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

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT OPTIMA HEALTH PLAN

Report Number 1C-PG-00-17-045
May 10, 2018

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Optima Health Plan

Report No. 1C-PG-00-17-045 **May 10, 2018**

Why Did We Conduct the Audit?

Optima Health Plan (Optima) is a subsidiary of Sentara Healthcare (Sentara) and contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Optima's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Optima to process and store data related to medical encounters and insurance claims for FEHBP members. The audit also included general IT controls managed by Optima's parent company, Sentara Healthcare.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of Optima and Sentara determined:

- Sentara has an adequate risk assessment methodology in place. However, Sentara could make improvements in this area by establishing a vendor risk management process.
- Sentara could improve its logical access controls by strengthening [redacted].
- Sentara could improve its network security posture by improving network segmentation controls. In addition, restricting user privileges on endpoint devices could protect against internal threats.
- Sentara conducts vulnerability scanning of its server network. However, it does not have policies and procedures to ensure vulnerabilities are adequately remediated.
- Sentara does not have formally documented security configuration standards for its servers. In addition, Sentara is not following its policies and procedures to ensure only supported software is used.
- Sentara maintains adequate disaster recovery and business continuity plans. However, a business impact analysis of Optima's FEHBP claims process has not been performed.
- Optima does not have procedures to validate vendor activities that support the claims process.

Optima did not provide any comments in response to the draft report, other than stating they have begun the process to implement the recommendations.

ABBREVIATIONS

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

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Optima Health Plan (Optima).

The audit was conducted pursuant to FEHBP contracts CS 2952; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act, enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for Federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

Optima is a subsidiary of Sentara Healthcare (Sentara) which offers a wide range of health care products and services in addition to its FEHBP line of business. This was our first audit of Sentara and Optima's information technology (IT) general and application controls. All Sentara and Optima personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

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

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

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of Optima'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 Optima'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 Optima to process medical insurance claims and/or store the data of FEHBP members. Sentara manages many of the information technology resources and processes supporting Optima. Therefore, the IT operations of Sentara were considered to be within the scope of this audit. The business processes reviewed are primarily located in Virginia Beach, Virginia.

The onsite portion of this audit was performed in August and September of 2017. 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 Optima and Sentara as of October 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Optima. 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 Optima's business structure and environment;
- Performed a risk assessment of Optima'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 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 Optima'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;

- Control Objectives for Information and Related Technologies 5: A Business Framework for the Governance and Management of Enterprise IT;

- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;

- 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 800-44, Version 2, Guidelines on Securing Public Web Servers;

- 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 Sentara and Optima's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Sentara and Optima were not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

The security management component of this audit involved the examination of the policies and procedures that are the foundation of Optima's overall IT security program. We evaluated Optima's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

Optima's parent company, Sentara, has implemented a series of formal policies and procedures that govern the security management program for Optima. Sentara has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Sentara has also implemented adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

The following section documents an opportunity for improvement related to Optima's security management program.

1) Vendor Risk

Optima contracts with several vendors that perform business processes related to health claims processing. However, Optima has not performed risk assessments of the IT security controls implemented by these vendors to protect the sensitive data they handle.

NIST SP 800-53, Revision 4, states that "Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities)." Failure to conduct risk assessments on all vendors to identify relevant threats, vulnerabilities, impacts, and likelihoods could leave Optima unknowingly susceptible to adverse events.

Recommendation 1

We recommend that Optima establish a formal process to assess vendor risk prior to service acquisition and then periodically over the course of the relationship. This process should also be applied to all existing vendors.

Optima Response:

"Optima Health does not have any comments concerning the draft report. Optima Health has begun the process to implement the recommendations outlined in the draft report."

OIG Comment:

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

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 Optima's facilities and the Sentara datacenter. We also examined the logical access controls protecting sensitive data in Sentara's network environment and Optima's claims processing applications.

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

- Procedures for appropriately granting and removing physical access to facilities and the datacenter;
- Procedures for appropriately granting and adjusting logical access to applications and software resources; and
- Routinely reviewing user access.

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

1) Windows Server Administrator Accounts

Sentara manages the server administration function for Optima, and has implemented administrative or technical controls to protect sensitive administrative accounts. [redacted]

NIST SP 800-53, Revision 4, states that, "The organization requires that users of information system accounts, or roles, with access to … security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions." [redacted]

Recommendation 2

We recommend that Sentara implement [redacted].

2) Privileged User Authentication

[redacted]

NIST SP 800-53, Revision 4, requires "multifactor authentication for local access to privileged accounts." [redacted]

Recommendation 3

We recommend that Sentara implement [redacted]

3) Segregation of Duties

Hiring managers are responsible for designating access rights to all information systems and applications for new employees. However, Optima does not have any formal guidance that prohibits the assignment of conflicting roles (i.e., a matrix of non-compatible roles).

FISCAM states that "Entity-wide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced." Failure to provide adequate segregation of duties guidance increases the risk that users could be granted access to data and processes inappropriate for their job function.

Recommendation 4

We recommend that Optima develop policies and procedures to ensure that access to information systems is granted with proper segregation of duties.

4) Service Account Management

Our logical access testing revealed a large number of active service accounts on Sentara systems. After receiving our test results, Sentara disabled the majority of these accounts, as they were no longer needed. We were told that [redacted] However, our test results indicate that this process has not been effective, resulting in a large number of unnecessary service accounts.

NIST SP 800-53, Revision 4, requires organizations to monitor the use of information system accounts and notify account managers when accounts are no longer required. Failure to disable unneeded service accounts increases the attack surface of information systems.

Recommendation 5

We recommend that Sentara implement an auditing process to ensure that service accounts are promptly disabled when no longer needed.

