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

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT CAPITAL DISTRICT PHYSICIANS' HEALTH PLAN

Report Number 1C-SG-00-16-007
August 12, 2016

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Capital District Physicians' Health Plan

Report No. 1C-SG-00-16-007 **August 12, 2016**

Background
Capital District Physicians' Health Plan (CDPHP) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

Why Did We Conduct the Audit?
The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in CDPHP's information technology (IT) environment.

What Did We Audit?
The scope of this audit centered on the information systems used by CDPHP to process and store data related to medical encounters and insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?
Our audit of the IT security controls of CDPHP determined that:

- CDPHP has established an adequate security management program.
- CDPHP has implemented a variety of physical and logical access controls. However, we noted several areas of concern related to CDPHP's access controls:
  - The management of physical access badges could be improved.
  - Physical controls surrounding the data center could be improved.
  - [redacted] permissions are not audited regularly.
  - The password policy does not address a minimum password age.
  - Privileged user system access does not require [redacted]
- CDPHP has implemented an incident response and network security program. However, we noted several areas of concern related to CDPHP's network security controls:
  - CDPHP performs routine vulnerability scans. However, not all servers in the environment have been subject to scanning.
  - Our test work indicated that software patches are not always implemented in a timely manner.
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized.
- CDPHP has developed formal configuration management policies and has approved security configurations for its operating platforms. However, the Plan does not routinely audit systems for compliance with the approved configurations.
- CDPHP's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. CDPHP 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, we noted two areas of concern related to CDPHP's contingency planning controls:
  - CDPHP has an informal agreement to use an alternate work space, but has no contractual guarantee of its availability.
  - The business continuity plan has not been subject to regular testing
- CDPHP has implemented many controls in its claims adjudication processes to ensure that FEHBP claims are processed accurately. However, we noted one area where physical claims storage could be improved.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
CDPHP	**Capital District Physicians' Health Plan**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Systems Control Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
Plan	**Capital District Physicians' Health Plan**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 4
- A. Security Management 4
- B. Access Controls 4
- C. Network Security 8
- D. Configuration Management 12
- E. Contingency Planning 13
- F. Application Controls 15

IV. **MAJOR CONTRIBUTORS TO THIS REPORT** 18

APPENDIX: The Capital District Physicians' Health Plan's April 25, 2016 response to the draft audit report, issued February 25, 2016.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims by Capital District Physicians' Health Plan (CDPHP or Plan).

The audit was conducted pursuant to FEHBP contract CS 2901; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act (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.

All CDPHP 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.

This was our first audit of CDPHP's information technology (IT) general and application controls. We discussed the results of our audit with OPM and CDPHP representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

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

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to CDPHP's claims processing systems.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of CDPHP's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of CDPHP'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 CDPHP to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. The business processes reviewed are primarily located in CDPHP's Albany, New York facility.

The on-site portion of this audit was performed in October and November of 2015. 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 CDPHP as of November 2015.

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

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed CDPHP's business structure and environment;
- Performed a risk assessment of CDPHP's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures were 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 CDPHP's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- 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, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

Security management controls encompass the policies and procedures that are the foundation of an organization's overall IT security program. We examined CDPHP's ability to develop and review security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various systems-related controls. We also examined personnel policies related to hiring, training, and terminating employees.

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

We found that CDPHP has implemented a series of formal policies and procedures that comprise its IT security management program. Specifically, we noted that CDPHP:

- Regularly updates and reviews its IT policies;
- Maintains an adequate risk management methodology that includes regular risk assessments across multiple functional areas; and
- Has procedures to verify that employees are vetted and appropriately trained for their position.

Nothing came to our attention to indicate that CDPHP has not implemented adequate controls over its security management program.

B. Access Controls

Access controls are the policies, procedures, and tools used to prevent or detect unauthorized physical or logical access to sensitive resources. We examined the physical access controls at CDPHP's facilities and data center located in [redacted], New York. We also examined the logical controls protecting sensitive data in CDPHP's network environment and applications.

