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 HAWAII MEDICAL SERVICE ASSOCIATION

Report No. 1D-97-00-12-012

Date: October 17, 2012

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 1058 & 1039
HAWAII MEDICAL SERVICE ASSOCIATION
PLAN CODES 871 / 872 / 104 / 105 / 111 / 112
HONOLULU, HAWAII

Report No. 1D-97-00-12-012

Date: 10/17/12

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 1058 & 1039
HAWAII MEDICAL SERVICE ASSOCIATION
PLAN CODES 871 / 872 / 104 / 105 / 111 / 112
HONOLULU, HAWAII

Report No. 1D-97-00-12-012

Date: 10/17/12

This final report discusses the results of our audit of general and application controls over the information systems at Hawaii Medical Service Association (HMSA). HMSA has two separate plans that service federal employees, an experience rated Health Maintenance Organization plan referred to as FED87 and a nationwide fee-for-service plan sponsored by the BlueCross and BlueShield Federal Employee Program (FEP).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for HMSA, 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

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

Access Controls

HMSA has implemented numerous controls to add and remove physical access to its data center, as well as logical controls to encrypt sensitive information. However, we did note several opportunities for improvement related to HMSA's physical and logical access controls such as

authentication controls over physical access to the data centers and the process for removing logical access for terminated employees. HMSA has since remediated these weaknesses.

Configuration Management

HMSA has developed formal policies and procedures providing 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 HMSA's configuration management program related to application patching. HMSA has since remediated the identified weaknesses.

Contingency Planning

We reviewed HMSA's business continuity plans and concluded that they contained most of the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis. However, HMSA's generator supporting the main facility does not have the capacity to support the data center in the event of a disaster.

Claims Adjudication

HMSA has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we recommended that HMSA implement several system modifications to ensure that its claims processing systems adjudicate FEHBP claims in a manner consistent with the OPM contract and other regulations.

Health Insurance Portability and Accountability Act (HIPAA)

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

Contents

I. Introduction

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) claims at Hawaii Medical Service Association (HMSA).

The audit was conducted pursuant to FEHBP contracts CS 1039 and CS 1058; 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 first audit of HMSA's general and application controls. We also reviewed HMSA's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

The business processes related to the scope of this audit are primarily located at HMSA's Honolulu, Hawaii facility. HMSA has two data centers supporting FEHBP processes on the island of Oahu. Employees responsible for processing FEHBP claims are predominantly located in Honolulu, Hawaii.

All HMSA personnel that worked with the auditors were particularly 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 HMSA's information technology (IT) environment.

These objectives were accomplished by reviewing the following areas:

- Security management;
- Access controls;
- Segregation of duties;
- Configuration management;
- Contingency planning;
- Application controls specific to HMSA'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 HMSA'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 HMSA'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.

HMSA has two separate plans that service federal employees, an experience rated Health Maintenance Organization plan referred to as FED87 and a nationwide fee-for-service plan sponsored by the BlueCross and BlueShield Federal Employee Program (FEP).

The scope of this audit centered on the information systems used by HMSA to process medical insurance claims for FEHBP members, with a primary focus on the QCSI New Extensible Technology (QNXT) and FEP Express claims adjudication applications. The QNXT system processes claims for both the FED87 and FEP Plans, and FEP Express performs additional adjudication on FEP claims. The business processes reviewed are primarily located in HMSA's Honolulu, Hawaii facility.

The on-site portion of this audit was performed in January and February 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 HMSA as of March 20, 2012.

In conducting our audit, we relied to varying degrees on computer-generated data provided by HMSA. 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 HMSA's business structure and environment;
- Performed a risk assessment of HMSA'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 HMSA's control structure. This criteria includes, but is not limited to, the following publications:

- 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 Federal Information System Controls Audit Manual;
- 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;
- 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 HMSA's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, HMSA 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 HMSA's overall IT security controls. We evaluated HMSA's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

Nothing came to our attention to indicate that HMSA 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 HMSA's Honolulu headquarters building and its data centers in Honolulu and Kapolei, Hawaii. We also examined the logical controls protecting sensitive data on HMSA's network environment and claims processing applications. Furthermore, we conducted an automated network topology scan to verify that all known assets were included within HMSA's system inventory list.

