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 HEALTH CARE SERVICE CORPORATION

Report No. 1A-10-17-13-026

Date: January 28, 2014

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
HEALTH CARE SERVICE CORPORATION
PLAN CODES 10/11
CHICAGO, ILLINOIS

Report No. 1A-10-17-13-026

Date: January 28, 2014

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
HEALTH CARE SERVICE CORPORATION
PLAN CODES 10 /11
CHICAGO, ILLINOIS

Report No. 1A-10-17-13-026

Date: January 28, 2014

This final report discusses the results of our audit of general and application controls over the information systems at Health Care Service Corporation (HCSC or Plan).

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

Nothing came to our attention to indicate that HCSC does not have an adequate security management program.

Access Controls

HCSC has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. All weaknesses identified during the audit were remediated.

Network Security

HCSC has implemented a thorough incident response and network security program. However, we noted several opportunities for improvement related to HCSC's network security controls. Several specific servers containing Federal data are not subject to routine vulnerability scanning. The results of the vulnerability scans also indicated that these servers had outdated system patches and software. HCSC has also not implemented a process to monitor and audit the activity of privileged users on their information systems.

Configuration Management

HCSC 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, HCSC has not documented a formal baseline configuration outlining the approved settings for its mainframe installation and therefore cannot effectively audit its mainframe security settings. HCSC has also not developed a process to audit its server configuration settings to ensure compliance with the approved standard images.

Contingency Planning

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

Claims Adjudication

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

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that HCSC 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 by Health Care Service Corporation (HCSC).

The audit was conducted pursuant to FEHBP contract CS1039; 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 HCSC's general and application controls. The first audit was conducted in 2005 and all recommendations from that audit were closed prior to the start of the current audit. We also reviewed HCSC's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All HCSC 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 HCSC'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 HCSC'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 HCSC'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 HCSC'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 HCSC to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. HCSC uses a system [redacted] to process claims locally before submitting the claims through [redacted] the BlueCross BlueShield Association's (BCBSA) claims adjudication system. The business processes reviewed are primarily located in HCSC's Chicago, Illinois; Abilene, Texas; Plano, Texas; and Ft. Worth, Texas facilities.

The on-site portion of this audit was performed from April through May of 2013. 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 HCSC as of May 2013.

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

HCSC has implemented a series of formal policies and procedures that comprise its security management program. HCSC's Chief Information Security Officer is responsible for creating, reviewing, editing, and disseminating IT security policies. HCSC's Risk Assessment Service Team developed an impressive risk management methodology and assessment process with procedures to document, track, and mitigate or accept identified risks. We also reviewed HCSC's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that HCSC 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 HCSC's headquarters building, two satellite locations, and its data centers. We also examined the logical controls protecting sensitive data on HCSC'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 network access for terminated employees; and
- Procedures for recertifying employees' access to systems and applications.

However, HCSC's process to remove employees' physical access after termination could be improved. We compared a list of employees with active access to HCSC facilities to a list of employees that were terminated in the last year. We discovered over 30 terminated employees that retained access to various facilities. None of the employees that retained access following termination had access to the data center.

HCSC does not currently have a process in place to routinely audit employees' physical access to non-data center facilities. NIST SP 800-53 Revision 3 states that an organization must terminate access upon termination of employment. NIST SP 800-53 also states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a

terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

At the end of the fieldwork phase of the audit, HCSC stated that it has instituted a temporary control to detect improper removal of facility access. The control involves [redacted] HCSC is currently testing a new card access system that should be a better long-term solution to ensure that physical access is appropriately removed following employee termination. The anticipated implementation date of the new system is in calendar year 2014.

Recommendation 1

As part of the audit resolution process, we recommend that HCSC provide evidence of several iterations of the weekly audit process.

HCSC Response:

"[redacted]

OIG Reply:

The evidence provided by HCSC in response to the draft audit report indicates that the Plan has implemented a weekly audit process; no further action is required.

Recommendation 2

We recommend that HCSC implement a methodology to ensure that physical access to facilities is removed promptly following employee termination.

HCSC Response:

"Reference Plan response in recommendation #1 above."

OIG Reply:

The evidence provided by HCSC in response to the draft audit report indicates that the Plan has implemented a process to ensure that physical access to facilities is removed promptly following an employee termination; no further action is required.

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.