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

- Procedures to appropriately grant and adjust physical access to facilities and data centers;
- Procedures to appropriately grant and adjust logical access to applications and software resources;
- Robust environmental controls within the data centers; and
- Role-based access provisioning with documented non-compatible roles.

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

1) Physical Access Badges

Physical access to CDPHP facilities is controlled through an electronic badge access system. Most employees have a unique electronic badge, and the system is designed to log when each individual uses their badge to enter the facility. However, we found that CDPHP has allocated generic badges to groups of individuals such as vendors, building services, and janitorial services. As a result, CDPHP is not able to leverage the system's logging capabilities to determine which specific individuals enter and exit the facility. The use of 'group' badges also increases the risk that a group member may be granted an inappropriate level of access.

NIST SP 800-53, Revision 4, necessitates that an organization must enforce physical access authorization by verifying individual access authorizations before granting access to a facility and by maintaining physical access audit logs.

Recommendation 1

We recommend that CDPHP assign a unique electronic access badge to every employee and vendor authorized to enter its facilities unescorted.

CDPHP Response

"COMPLETE – CDPHP agrees all vendors and employees should have unique badges. A log was created and implemented on April 18th to track the [redacted] of vendors assigned temporary cards for short term work. All other vendors have unique assigned badges."

OIG Comment

Evidence was provided in response to the draft audit report that indicates that CDPHP has enhanced its procedures for uniquely tracking badge access to its facilities; no further action is required.

2) Physical Access to Data Center

CDPHP's data center is located within its primary building, and access is controlled by an electronic badge reader. However, we expect data centers of all FEHBP contractors to also have the following additional controls:

- [redacted];

- [redacted]; and
- [redacted].

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 2

We recommend that CDPHP implement [redacted] at its data center.

CDPHP Response

"CDPHP agrees and [redacted] in the data center (Target Date (05/30/16)."

OIG Comment

Evidence was provided that indicates that CDPHP has implemented [redacted] and [redacted], and has [redacted] within the data center; no further action is required.

3) Logical Access Review

CDPHP assigns system access permissions based on the user's role and job requirements. CDPHP policy requires that user access recertification occur at least [redacted] users for all systems and applications. For [redacted], CDPHP does routinely review privileged user access, but currently does not review standard user accounts to verify that the individual is still employed at CDPHP and that their level of access is still appropriate.

NIST SP 800-53, Revision 4, requires the organization to review "privileges assigned to [users] to validate the need for such privileges;" and then reassign or remove privileges to reflect organizational business needs. Failure to review logical access permissions increases the risk that an authenticated individual will have improper authorized access to sensitive data and systems.

Recommendation 3

We recommend that CDPHP implement a process to routinely audit all [redacted] accounts to verify that each employee's access remains appropriate.

CDPHP Response

"CDPHP is enhancing the [redacted] recertification process to ensure all standard account access is appropriate (Target Date 08/31/2016)."

OIG Comment

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

4) Password Age

CDPHP maintains a password policy, however, this policy does not establish a minimum password age for users changing their password on a CDPHP information system. A minimum password age determines how long users must keep a password before they can change it. Our review indicated that CDPHP's [redacted]

NIST SP 800-53, Revision 4, requires that an organization implement a minimum password age. Failure to require this could allow users to reset their password multiple times in a short period, in effect allowing them to bypass restrictions regarding the reuse old passwords, increasing the risk that the password could become compromised.

Recommendation 4

We recommend that CDPHP update its password policy to address minimum password age and accordingly reconfigure its information systems to ensure compliance with the adjusted corporate approved password policy.

CDPHP Response

"COMPLETE - CDPHP implemented the recommended password age setting in [redacted] (completed 03/18/2016)."

OIG Comment

Evidence was provided in response to the draft audit report that indicates that CDPHP has adjusted its information systems to apply an improved standard; no further action is required.

5) [redacted] Authentication

All CDPHP information systems can be accessed via [redacted]. The use of [redacted] would increase the security of all user accounts, but at a minimum should be immediately implemented for [redacted].

NIST SP 800-53, Revision 4, necessitates that [redacted] Failure to require [redacted] on privileged accounts increases the risk of unauthorized access to sensitive data and the ability to modify system controls.