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.

However, the following sections document several opportunities for improvement related to HMSA's physical and logical access controls.

1. Access to Data Center

HMSA's primary and back-up data centers use electronic card readers and stand-alone cipher locks to control physical access. However, we expect all FEHBP contractors to also have multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at data center entrances. In addition to implementing these minimum controls, HMSA should analyze the benefit of implementing the common physical access controls listed below that we typically see at other FEHBP carrier facilities.

- video monitoring capabilities (limited video monitoring is in place, but there are several blind spots within the computer room);
- piggybacking alarms to enter the computer room (alarm that sounds if more than one person walks past a sensor for each access card that is swiped);
- "man-trap" entrances (small space with two locking doors where the first door must close before the second opens); and,
- automated data center access logs (device that monitors and records access attempts).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to HMSA data centers and the sensitive IT resources and confidential data they contain. NIST SP 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 1

We recommend that HMSA reassess its data centers' physical access management and implement controls that will ensure proper physical security. At a minimum, HMSA should implement multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at data center entrances.

HMSA Response:

"HMSA agrees with the recommendation. Effective June 22, 2012, HMSA installed a cypher lock to be used with the existing electronic badge reader, at the Keeaumoku (main) data center. Individuals must now enter their unique code into the cypher lock and have the electronic badge reader authenticate their unique badge before entering the data center. Also effective June 22, 2012, HMSA installed an electronic badge reader to be used with the existing cypher lock at the Kapolei (second) data center. Individuals must now have the electronic badge reader authenticate their unique badge and enter their unique code into the cypher lock before entering the data center."

OIG Reply:

The evidence provided by HMSA in response to the draft audit report indicates that the Plan has implemented multi-factor authentication at data center entrances; no further action is required.

2. Auditing/Monitoring of the HHIN Web Application

HMSA's Hawaii Healthcare Information Network (HHIN) web application allows medical providers to access and review HMSA member information. HMSA's access controls over its HHIN application include:

- requiring providers to sign an Electronic Trading Partner Agreement, which establishes confidentiality and security requirements;
- requiring providers to sign the HMSA Access Request and Contract to Preserve Confidential Information; and,
- providing application training upon request.

Although the process for granting access to the HHIN application has adequate controls in place, there is no auditing or monitoring process in place to ensure that user access to the application remains appropriate. HMSA is in the process of implementing an auditing and monitoring process for HHIN, but it has not been fully implemented at this time.

Failure to routinely audit or monitor the application increases the risk an unauthorized user can gain access to confidential and personal member information. NIST SP 800-53 states that an organization should disable or remove accounts that no longer require access to the information system.

Recommendation 2

We recommend HMSA implement an audit/monitoring process for the HHIN application.

HMSA Response:

"HMSA agrees with the recommendation. HMSA implemented a formal audit/monitoring process for the HHIN application to ensure that user access to the application remains appropriate. This process has been documented and was implemented as of June 20, 2012. In addition, an initial review and deletion of terminated provider IDs was completed as of June 15, 2012."

OIG Reply:

The evidence provided by HMSA in response to the draft audit report indicates that the Plan has implemented an auditing process for the HHIN application; no further action is required.

3. Logical Access Management

We conducted a series of logical access control tests for five separate HMSA applications. For one test we compared a list of terminated employees to active user lists for each application, and discovered that several systems still had active user accounts for terminated employees. HMSA indicated that human error was the reason for the failure to remove access of those terminated employees.

Although HMSA corrected all identified errors, our findings indicate that HMSA's process to routinely audit application user accounts is not effective. HMSA is currently evaluating the access removal process to identify ways to reduce the potential for human error.

FISCAM states that "Inactive accounts and accounts for terminated individuals should be disabled or removed in a timely manner." Failure to promptly remove system and application access after termination increases the risk a terminated employee could access and corrupt sensitive and proprietary information.