HCSC has implemented a thorough incident response and network security program. As noted in Section A, Security Management, HCSC has also implemented a robust risk assessment process. HCSC's risk assessment procedures include a thorough vulnerability scan and penetration test on the target information system, followed by a remediation process for any weaknesses identified.

We evaluated HCSC's network security program and also reviewed the results of automated vulnerability scans performed during this audit. We noted the following opportunities for improvement related to HCSC's network security controls.

1. Full Scope Vulnerability Scanning

We reviewed HCSC's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities.

Although HCSC routinely performs vulnerability scans, we discovered that several servers containing Federal data are not subject to routine vulnerability scanning. NIST SP 800-53 Revision 3 states that the organization should scan "for vulnerabilities in the information system and hosted applications…."

Failure to perform full scope vulnerability scanning increases the risk that HCSC's systems could be compromised and sensitive data stolen or destroyed.

Recommendation 3

We recommend that HCSC ensure that vulnerability scanning is conducted on all servers, specifically the servers housing Federal data that are not currently part of HCSC's vulnerability management program.

HCSC Response:

"The Plan stated it is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security baselines and measuring the remediation of security vulnerabilities through the application of patches. The validation capabilities are being rolled out by platform, with the initial deployment operational by [redacted]. At that time, a server list will be compiled by the

HCSC configuration management system; the servers identified will be scanned at least annually."

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's Healthcare and Insurance Office (HIO) with evidence that vulnerability scanning has been implemented for all servers.

2. Vulnerabilities Identified in Scan Results

System Patching

HCSC has documented patch management policies and procedures. However, the results of the vulnerability scans indicate that critical patches, service packs, and hot fixes are not always implemented in a timely manner.

FISCAM Critical Element CM-5 states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 section SI-2 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 important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 4

We recommend that HCSC implement procedures and controls to ensure that production servers are installed with appropriate patches, service packs, and hotfixes on a timely basis.

HCSC Response:

"The Plan states [redacted] it will develop a plan to supplement existing operational patching processes. The Plan will include a revised patch management policy, milestones for creating platform-specific standards, and a roadmap for implementing operational process enhancements."

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's HIO with evidence of the new patch management process implementation and the correlating vulnerability scan results that indicate that patching has occurred.

Noncurrent software

The results of the vulnerability scans indicated that several servers contained noncurrent software applications that were no longer supported by the vendors and 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 5

We recommend that HCSC implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

HCSC Response:

"The Plan states it is aware that some unsupported software runs on its network and agrees it would be preferable for all software to be at current versions. There will be occasions where their business and Information Technology Group (ITG) departments partner to make risk-aware decisions to not upgrade or replace software. Software that is to become unsupported is inventoried and the impacts of upgrading, replacing, or accepting risk are discussed with business owners. Decisions to not upgrade low risk software may be based on business drivers such as 'Reliant applications are to be retired' or 'the Plan will pay for extended vendor support until internal resources are available for the upgrade'.

In 2011, the Plan initiated a Technology Lifecycle Management program to address software and hardware currency. Under this program, the Plan maintains a centralized repository of technologies (Enterprise Technology Catalog) containing internal technology owner, vendor, HCSC lifecycle dates, next in line products (for products going out of support) and other metadata that describes the uses within HCSC. Regular audits of our applications are conducted to ensure support teams consider software currency. We expect the amount of unsupported software to decrease as the program matures."

OIG Reply:

The evidence provided by HCSC in response to the draft audit report indicates that the Plan has implemented a methodology to ensure that only current and supported versions of system software are installed on the production servers unless there is a business justification; no further action is required.

3. Privileged User Access Monitoring

HCSC has configured its network devices to record the activity of privileged users (i.e., system administrators). However, the event logs generated by these servers are only reviewed retroactively if a problem has been reported or detected.

NIST SP 800-53 Revision 3 requires that an organization "Reviews and analyzes information system audit records . . . for indications of inappropriate or unusual activity, and reports findings to designated organizational officials."

Failure to routinely review elevated user activity increases the risk that malicious activity could go undetected and sensitive information could be compromised.

Recommendation 6

We recommend that HCSC implement a process to routinely review elevated user (administrator) activity.

HCSC Response:

"The Plan states it maintains a near real-time security monitoring and analysis program. Security event correlation rules are in place to monitor user activity including those with elevated privileges. When correlation rules are triggered for all types of users, including those with elevated privileges, they are investigated and documented [redacted]. These completed investigations, including case closure notes, are then presented to senior leadership on a quarterly and annual basis. Senior leadership reviews the documentation and provides feedback as appropriate."