Recommendation 5

We recommend that CDPHP implement [redacted] on its information systems.

CDPHP Response

"CDPHP is implementing [redacted] (Target Date 7/31/2016)."

C. Network Security

Network security includes the policies and controls in place to manage and monitor the use and security of a computer network and network-accessible resources.

During our review we noted that CDPHP has implemented the following controls:

- A documented incident response methodology;
- Both intrusion detection and prevention controls; and

- Thorough network segregation.

However, we noted several opportunities for improvement related to CDPHP's network security controls.

1) Authenticated Vulnerability Scanning

CDPHP's documented vulnerability scanning methodology requires vulnerability scans to be run against all systems on a [redacted] basis. However, we determined that CDPHP does not perform authenticated/credentialed scans for [redacted]. CDPHP plans to expand the use of credentialed scans to the entire environment in the future.

NIST SP 800-53, Revision 4, states that administrative credentials should be used for automated vulnerability scans so that the scanning tools can access all necessary information, and therefore run a more thorough vulnerability scan. Failure to perform authenticated scans increases the risk that vulnerabilities may persist undetected in the environment.

CDPHP has not historically conducted authenticated vulnerability scanning on all systems in its entire technical environment.

Recommendation 6

We recommend that CDPHP perform authenticated vulnerability scans on its entire network inventory.

CDPHP Response

"CDPHP is implementing recommended changes to support [redacted] (Target Date 07/31/2016).

In addition, [redacted] will be extended [redacted] by the end of October (Target Date 10/31/2016)."

OIG Comment

Evidence was provided that indicated that CDPHP has implemented procedures to ensure that all vulnerability scans are performed with valid credentials; no further action is required.

2) Patching Vulnerabilities Identified in Scans

As part of this audit, we independently performed our own automated vulnerability scans on a sample of CDPHP's servers. The specific vulnerabilities that we identified will not be detailed in this report, but are summarized at a high level below. Copies of the full scan reports were provided directly to CDPHP during the audit.

Our scans detected CDPHP systems that were missing [redacted] system and third party patches that were older than the grace period allowed by CDPHP's patching policy. This included several instances where specific patches were missing on a widespread basis throughout the network, and also instances of individual servers that were missing a large number of patches. CDPHP acknowledged previously detecting these missing patches in its own vulnerability scans, but did not provide a justification as to why the patches are missing. CDPHP also had no documentation indicating that it had formally acknowledged and accepted the risk of the missing patches.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, requires "the organization … Identifies, reports, and correct information system flaws . . . [and] Installs security-relevant software and firmware updates" promptly.

The vulnerabilities identified in our test work increase the risk that a malicious attack on CDPHP's technical environment would be successful.

Recommendation 7

We recommend that CDPHP perform an analysis to determine the root cause for the [redacted] system and third party patches missing on its servers. This should include analysis of both the patches missing on a widespread basis and the individual servers that were missing a large number of patches, as the root cause for each issue may be unique. Based on this analysis, CDPHP should also update its procedures and/or implement additional controls to address the problem of missing patches in its environment.

CDPHP Response

"CDPHP completed a root cause analysis and as a result is implementing changes to the patching process, procedure, and technology to mitigate this risk in the future (Target Date 06/30/2016)."

OIG Comment

Evidence was provided that indicates that CDPHP has conducted a root cause analysis and has updated its patching methodology to include validation and remediation steps that are performed after the patch process is run to ensure patches were applied as expected; no further action is required.

Recommendation 8

We recommend that CDPHP remediate the specific vulnerabilities detected in our vulnerability scans.

CDPHP Response

"CDPHP is remediating the vulnerabilities detected in the scans (Target Date 08/31/2016)."

3) Unsupported [redacted] Platforms

Our scans also confirmed the presence of [redacted] platforms that are no longer supported by the vendor. CDPHP stated that some of the systems are being phased out in the short term, but the majority of identified systems do not yet have a phase out plan.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems." Noncurrent software may be vulnerable to malicious code and exploits that will never be patched by the vendor, increasing the risk that an attacker will be able to successfully gain access or compromise a system.

Recommendation 9

We recommend that CDPHP implement a phase-out plan to decommission or upgrade all unsupported software in its environment as soon as possible.