Recommendation 3

We recommend HMSA improve the existing audit process by routinely comparing the termination list to the active user lists for claims processing systems and applications.

HMSA Response:

"HMSA agrees with the recommendation. Effective February 1, 2012, the existing audit process was remediated. The process now requires the Information Privacy & Protection department and Human Resources to enter upcoming terminations into a collaboration site on the intranet (Sharepoint site) to track terminations. The site will send automated alerts to the Access Management unit and will escalate to management if action has not been taken on a timely basis."

OIG Reply:

The evidence provided by HMSA in response to the draft audit report indicates that the Plan has improved the existing terminated user audit process. While the new process does not involve comparing the termination list to the active user list, the evidence indicates that the new process is an effective control; no further action is required.

C. Configuration Management

HMSA uses a third party application called QCSI New Extensible Technology (QNXT) to adjudicate claims. This system is housed on a Microsoft Windows server with Microsoft SQL Server databases. We evaluated HMSA's management of the configuration of its server environment and determined that the following controls were in place:

- policies for ensuring that operating platforms are securely configured;
- controls for securely managing changes to the operating platform and claims processing application;
- controls for monitoring privileged user activity on the operating platform; and,
- documented patch management procedures.

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

1. Application Level Patching

We conducted a vulnerability scan on 19 HMSA production servers and 2 databases using automated tools. We discovered several weaknesses related to missing or outdated critical patches on applications residing on production servers (e.g., IBM Tivoli Storage Manager, Microsoft Office, and Wireshark). HMSA has documented patch management procedures, and although it appears to adequately patch the servers' operating systems, it does not prioritize application level patching. HMSA is currently in the process of developing and implementing an Application Patch Cycle process that will address patching for both in-house developed applications and third party vendor applications by October 31, 2012.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 states "The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously."

Failure to promptly install patches increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 4

We recommend HMSA develop and implement an Application Patch Cycle process.

HMSA Response:

"HMSA agrees with the recommendation. As of June 15, 2012, the Tivoli Storage Manager, Wireshark, and Microsoft Office servers identified in the finding have been either upgraded or removed. As of June 20, 2012, HMSA formalized and implemented its Windows Server Compliance and Remediation process that encompasses all Microsoft installed products. This process includes the application of all security related patches at both the operating system and application levels."

OIG Reply:

The evidence provided by HMSA in response to the draft audit report indicates that the Plan has developed and implemented an application patch cycle process; no further action is required.

2. Unsupported System Software

HMSA is currently using system software (Windows 2000 and Microsoft IIS 5.0) that is no longer supported by its vendor. HMSA is in the process of decommissioning and retiring the servers that house the unsupported software.

FISCAM states that "All vendor supplied system software should be supported by the vendor." Additionally, "Outdated versions of system software should be removed from the production environment to preclude their use."

Failure to remove unsupported system software increases the risk of an attack that exploits the known vulnerabilities within the outdated versions of the software.

Recommendation 5

We recommend HMSA complete the decommissioning of servers that house outdated and unsupported system software.

HMSA Response:

"HMSA agrees with the recommendation. As of March 31, 2012, the Windows 2000 and Microsoft IIS 5.0 servers have been decommissioned or upgraded."

OIG Reply:

The evidence provided by HMSA in response to the draft audit report indicates that the Plan has completed decommissioning of servers that house outdated and unsupported system software; no further action is required.

D. Contingency Planning

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

- business continuity for several business units and data center operations;
- disaster recovery plan for the claims processing system;
- disaster recovery plan tests conducted in conjunction with the recovery site; 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." HMSA 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.

However, one area for improvement was noted during our review of HMSA's data center. The generator supporting the main facility does not have the capacity to support the data center in the event of a power outage. HMSA is aware of this weakness and is currently working to address this by installing a larger generator that could support data center operations.

Recommendation 6

We recommend that HMSA install a power generator that can maintain data center operations in the event of power loss.

