system modification to enforce proper procedure code billing guidelines; no further action is required.

d. Near Duplicate

We submitted two separate test claims into [redacted] with an identical patient, procedure code, diagnosis code, date of service and billed amounts; the only difference between the two claims was the provider. These claims processed without encountering any edits and paid both providers the same amount.

Due to the similarity of these claims, we expected the second claim to be deferred by a suspected duplicate edit so that a claims processor could determine if the claim was submitted correctly.

Recommendation 9

We recommend that Aetna implement controls to prevent near duplicate claims from processing.

Aetna Response:

- ***"A recommendation for revision to our duplicate editing logic will be presented internally to our policy area for review.***
- ***The recommendation will be presented to the policy council at their March meeting. Target date: 3/30/13***
- ***Any additional management action plans will be reviewed with the OIG based upon the review committees decision."***

OIG Reply:

As part of the audit resolution process, we recommend that Aetna provide OPM's HIO with evidence that the claims processing system has been modified to prevent near duplicate claims from processing.

G. Health Insurance Portability and Accountability Act

We reviewed Aetna's efforts to maintain compliance with the security and privacy standards of HIPAA.

Aetna has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. Aetna has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. Aetna reviews its HIPAA privacy and security policies annually and updates when necessary. Aetna has designated a Privacy Official who has the responsibility of ensuring compliance with HIPAA Privacy and Security policies. Each year, all employees must complete Aetna's "Business

Conduct and Integrity" training course. This training encompasses HIPAA regulations as well as general compliance.

Nothing came to our attention that caused us to believe that Aetna is not in compliance with the various requirements of HIPAA regulations.

III. Major Contributors to This Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted], Auditor-In-Charge
- [redacted], Lead IT Auditor
- [redacted], IT Auditor

Appendix

Aetna Inc.
151 Farmington Avenue
Hartford, CT 06156

[redacted]
Senior Program Manager
Aetna Information Systems
[redacted]

December 19, 2012

[redacted]
Auditor-in-Charge
Information Systems Audits Group
U.S. Office of Inspector General
1900 E Street, NW - Room 6400
Washington, D.C. 20415-1100

RE: Aetna's response to Draft Report No.1 C-22-00-12-065

Dear [redacted]:

Aetna submits the following response to the above-referenced Draft Audit Report issued by the Office of Personnel Management (OPM) Office of the Inspector General (OIG) under the Federal Employees Health Benefits Program (FEHBP). The audit covered the general and application controls over the automated claims processing systems and other computer-based systems at Aetna.

Enclosed you will find two copies of the Draft Report. The first attachment is labeled "Aetna's Comments to the Draft Report" and the second attachment is labeled "Proposed Redactions". Aetna has responded to all of OIG's recommendations and has included a proposed timetable for completion in the first attachment. The second attachment includes Aetna's response to the Draft Report with proposed redactions. Aetna respectfully requests OIG to implement the proposed redactions prior to the Final Report's posting on the OIG website under the Freedom of Information Act.

If you have any questions or concerns about our response, please feel to contact me at [redacted]

Sincerely,

[redacted]

CC: [redacted], Senior Vice President, Aetna Federal Plans
[redacted], Chief, Information Systems Audits Group
[redacted] Underwriting Head of Aetna Federal Plans

Recommendation 1

Aetna will implement a methodology that includes:

- Establish configuration baselines
- Schedule scans to determine deviation from baseline
- Establish a risk based approach for remediation of configuration deviations

Closure ETA: Management has presented an issue closure plan by 01/31/2013. [redacted]
1[redacted]

Recommendation 2

Aetna currently utilizes a risk based approach in support of completing vulnerability assessments by focusing its scanning resources to high risk environments. As a result, these environments are scanned with significant rigor by both Aetna and externally contracted partners. Currently, Aetna's internal trusted network is subjected to annual and ad hoc assessments that scan a sample of Aetna's [redacted] and provide results with remediation advice to the system owners responsible for remediation.
To evolve Aetna's strategic vulnerability management program in 2012, the investment of deploying a scanning technology framework across the enterprise was achieved. Aetna's strategic vision of its vulnerability management program further evolved in 2012 due to the integration effort of the scanning infrastructure into the IT GRC (Governance, Risk and Compliance) tool. Integrating vulnerability scan results into the IT GRC tool will provide increased risk management oversight for remediation and prioritization. This new vulnerability management program will establish a strategic foundation for findings management and remediation workflow by providing data to assess and deploy timely patches across the enterprise... This accomplishment will allow for the management of more frequent scanning and drive timely implementation of system patches.
Aetna will implement a methodology that includes:

- Aetna has continued to expand its vulnerability management program to other environments with the solution in place as of 1/31/201[3].
- To complete the migration of its strategic vulnerability management program, Aetna is scheduled to include all [redacted] within the Internal Trusted network by [redacted]

Recommendation 3

Aetna will continue to evolve its enterprise vulnerability management program, enabling more stringent oversight and communication with system owners on vulnerability findings and remediation expectations.

Aetna will implement a methodology that includes:

- Review of current [redacted] patching process to identify gaps
- Refinement of [redacted] patching process
- Post-implementation scan to ensure successful completion of upgrades

Closure ETA: [redacted]

Recommendation 4

Aetna will implement a methodology that includes:

- Review of current [redacted] software patching process to identify gaps
- Refinement of [redacted] software patching process
- Schedule of scans
- Establish a risk based approach for remediation of non-current and unsupported software

Closure ETA: Management has submitted an issue closure plan by 01/31/2013. Closure target date was presented as part of the closure plan.

Recommendation 5

Aetna will implement a methodology that includes:

- Schedule of scans to identify unnecessary software installations
- Establish a risk based approach for removal of unnecessary software.

Closure ETA: Management has presented an issue closure plan by 01/31/2013. Closure target date was presented as part of the closure plan.

Recommendation 6

Going forward, when Aetna is notified of a new state mandate the HMO Product Admin team will be sent a list of all groups with plans in that particular state. The team will scan the list for the federal plans and remove them from the list.

In the unlikely instance that a plan participant would receive more than one routine mammogram in a year, due to system limitations, Aetna's HMO system does not have the ability to limit to this frequency. With the planned migration off of HMO to Aetna's [redacted] there is not anticipated investment in enhancements to the legacy platform.

Recommendation 7

Aetna has carefully reviewed this issue and based on a significantly extensive activity to implement such a solution for what would is considered a highly unlikely event, Aetna will continue to place reliance on the downstream SIU process.

Recommendation 8

A system enhancement was implemented November 10, 2012 which is now denying services for this scenario. Evidence has been provided to the OIG to demonstrate closure.

Recommendation 9

- A recommendation for revision to our duplicate editing logic will be presented internally to our policy area for review.
- The recommendation will be presented to the policy council at their March meeting. Target date: 3/30/13
- Any additional management action plans will be reviewed with the OIG based upon the review committees decision.