CDPHP Response

"CDPHP is actively decommissioning [redacted] (Target Date 1/31/2017).

In addition, the unsupported software identified in the report will either be updated or removed by the end of year (Target Date 01/31/2017)."

Recommendation 10

We recommend that CDPHP implement a software lifecycle management process to ensure that it has controls in place to upgrade or decommission [redacted] platforms prior to the date that the vendor ends its support of the product.

CDPHP Response

"A policy to govern [redacted] System Lifecycle management was developed and a process was implemented to ensure CDPHP has a plan of action in place prior to an [redacted] system reaching end-of-life (completed 04/05/2016)."

OIG Comment

Evidence was provided in response to the draft audit report that indicates that CDPHP has created an [redacted] System Lifecycle Management Policy. This policy requires the creation of "an action plan to manage the replacement of [redacted] systems . . . ." As part of the audit resolution process, we recommend that CDPHP provide OPM's Healthcare and Insurance Audit Resolution Group with evidence that it has created action plans for the [redacted] systems it currently uses that are no longer supported by the vendor.

D. Configuration Management

Configuration management controls are the policies and procedures used to define and implement system security standards. We evaluated CDPHP's configuration management program as it relates to the operating platforms that support the processing of FEHBP claims, and determined that the following controls were in place:

- Established server security standards; and,
- A system software change control process.

However, we did note one opportunity for improvement related to CDPHP's configuration management controls.

1) Configuration Compliance Auditing

CDPHP has procedures in place to build systems that are compliant with its approved security standards. However, CDPHP has not established a process for routinely auditing or monitoring compliance with the standards after the initial configuration of the system. Over

time as systems are maintained and updated, there is an increasing risk that systems will become non-compliant with the approved standards.

FISCAM states that organizations should ensure that, "Current configuration information should be routinely monitored for accuracy. Monitoring should address the current 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.

CDPHP has established server configuration security standards, but does not routinely audit systems for compliance.

Recommendation 11

We recommend that CDPHP routinely audit all server and database security configuration settings to ensure they are in compliance with the approved standards.

CDPHP Response

"CDPHP implemented compliance checks for [redacted] at the end of 2015 (completed 12/31/2015). The implementation of compliance checks for database security configurations is in progress (Target Date 06/30/2016). The implementation of compliance checks for [redacted] is in progress (Target Date 01/31/2017)."

E. Contingency Planning

We reviewed elements of CDPHP's contingency planning program to determine whether controls were in place to prevent or minimize interruptions to business operations when disrupting events occur. Our review indicated that CDPHP has developed the following plans and procedures:

- Disaster recovery plan;
- Business continuity plan; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1. CDPHP 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.

The sections below document areas for improvement related to CDPHP's contingency planning program.

1) Alternate Site Agreement

CDPHP's business continuity plan depends on the use of an alternate work site at [redacted] to support its claims processing staff should their primary location become unavailable. While there is an informal agreement in place for this arrangement, there is not yet a formalized contract with the other company to guarantee the availability of the work space. CDPHP has indicated that this was a work in progress. Failure to formalize the agreement could lead to differences of opinion in terms of the service level provided for an outside organization, and this increases the risk that the alternate site will not be fully available or functional in the event of a disaster.

Recommendation 12

We recommend CDPHP formalize the location sharing agreement with the alternate site.

CDPHP Response

"COMPLETE - CDPHP has formalized arrangements with the alternate site effective 1/18/2016 (completed 3/1/2016)."

OIG Comment

Evidence was provided in response to the draft audit report that indicates that CDPHP has formalized the agreement with the alternate site; no further action is required.

2) Business Continuity Testing

CDPHP maintains a documented business continuity plan and performs regular (at least annual) testing of the corresponding call trees used to communicate emergency situations with employees. However, CDPHP does not conduct formal testing of the entire business continuity plan. Testing should be used to validate that the plan is feasible.

NIST SP 800-53, Revision 4, states that an organization should test "the contingency plan for the information system . . . to determine the effectiveness of the plan and organization readiness to execute the plan …."