HMSA Response:

"HMSA agrees with the recommendation. On March 29, 2012, a formal contract to expand the capacity of HMSA's existing generator and UPS was signed with IBM and funds were committed. Installation of the generator requires a zoning variance because changes to the square footage of the building slightly exceeds Code (by 0.26%). The approved application is being submitted as evidence that the project is moving forward. A decision by the planning department is not expected for 90 - 120 days. Because structural changes are required to the building, this effort is expected to complete in the first quarter of calendar year 2013."

OIG Reply:

As part of the audit resolution process, we recommend that HMSA continue to update OPM's Healthcare and Insurance Office (HIO) on its progress in installing the new generator. HMSA should also provide HIO with evidence that the new generator can fully maintain data center operations in the event of a power loss.

E. Claims Adjudication

The following sections detail our review of the applications and business processes supporting claims adjudication at HMSA.

Application Configuration Management

We evaluated the policies and procedures governing software development and change control of HMSA's claims processing applications.

HMSA has policies and procedures related to application configuration management. HMSA 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:

- HMSA 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,
- HMSA uses a separate business unit to move the code between development and production to ensure adequate segregation of duties.

Claims Processing System

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

- claims scheduled for payment are actually paid;
- claims are monitored as they are processed through the systems with real time tracking of the system's performance; and,
- paper claims that are received in the mail room are tracked to ensure timely processing (aging reports).

Enrollment

We evaluated HMSA's procedures for managing its database of member enrollment data. For FEP members, enrollment is handled centrally by the BlueCross BlueShield Association Federal Employee Program Director's Office (BSBSA), not by HMSA. For the FED87 plan, changes to member enrollment information are received via an encrypted electronic transmission. A report of enrollment changes is generated, and these updates are manually entered into the enrollment database. HMSA has an audit function for each step of the enrollment process that requires manual data manipulation.

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

Debarment

HMSA has adequate procedures for updating its claim system with debarred provider information, and the Plan routinely audits its debarment database for accuracy.

HMSA downloads the OPM OIG debarment list every month and compares it to its provider maintenance file. Any debarred providers that appear in HMSA's provider master database are flagged to prevent claims submitted by that provider from processing successfully during the claims adjudication process.

We do not have any concerns regarding HMSA's debarment policies and procedures.

Special Investigations and Fraud

HMSA has a sufficient program in place to detect and review potentially fraudulent claims.

We did determine one area for improvement regarding the reporting of fraudulent cases. HMSA currently has a process in place to report these cases to the BCBSA on a quarterly and annual basis. While we have no concerns regarding HMSA's communication with the BCBSA, HMSA is not currently reporting cases directly to the OPM OIG Office of Investigations in accordance with OPM FEHBP Program Carrier Letter No. 2007-12. The Carrier Letter provides guidance on reporting thresholds and timelines that all FEHBP carriers must follow.

Recommendation 7

We recommend that HMSA review its policies and procedures regarding the reporting of potentially fraudulent cases to OPM OIG to ensure compliance with OPM Carrier Letter 2007-12 and all subsequent Carrier Letters.

HMSA Response:

"HMSA agrees with the recommendation. On September 13, 2011, HMSA implemented policies and procedures to ensure proper reporting of potentially fraudulent cases to OPM OIG and compliance with OPM Carrier Letter 2007-12 and all subsequent Carrier Letters. HMSA has submitted cases to OPM OIG that met the OPM Carrier Letter 2007-12 criteria."

OIG Reply:

Our audit work indicated that the policies and procedures created on September 13, 2011 were not adequately implemented as of March 20, 2012. Subsequent evidence provided by HMSA indicates that the procedures are now appropriately implemented and cases are reported to OPM OIG in a manner consistent with OPM Carrier Letter 2007-12; no further action is required.

Application Controls Testing

We conducted a test on HMSA's claims adjudication applications to validate the systems' claims processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which HMSA's systems adjudicated the claims.