OIG Reply:

Our understanding of the controls described in HCSC's response is that they only apply to monitoring initial user login activity. The intent of this recommendation is for HCSC to implement a process to routinely review the activity of users with specialized access, not just to review the log-on activity associated with specialized users. During our audit, we observed the SEM tool and determined that the level of review that results from the correlation rules is not sufficient. Managers should be reviewing all activity performed by specialized users to ensure the elevated privileges are not being abused.

D. Configuration Management

System Software

The HCSC claims processing application, [redacted]. The platform includes many supporting applications and system interfaces. We evaluated HCSC's management of the configuration of [redacted] and determined that the following controls were in place:

- Documented corporate configuration policies and procedures;
- Approved server configuration images; and
- Thorough change management procedures for system software.

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

1. Baseline Configuration Policy

HCSC has created corporate configuration policies to establish configuration management responsibilities within IT functional areas and to ensure security requirements are met. However, HCSC has not documented a formal baseline configuration outlining the approved settings for its mainframe installation.

NIST SP 800-53 Revision 3 states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not meet performance requirements defined by the organization.

Recommendation 7

We recommend that HCSC document approved mainframe security configurations.

HCSC Response:

"The Plan states it currently configures its mainframe systems to adhere to a common, consistent set of security settings. These security configuration settings are applied to the mainframe baselines. The Plan will formally document the existing security configuration standard for mainframe systems by September 30, 2013."

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's HIO with evidence the security configuration standard for mainframe systems are formally documented.

2. Configuration Compliance Auditing

As noted above, HCSC does not maintain approved mainframe security configurations, and therefore cannot effectively audit its mainframe security settings (i.e., there are no approved settings to which to compare the actual settings.)

Although HCSC does have approved configuration images for its network servers, it does not routinely audit its servers for compliance with the approved configuration settings.

NIST SP 800-53 Revision 3 also states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures. FISCAM requires current configuration information to 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 implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers remain undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 8

We recommend that HCSC routinely audit mainframe security configurations settings to ensure they are in compliance with the approved baseline.

HCSC Response:

"The Plan is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security baselines and measuring the remediation of security vulnerabilities through the application of patches. Planned steps and timeline include:

- ***Finalize mainframe security configuration standard (in process);***
- [redacted] ***and***
- ***Build and execute configuration review process for mainframe.***

The validation capabilities are being rolled [redacted]***. A plan for the mainframe checks will be in place by*** [redacted]***."***

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's HIO with evidence that the mainframe security configuration settings are being routinely audited to comply with the baseline created as a result of Recommendation 7.

Recommendation 9

We recommend that HCSC routinely audit network server security configuration settings to ensure they are in compliance with the approved configuration images.

HCSC Response:

"The Plan states it is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security baselines and measuring the remediation of security vulnerabilities through the application of patches. The validation capabilities are being rolled out [redacted]***. Network server setting configurations are scheduled to be in place by*** [redacted]

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's HIO with evidence that the network server security configuration settings are being routinely audited to comply with the approved configuration images.

E. Contingency Planning

We reviewed the following elements of HCSC'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." HCSC 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 HCSC 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 HCSC's claims adjudication process.

1. Application Configuration Management

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

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

- HCSC 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
- HCSC 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 HCSC 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 HCSC's claims processing systems. We determined that HCSC 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 HCSC has not implemented adequate controls over the claims processing system.

3. Debarment

HCSC has adequate procedures for updating the [redacted] system with debarred provider information, but it does not routinely audit the debarment database for accuracy.

HCSC receives the OPM OIG debarment list every month and compares the monthly changes to the [redacted] debarred provider file. Any new debarred providers are added in order to flag claims submitted by that provider to notify the member of the provider's status and initiate the 15 day grace period in which the member has to find a new provider before further service will be denied by the system.

However, this process is done manually, and HCSC does not have an auditing process in place to ensure that all modifications are accurate and complete.

Failure to audit the accuracy of the debarment file increases the risk that claims are being paid to providers that are debarred.

Recommendation 10

We recommend that HCSC implement a process to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate.