Additionally, NIST SP 800-53, Revision 4, provides supplemental guidance around several methods for testing. These can include full function comprehensive tests (a single testing exercise at the alternate processing site to familiarize contingency personnel with the facility

and available resources and to evaluate the site's capabilities to support contingency operations), partial functional tests of the plan at different times (isolated relocation testing by department or group), or tabletop exercises (a verbal walk through/simulation of the business continuity plan given a hypothetical disaster).

Business continuity tests allow an organization to evaluate the effectiveness of the contingency plan with regard to the effect on the organizational operations and individuals. Failure to do so increases the risk that an organization cannot recover from a disruptive situation in a timely manner.

Recommendation 13

We recommend CDPHP routinely conduct tests of its business continuity plans to evaluate its effectiveness and feasibility.

CDPHP Response

"CDPHP has engaged an external firm to assist in conducting tabletop tests of the CDPHP Business Continuity Plans in 2016 (Target Date 12/31/2016)."

F. Application Controls

The following sections detail our review of the applications and business processes supporting CDPHP's claims adjudication process. CDPHP prices and adjudicates claims using a combination of [redacted] and [redacted] claims adjudication software. Our review included the following processes: application change control, claims lifecycle, member enrollment, and provider debarment.

1) Application Configuration Management

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

CDPHP 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:

- Policies and procedures that allow modifications to be tracked throughout the change process;

- Code, unit, system, and quality testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

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

2) **Claims Input, Processing, and Output Controls**

We evaluated the input, processing, and output controls associated with CDPHP's claims adjudication process. We have determined that the following controls are in place over CDPHP's claims adjudication system:

- Sufficient controls over the input and processing of claims;
- Documented policies and procedures for full reconciliation of claim output files; and
- Quality assurance reviews of each step in the lifecycle of a claim.

During the claims processing walkthrough we noted that claims files are not securely stored [redacted]. Failure to protect health information assets increases the probability of loss.

Recommendation 14

We recommend that CDPHP implement a process to securely store claim files that are currently stored insecurely [redacted].

CDPHP Response

"Facilities has installed card access to the storage room [redacted] that houses the claims documents (completed 3/27/2016)."

OIG Comment

Evidence was provided in response to the draft audit report that indicates that CDPHP has enhanced security for its claims storage area; no further action is required.

3) **Enrollment**

We assessed CDPHP's procedures for managing its member enrollment data. The process is mostly automated. Enrollment information is received electronically and a change report is

created to update the member database. The report is uploaded to the claims systems and errors are manually reviewed.

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

4) **Debarment**

We evaluated CDPHP's procedures for updating its claims system with debarred provider information. CDPHP downloads the OPM OIG debarment list every month and provider flags are placed in the claims processing system. If a debarred provider is listed as a member's primary care physician, member notification occurs immediately. Otherwise, any claim submitted for a debarred provider is flagged by CDPHP to adjudicate through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial of claims.

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

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor in Charge

[redacted], IT Auditor

[redacted], Senior Team Leader

[redacted], Senior Team Leader

[redacted], Group Chief

APPENDIX

500 Patroon Creek Blvd.
Albany, NY 12206-1057
www.cdphp.com

April 25, 2016
[redacted], Auditor-In-Charge
U.S. Office of Personnel Management
RE: Audit of Information Systems General and Application Controls at Capital District Physicians' Health Plan

Dear [redacted]:

This letter is in response to the findings and recommendations noted in the draft audit report issued on February 25, 2016. CDPHP has reviewed the findings and recommendations in the draft report and have the following response.

Access Controls

Recommendation 1
We recommend that CDPHP assign a unique electronic access badge to every employee and vendor authorized to enter its facilities unescorted.

CDPHP Response: COMPLETE – CDPHP agrees all vendors and employees should have unique badges. A log was created and implemented on April 18th to track the [redacted] out of vendors assigned temporary cards for short term work. All other vendors have unique assigned badges.

Recommendation 2
We recommend that CDPHP implement [redacted] at its data center.

CDPHP Response: CDPHP agrees and [redacted] in the data center (Target Date (05/30/16).