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

1. Overlapping Hospital Stays

The QNXT system paid duplicate room and board charges on test claims for a member with two overlapping hospital stays.

The system does not have edits in place to prevent duplicate room and board (R&B) charges for the same time period. We submitted claims for the same member for two instances of R&B at the same facility on the same day. We also submitted claims for the same member for R&B at different facilities on the same day. QNXT inappropriately processed and paid the duplicate services for both sets of claims.

This system weakness increases the risk that hospitals are being paid for duplicate room and board expenses.

At the conclusion of the fieldwork phase of our audit, HMSA provided evidence that pre-payment reports are generated that identify possible duplicate inpatient claims billed for both scenarios: overlapping stays at a single facility and different facilities. The implementation of pre-payment reports is an acceptable compensating control, but we were unable to test its effectiveness due to the timing in which this information was provided to us.

Recommendation 8

We recommend that HMSA provide evidence that it is appropriately utilizing pre-payment reports related to overlapping hospital stays over a six month time period.

HMSA Response:

"HMSA agrees with the recommendation. HMSA applies systematic duplicate editing to overlapping hospital stays billed by the same provider or facility. To supplement the systematic editing, a prepayment report was created to identify overlapping hospital stays billed by different facilities.

The process includes a review of the prepayment report to ensure that claims with overlapping service dates are not duplicate claims. If the claim contains overlapping service dates, the examiner will determine whether a transfer or re-admission to a second facility occurred and once validated, will allow the claim to pay. If the examiner is unable to validate that a transfer or re-admission to a second facility occurred, the claim will be denied as a duplicate claim.

The remediation was implemented on February 27, 2012 and OPM has received and acknowledged receipt of the evidence showing implementation of the review. OPM's request for further documentation spanning the 6 month period February 27, 2012 to August 27, 2012 is not possible due to the OPM imposed deadline for our response of June 30, 2012. As such, HMSA will be submitting the prepayment reports from date of implementation through June 22, 2012."

OIG Reply:

The evidence provided by HMSA as a response to the draft audit report indicates that the Plan has implemented and is utilizing pre-payment reports to detect overlapping hospital stays; no further action is required.

2. Medical Editing

Our claim testing exercise identified several scenarios where QNXT failed to detect the following medical editing inconsistencies:

a. Gender Inconsistency

A test claim was processed in the QNXT system for a male member receiving a [redacted] procedure. Despite the inconsistency between the gender and procedure, the claim processed through the system without encountering any edits.

b. Diagnosis/Procedure Inconsistency

A test claim was processed in QNXT with a procedure code for a [redacted] and a diagnosis of [redacted]. Despite the inconsistency between the diagnosis and procedure, the claims processed through the system without encountering any edits.

c. Provider/Procedure Inconsistency

Two test claims were processed where a provider was paid for services outside the scope of their license.

We entered a test claim for a FED87 member receiving a [redacted] procedure performed by an [redacted] This procedure would generally be performed by a [redacted]. Despite the provider/procedure inconsistency, the claim was processed by QNXT without encountering any edits.

This claim scenario was also submitted for an FEP member. Again, the claim was processed by QNXT without encountering any edits. This claim was also processed and paid by the FEP Express system that is used to process FEP claims nationwide.

We had an open audit recommendation from an audit of the CareFirst BlueCross BlueShield and the Federal Employee Program Operations Center (FEPOC) (Report No. 1A-10-85-11-029) requesting that the FEPOC implement comprehensive medical editing capabilities on FEP Express. The provider/procedure inconsistency for the HMSA member claim described above would not have been processed if the FEPOC had complied with our recommendation. We received evidence related to the recommendation in the FEPOC audit that a comprehensive plan was in place to install medical editing capabilities on FEP Express. The audit recommendation has been satisfied, but we suggest that OPM's audit resolution group continue to monitor FEPOC's progress.

d. Invalid Place of Service

Test claims were processed where the place of service was not valid for the procedure performed.