HCSC Response:

"The Plan currently has technicians in the Service Delivery Operations (SDO) department pull Debarred Provider reports. The Debarred Provider reports are sent to responsible resources in the Federal Employee Program (FEP) Operations, Corporate Compliance, Government Programs Marketing, and Government Contracts Processing departments for review. Once each area performs their review of the report, a notification e-mail is sent to the responsible SDO Technicians and FEP Operations Management.

On a quarterly basis, FEP Operations Management will pull a sample from the original reports to confirm the accuracy and timeliness of the updates. Partial quarterly reviews were performed in April 2013 and June 2013. The first full quarter review will be performed in 4th Quarter 2013."

OIG Reply:

As part of the audit resolution process, we recommend that HCSC provide OPM's HIO with evidence of the full review process at the end of the 4th quarter, 2013, as well as evidence of several subsequent full quarterly reviews.

4. Application Controls Testing

We conducted a test on HCSC's claims adjudication application, [redacted] to validate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which HCSC's systems adjudicated the claims.

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

- Invalid members and providers;
- Member eligibility;
- Gender inconsistence;
- Overlapping facility claims;
- Timely filing; and
- Catastrophic maximum.

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

a. Place of Service/Procedure Inconsistency

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

We entered test claims into [redacted] with a [redacted] Despite this inconsistency, neither [redacted] deferred or suspended 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, BCBSA provided evidence that an edit exists regarding types of bill and procedure codes that are not compatible to place of service codes. [redacted] 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.

This risk was acknowledged by the BCBSA, and we were informed that they "will be initiating a project at the Operations Center to review the validity of the acceptable services on this Table."

Recommendation 11

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

HCSC Response:

"FEP currently has an edit in [redacted] that would defer claims if the criteria for place of service (POS) is not appropriate for the procedure performed. The OIG Audit [redacted] Based upon the exception noted, the FEP Operations Center and the FEPDO will conduct a review of the procedures and POS to ensure that this edit is functioning as designed and that the Place of Services are correctly identified on the allowable claims table. At this time, we do not have an expected completion date for this project."

OIG Reply:

As part of the audit resolution process, we recommend that the BCBSA provide OPM's HIO with evidence to ensure that a full review of place of service codes was conducted and that system modifications have been made to ensure claims are not being inappropriately processed.

b. Non-Par Pricing

A non-participating (non-par) provider was paid an amount significantly greater than the amount allowed by the Medicare fee schedule.

Non-par professional claims are priced by [redacted] We submitted a test claim directly into [redacted] for a Medicare subscriber visiting a non-par provider. This claim contained a procedure code for an office visit, a diagnosis code for [redacted] and submitted charges of $6,000. Although the Medicare fee schedule allows $38.50 for an office visit, the system paid the provider the full $6,000 of submitted charges.

According to the BlueCross BlueShield benefit brochure, the non-participating provider allowance (NPA) is calculated as the greater of the Medicare fee schedule or the Plan's usual, customary, and reasonable pricing allowance (PPA). In this test case, the processor entered a PPA equal to the submitted charges of $6,000.

During a prior audit in 2008, we discovered this exact problem in the [redacted] system. In response to our recommendation to modify the system, we were told that the BCBSA was "conducting a study to determine the specifications required to implement an edit that would defer any non-par priced claim that exceeds 40% of the Medicare Fee Schedule. The results of the study are expected during the fourth quarter 2008 with implementation of the recommendation in 2009." We submitted these claims as a follow-up test of the functionality of the controls purported to be in place by 2009. We expected the system to suspend the claim after detecting the large variance between the PPA and the Medicare fee schedule.

This system weakness increases the risk that non-par providers are being significantly overpaid when they inadvertently or fraudulently submit charges well in excess of the Medicare fee schedule amount.

Recommendation 12

We recommend that BCBSA implement the appropriate system modifications to ensure that non-par provider claims are suspended for review when there is a large variance between the NPA and the Medicare fee schedule.

HCSC Response:

"In order to comply with the above OIG recommendation, a request has been submitted to our system-intake committee to conduct an analysis of the required changes needed to be implemented into [redacted] The completion of this analysis is not expected until the [redacted] due to the year-end benefit changes."

OIG Reply:

As part of the audit resolution process, we recommend that the BCBSA provide OPM's HIO with evidence that system modifications have been made to ensure that non-par provider claims are suspended for review when there is a large variance between the NPA and the Medicare fee schedule.