Recommendation 3
We recommend CDPHP implement a process to routinely audit all [redacted] accounts to verify that each employee's access remains appropriate.

CDPHP Response: CDPHP is enhancing the [redacted] recertification process to ensure all standard account access is appropriate (Target Date 08/31/2016).

Recommendation 4
We recommend that CDPHP update its password policy to address minimum password age and accordingly reconfigure its information systems to ensure compliance with the adjusted corporate approved password policy.

> **CDPHP Response: COMPLETE** - CDPHP implemented the recommended password age setting in [redacted] (completed 03/18/2016)

Recommendation 5
We recommend that CDPHP implement [redacted] on its information systems.

> **CDPHP Response:** CDPHP is implementing [redacted] (Target Date 7/31/2016).

Network Security

Recommendation 6
We recommend that CDPHP perform authenticated vulnerability scans on its entire network inventory.

> **CDPHP Response:** CDPHP is implementing recommended changes to support [redacted] (Target Date 07/31/2016).
> In addition, [redacted] will be extended [redacted] by the end of October (Target Date 10/31/2016).

Recommendation 7
We recommend that CDPHP perform an analysis to determine the root cause for the [redacted] system and third party patches missing on its servers. This should include analysis of both the patches missing on a widespread basis and the individual servers that were missing a large number of patches, as the root cause for each issue may be unique. Based on this analysis, CDPHP should also update its procedures and/or implement additional controls to address the problem of missing patches in its environment.

> **CDPHP Response:** CDPHP completed a root cause analysis and as a result is implementing changes to the patching process, procedure, and technology to mitigate this risk in the future (Target Date 06/30/2016).

Recommendation 8
We recommend that CDPHP remediate the specific vulnerabilities detected in our vulnerability scans.

> **CDPHP Response:** CDPHP is remediating the vulnerabilities detected in the scans (Target Date 08/31/2016).

Recommendation 9
We recommend that CDPHP implement a phase out plan to decommission or upgrade all unsupported software in its environment as soon as possible.

> **CDPHP Response:** CDPHP is actively decommissioning [redacted] servers (Target Date 1/31/2017).
> In addition, the unsupported software identified in the report will either be updated or removed by the end of year (Target Date 01/31/2017).

Recommendation 10
We recommend that CDPHP implement a software lifecycle management process to ensure that it has controls in place to upgrade or decommission [redacted] platforms prior to date that the vendor ends its support of the product.

> **CDPHP Response: COMPLETE**. A policy to govern [redacted] System Lifecycle management was developed and a process was implemented to ensure CDPHP has a plan of action in place prior to an [redacted] system reaching end-of-life (completed 04/05/2016).

Configuration Management

Recommendation 11
We recommend that CDPHP routinely audit all server and database security configuration settings to ensure they are in compliance with the approved baselines.

> **CDPHP Response:** CDPHP implemented compliance checks for [redacted] at the end of 2015 (completed 12/31/2015). The implementation of compliance checks for database security configurations is in progress (Target Date 06/30/2016). The implementation of compliance checks for [redacted] is in progress (Target Date 01/31/2017).

Contingency Planning

Recommendation 12
We recommend CDPHP formalize the location sharing agreement with the alternate site.

> **CDPHP Response: COMPLETE** - CDPHP has formalized arrangements with the alternate site effective 1/18/2016 (completed 3/1/2016).

Recommendation 13
We recommend CDPHP routinely conduct tests of its business continuity plans to evaluate its effectiveness and feasibility.

> **CDPHP Response:** CDPHP has engaged an external firm to assist in conducting tabletop tests of the CDPHP Business Continuity Plans in 2016 (Target Date 12/31/2016).

Claims Adjudication

Recommendation 14

We recommend that CDPHP implement a process to securely store claim files that are currently stored insecurely [redacted].

CDPHP Response: COMPLETE. Facilities has installed card access to the storage room [redacted] that houses the claims documents (completed 3/27/2016).

Sincerely,

CAPITAL DISTRICT PHYSICIANS' HEALTH PLAN, INC.

By: [redacted]

Name: [redacted]

[redacted]
VP Audit and Assurance, CISO, CRO
Capital District Physicians' Health Plan

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100