We entered test claims into QNXT with a procedure code for a [redacted] with place of service codes corresponding to a [redacted] and an [redacted]. Despite this inconsistency, QNXT did not defer or suspend these claims.

These system weaknesses increase the risk that benefits are being paid for procedures that were not actually performed.

At the conclusion of the fieldwork phase of our audit, HMSA provided evidence that post-payment reports were created to identify diagnosis and procedure inconsistencies and invalid place of service inconsistencies. Pre-payment reports were created to identify gender inconsistencies and procedure and provider inconsistencies that we determined were not in place during our testing.

However, we found that the report parameters regarding invalid place of service were only enabled to include the two situations specifically identified in our testing. The intent of our claims testing is to identify areas for improvement within the claims processing system that can be generalized and extrapolated. The overall risk that claims are being paid for services with invalid place of service codes is still present.

Recommendation 9

We recommend that HMSA conduct a full review of place of service codes to appropriately tailor the reporting function to ensure claims are not being inappropriately processed.

HMSA Response:

"HMSA partially agrees with the recommendation.

1) HMSA agrees with the recommendation as it relates to surgical services noted as exceptions during the fieldwork phase of the audit. HMSA has already provided evidence that the recommendation was implemented on March 20, 2012. The remediation consists of a review of post payment reports to identify potential cases of surgical services being performed at inappropriate service locations. All eligible cases are then reviewed by in-house physicians to confirm that the claim is invalid. Based on the response and evidence provided, HMSA believes this recommendation has been implemented.

2) HMSA disagrees with the broader recommendation to implement a full review of all possible cases of invalid place of service codes to mitigate the overall risk of overpayment. HMSA disagrees with the recommendation because we currently have two programs in place that adequately address the remainder of services performed in

customary settings such as the ambulatory surgical center, inpatient & outpatient hospital, emergency room and military treatment facilities. Below is a description of the two programs:

a) Place of Treatment Program (POTP)
This program requires certain medical services identified in the POTP be performed in a physician's office or outpatient setting. If a more acute setting is required, the physician must request precertification prior to rendering services. The lack of precertification will result in the claim being routed for review by HMSA's in-house medical consultants for determination or returned to the physician with a request for additional information.
The following attachment is being provided in relation to this response: . . .

b) Place of Service (POS) Claims Editing
HMSA currently uses a vendor package called iCES KnowledgeBase by OPTUM to systematically apply place of service editing on a procedure code level. This vendor package is interfaced with our claims adjudication system, QNXT. The iCES KnowledgeBase edits approximately 86% of CPT and HCPCS procedure codes identified through Medicare Local Coverage Determinations (LCD), Medical National Coverage Determinations (NCD), provider specialty societies and code descriptors."

OIG Reply:

We continue to recommend that HMSA conduct a thorough review of place of service codes and update the system to ensure claims are processed appropriately. As HMSA stated in its reply to the recommendation, the iCES vendor package only edits 86% of CTP and HCPCS procedure codes. We subjectively submitted two claims with invalid place of service codes without reviewing any iCES edit documentation. Both of these claims processed without encountering any edits. We are therefore not confident that the current vendor packages can adequately detect place of service inconsistencies.

Recommendation 10

We recommend that HMSA ensure the appropriate system modifications are made to prevent medically inconsistent claims from processing. Furthermore, we request that HMSA provide evidence that it is appropriately utilizing these post-payment reports related to invalid place of service over a six month time period.

HMSA Response:

"HMSA partially agrees with the recommendation.

1) HMSA disagrees with the recommendation to implement additional system modifications due to the robustness of HMSA's existing programs and system edits outlined above in our response to Recommendation 9. We believe that the combination of the PTOP program, the POS edits and the review of prepayment and post payment reports provides adequate coverage to mitigate the risk of overpayment for services

being performed at possible inappropriate service locations. Please refer to the response provided in Recommendation 9.