G. Health Insurance Portability and Accountability Act

The OIG reviewed HCSC's efforts to maintain compliance with the security and privacy standards of HIPAA.

HCSC has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. HCSC has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. HCSC reviews its HIPAA privacy and security policies annually and updates when necessary. HCSC has designated a Privacy Official who has the responsibility of ensuring compliance with HIPAA Privacy and Security policies. Each year, all employees must complete HCSC's computer based training course. This training encompasses HIPAA privacy and security regulations as well as general IT compliance.

Nothing came to our attention that caused us to believe that HCSC 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] Deputy Assistant Inspector General for Audits
- [redacted] Chief, Information Systems Audit Group
- [redacted], Lead IT Auditor-In-Charge
- [redacted], IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

Appendix

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

[redacted]

September 10, 2013

[redacted] Senior Team Lead
Information Systems Audits Group
Insurance Service Programs
Office of Personnel Management
1900 E Street, N.W., Room 6400
Washington, D.C. 20415

Reference: OPM DRAFT EDP AUDIT REPORT
HCSC BlueCross BlueShield Plans
Audit Report Number 1A-10-17-13-026
Report Dated July 3, 2013 and Received July 3, 2013

Dear [redacted]

This report is in response to the above-referenced U.S. Office of Personnel Management (OPM) Draft Audit Report covering the Federal Employees Health Benefits Program (FEHBP) Audit of Information Systems General and Application Controls for the Plan's interface with the FEP claims processing system, access, and security controls. Our comments regarding the recommendations in this report are as follows:

A. Security Management

No recommendations made in this area.

B. Access Controls

1. Privileged User Monitoring

Recommendation 1

The OIG Auditors recommend that HCSC provide evidence of several iterations of the weekly audit process.

Response to Recommendation 1

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 2

The OIG Auditors recommend that HCSC implement a methodology to ensure that physical access to facilities is removed promptly following employee termination.

Response to Recommendation 2

Reference Plan response in recommendation #1 above.

C. Network Security

1. Full Scope Vulnerability Scanning

Recommendation 3

The OIG Auditors recommend that HCSC ensure that vulnerability scanning is conducted on all servers, specifically the servers housing Federal data that are not currently part of HCSC's vulnerability management program.

Response to Recommendation 3

The Plan stated it is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security baselines and measuring the remediation of security vulnerabilities through the application of patches. The validation capabilities are being rolled out by platform, with the initial deployment operational by [redacted]. At that time, a server list will be compiled by the HCSC configuration management system; the servers identified will be scanned at least annually.

2. Vulnerabilities Identified in Scan Results

Recommendation 4

The OIG Auditors recommend that HCSC implement proper procedures and controls to ensure that production servers are installed with appropriate patches, service packs, and hot-fixes on a timely basis.

Response to Recommendation 4

The Plan states by [redacted], it will develop a plan to supplement existing operational patching processes. The Plan will include a revised patch management policy, milestones for creating platform-specific standards, and a roadmap for implementing operational process enhancements.

Recommendation 5

The OIG Auditors recommend that HCSC implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

Response to Recommendation 5

The Plan states it is aware that some unsupported software runs on its network and agrees it would be preferable for all software to be at current versions. There will be occasions where their business and Information Technology Group (ITG) departments partner to make risk-aware decisions to not upgrade or replace software. Software that is to become unsupported is inventoried and the impacts of upgrading, replacing, or accepting risk are discussed with business owners. Decisions to not upgrade low risk software may be based on business drivers such as “Reliant applications are to be retired “or “ the Plan will pay for extended vendor support until internal resources are available for the upgrade”.

In 2011, the Plan initiated a Technology Lifecycle Management program to address software and hardware currency. Under this program, the Plan maintains a centralized repository of technologies (Enterprise Technology Catalog) containing internal technology owner, vendor, HCSC lifecycle dates, next in line products (for products going out of support) and other metadata that describes the uses within HCSC. Regular audits of our applications are conducted to ensure support teams consider software currency. We expect the amount of unsupported software to decrease as the program matures.

3. Privileged User Access Monitoring

Recommendation 6

The OIG Auditors recommend that HCSC implement a process to routinely review elevated user (administrator) activity.