2) HMSA agrees with the request to provide OPM with additional evidence of prepayment and post-payment reports related to Recommendation 9. The remediation was implemented on February 27, 2012 and OPM has received and acknowledged receipt of the evidence showing implementation of the review. OPM's request for further documentation spanning the 6 month period February 27, 2012 to August 27, 2012 is not possible due to the OPM imposed deadline for our response of June 30, 2012. As such, HMSA will be submitting samples of the prepayment and post-payment reports from date of implementation through June 22, 2012."

OIG Reply:

We have reviewed the provided evidence and agree that pre-payment and post-payment reports have been implemented to detect gender inconsistencies, diagnosis to procedure inconsistencies, and provider to procedure inconsistencies. However, as stated in our reply to recommendation 9, we have not received adequate evidence that the claims adjudication system can adequately detect place of service inconsistencies. Therefore, we continue to recommend that HMSA conduct a full review of place of service codes.

3. Prior Authorization

The QNXT system paid a professional claim for [redacted] without receiving the appropriate prior authorization required by the benefit brochure.

HMSA informed us that they do not require all providers to obtain prior authorization for services. HMSA has a tiered variable intensity precertification review system for their providers and each tier represents a different requirement level for prior authorization.

This system structure increases the risk that benefits are not being paid in accordance with the benefit brochure for procedures requiring prior authorization.

Recommendation 11

We recommend that HMSA make the appropriate system modifications to ensure that claims without the appropriate prior authorizations are suspended and flagged for review.

HMSA Response:

"HMSA disagrees with the recommendation. . . .

HMSA disagrees with the recommendation to make further system modifications to the claims adjudication system since HMSA currently has two approaches to adequately administer the prior authorization (precertification) program as follows:

1) Most services are handled traditionally, where a claim will be denied without prior authorization. In these cases, the claim will stop processing and pend if an authorization is not present and an adjudicator will validate whether or not a review has been completed.

If it has, and authorization was denied, the claim will be denied. If no review was requested, a post-service review will be undertaken and the claim processed or denied based on the outcome of the medical necessity review.

2) Other services are eligible for our variable intensity precertification review program (VIR). For eligible categories of services requiring precertification, the VIR program allows us to pre-certify services efficiently and encourages provider self-monitoring, incenting better quality. Following an intensive data review of a provider's practice by our medical physicians and consultants, HMSA makes a determination whether the provider qualifies for an annual waiver for a particular service. If they qualify, our claims system allows the claim for the approved service to proceed to payment. Waivers are reviewed at least annually and may be rescinded.

Specific to claims related to [redacted] services, HMSA operates a VIR program that has three tiers. Analysis of the number of visits for conditions treated and the intensity of services furnished within each visit are used to stratify the providers into one of three tiers based on their efficiency of utilization and understanding of the member's benefits. Authorization points vary depending on the tier to which the [redacted] is assigned. For the claim that was noted as an exception during this audit, the [redacted] provider was categorized into an approved tier which allowed automatic precertification of 8 visits per benefit period. Due to the precertification provided by the VIR process, the claim was paid correctly. Thus, we believe no further modification is necessary to our claims adjudication system.

To provide further clarity within the benefit brochure, HMSA received instructions from the OPM contract office to modify the 2013 benefit brochure to explicitly state that prior authorization is required but is subject to HMSA's criteria. As of the date of this response, HMSA has acknowledged their instructions and has submitted the modifications to the OPM contract office and is awaiting confirmation."

OIG Reply:

As part of the audit resolution process, we recommend that HMSA continue to work with OPM's Contract Office to ensure that the language in the 2013 benefit brochure appropriately describes prior authorizations related to VIR program.

F. Health Insurance Portability and Accountability Act

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

HMSA has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. HMSA has also developed a series of privacy policies and procedures that address all requirements of the HIPAA privacy rule. HMSA uses HIPAA regulations as the baseline for the creation of its policies. The plan has a designated Privacy Official who is responsible for ensuring HMSA's compliance with HIPAA Privacy and Security

regulations. HMSA employees receive annual compliance training that encompasses HIPAA regulations.

We do not have any concerns regarding HMSA's 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], IT Auditor
- [redacted], IT Auditor