Response to Recommendation 6

The Plan states it maintains a near real-time security monitoring and analysis program. Security event correlation rules are in place to monitor user activity including those with elevated privileges. When correlation rules are triggered for all types of users, including those with elevated privileges, they are investigated and documented within our [redacted]. These completed investigations, including case closure notes, are then presented to senior leadership on a quarterly and annual basis. Senior leadership reviews the documentation and provides feedback as appropriate.

D. Configuration Management

1. Baseline Configuration Policy

Recommendation 7

The OIG Auditors recommend that HCSC document approved mainframe security configurations.

Response to Recommendation 7

The Plan states it currently configures its mainframe systems to adhere to a common, consistent set of security settings. These security configuration settings are applied to the mainframe baselines. The Plan will formally document the existing security configuration standard for mainframe systems by [redacted]. See Attachment 4.

1. Configuration Compliance Auditing

Recommendation 8

The OIG Auditors recommend that HCSC routinely audit mainframe security configurations settings to ensure they are in compliance with the approved baseline.

Response to Recommendation 8

The Plan is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security

baselines and measuring the remediation of security vulnerabilities through the application of patches. Planned steps and timeline include:

- Finalize mainframe security configuration standard (in process);
- [redacted]; and
- Build and execute configuration review process for mainframe.

The validation capabilities are being rolled out [redacted] A plan for the mainframe checks will be in place by [redacted].

Recommendation 9

The OIG Auditors recommend that HCSC routinely audit network server security configurations settings to ensure they are in compliance with the approved configuration images.

Response to Recommendation 9

The Plan states it is currently deploying the capabilities to validate security settings of systems to ensure their security posture is regularly validated and reported. The Security Validation capabilities will focus on measuring adherence to approved security baselines and measuring the remediation of security vulnerabilities through the application of patches. The validation capabilities are being rolled out [redacted]. Network server setting configurations are scheduled to be in place by [redacted].

1. Contingency Planning

No recommendations made in this area.

1. Claims Adjudication

1. Debarment

Recommendation 10

The OIG Auditors recommend that HCSC implement a process to routinely audit the provider file to ensure that all debarment related modifications are complete and accurate.

Response to Recommendation 10

The Plans currently has technicians in the Service Delivery Operations (SDO) department pull Debarred Provider reports. The Debarred Provider reports are sent to responsible resources in the Federal Employee Program (FEP) Operations, Corporate Compliance, Government Programs Marketing, and Government Contracts Processing departments for review. Once each area performs their review of the

report, a notification e-mail is sent to the responsible SDO Technicians and FEP Operations Management.

On a quarterly basis, FEP Operations Management will pull a sample from the original reports to confirm the accuracy and timeliness of the updates. Partial quarterly reviews were performed in April 2013 and June 2013. The first full quarter review will be performed in 4th Quarter 2013. See Attachments 5a – 5d for April 2013 Validations and June 2013 Validations.

2. Place of Service/Procedure Inconsistency

Recommendation 11

The OIG Auditors recommend that BCBSA conduct a full review of place of service codes to appropriately tailor the edit to ensure claims are not being inappropriately processed.

Response to Recommendation 11

FEP currently has an edit in [redacted] that would defer claims if the criteria for place of service (POS) is not appropriate for the procedure performed. The OIG Audit submitted a claim [redacted] Based upon the exception noted, the FEP Operations Center and the FEPDO will conduct a review of the procedures and POS to ensure that this edit is functioning as designed and that the Place of Services are correctly identified on the allowable claims table. At this time, we do not have an expected completion date for this project.

3. Non-Par Pricing

Recommendation 12

The OIG Auditors recommend that BCBSA implement the appropriate system modifications to ensure that non-par provider claims are suspended for review when there is a large variance between the Non Par Allowance (NPA) and the Medicare fee schedule.

Response to Recommendation 12

In order to comply with the above OIG recommendation, a request has been submitted to our system-intake committee to conduct an analysis of the required changes needed to be implemented into [redacted] The completion of this analysis is not expected until the [redacted] due to the year-end benefit changes.

G. Health Insurance Portability and Accountability Act

No recommendations made in this area.

We appreciate the opportunity to provide our response to this Draft Audit Report and request that our comments be included in their entirety as an amendment to the Final Audit Report.

Sincerely,

[redacted], Managing Director
Program Assurance

Attachments

cc: [redacted], OPM
[redacted], OPM
[redacted] HCSC
[redacted], HCSC
[redacted], FEPDO
[redacted], FEPDO