5) Inactive Accounts

Sentara does not have a process or technical control to disable accounts that have been inactive for an extended period of time.

NIST SP 800-53, Revision 4, requires information systems to automatically disable inactive accounts. Failure to timely disable inactive accounts increases the risk of the accounts being subjected to attack and misused for malicious purposes.

Recommendation 6

We recommend that Sentara implement a process to disable accounts that have not been logged into for a defined period of time.

6) Physical Access Reviews

Optima conducts business operations at [redacted]. A centralized facility management group at Sentara issues electronic access ID badges to all employees. Upon termination of employment, Sentara disables ID badge access. However, Sentara does not perform audits to ensure access has been disabled or to routinely verify that employees' level of access remains appropriate.

FISCAM states that "Management should regularly review the list of persons authorized to have physical access to sensitive facilities, including contractors and other third parties." Failure to review physical access increases the risk that terminated employees have the opportunity to gain unauthorized entry to company facilities.

Recommendation 7

We recommend that Sentara implement procedures to conduct regular reviews of physical access to facilities to ensure only authorized personnel have physical access.

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. Sentara manages the technical environment that supports Optima's claims adjudication process; we therefore evaluated Sentara's controls related to network design, data protection, and systems

monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A documented incident response program.

The following sections document several opportunities for improvement related to Sentara's network security controls.

1) Firewall Configuration Review

Sentara has firewalls placed at key locations at the network perimeter and maintains documented configuration settings of the firewalls in a central repository. However, Sentara does not routinely compare the documented configuration settings against the current configuration settings implemented on its firewalls.

NIST SP 800-41, Revision 1, requires rulesets to be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization's policies. Failure to routinely audit firewall settings increases the risk that unauthorized changes to the firewall's configuration remain undetected.

Recommendation 8

We recommend that Sentara perform routine audits of its current firewall configurations against an approved firewall policy.

2) Internal Network Segmentation

Firewalls are used at ingress and egress locations on Sentara's network in order to control network traffic from external connections and vendors. [redacted]

[redacted]

NIST SP 800-41, Revision 1, advises that, "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. Important internal systems should be placed behind internal firewalls." [redacted]

Recommendation 9

We recommend that Sentara [redacted]

3) Administrator Rights

Sentara has policies that prohibit the installation or modification of software without approval. [redacted]

FISCAM states that "Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or manage emergency situations." Failure to restrict local administrator rights increases the risk of employees bypassing security policies resulting in unapproved software installation and system misconfiguration.

Recommendation 10

We recommend that Sentara limit the number of personnel who have administrator privileges on their workstations to those with a need based on their job function.

4) Removable Media

Sentara and Optima user endpoint devices are configured to enforce encryption on all data copied to removable media. [redacted]

[redacted]

NIST SP 800-53, Revision 4, requires that an organization must employ the principle of least privilege, allowing only authorized access for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

In addition, NIST SP 800-53, Revision 4, states that "Organizations may restrict the use of portable storage devices, for example, by … disabling/removing the ability to insert, read or write to such devices." [redacted] increases the risk that sensitive data could be stolen and also increases the risk of introducing malware to Sentara's network.

Recommendation 11

We recommend that Sentara restrict the use of removable media on users' workstations to those with a valid and approved business need.

5) Web Application Vulnerability Scanning

Sentara does not conduct routine web application vulnerability scanning. We were informed that web application scanning is conducted, but only when changes to the web application are made.

NIST SP 800-44, Version 2, states that "Periodic security testing of public Web servers is critical." Furthermore, NIST SP 800-44, Version 2, explains that "Vulnerability scanning assists a Web server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective." Failure to conduct routine web application vulnerability scanning increases the risk that unidentified weaknesses could be exploited.

Recommendation 12

We recommend that Sentara conduct routine credentialed web application vulnerability scanning on all of its web applications.

6) Vulnerability Remediation

Sentara conducts [redacted] credentialed vulnerability scanning on a subset of servers and workstations in its network environment. The scan results are reviewed to ensure that the scans completed successfully. However, Sentara does not have a process in place to ensure that vulnerabilities identified by the scans are remediated in a timely manner.

FISCAM states that, "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective." Additionally, NIST SP 800-53, Revision 4, requires organizations to remediate legitimate vulnerabilities identified in information systems and hosted applications. Failure to remediate vulnerabilities increases the risk that bad actors could exploit system weaknesses for malicious purposes.

Recommendation 13

We recommend that Sentara implement a process to ensure that vulnerabilities identified from vulnerability scanning are remediated in a timely manner.

D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. Sentara employs a team of technical personnel who manage system software configuration for the organization. We evaluated Sentara's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented system change control process; and
- Established patch management process.

Sentara does not maintain approved security configuration standards for its operating platforms.

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

1) Security Configuration Standards

Sentara deploys servers from pre-established system images. Servers are then further configured according to functional requirements. Sentara provided us with evidence of documented configuration standards, but the standards were in draft form and were not approved by management. Furthermore, the draft standards did not cover all operating systems that are currently in use by the organization. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements … ."

In addition, NIST SP 800-53, Revision 4, requires an organization to develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk that the system may not be configured in a secure manner.

Recommendation 14

We recommend that Sentara document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

2) Security Configuration Auditing

As noted above, Sentara does not maintain approved security configuration standards for its operating platforms, and therefore it cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, 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 configuration compliance auditing program increases the risk that servers are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 15

We recommend that Sentara implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 14 are in place.

3) System Lifecycle Management

Sentara's server inventory includes [redacted] unsupported versions of operating systems. Software vendors typically announce projected dates (known as end-of-life dates) for when they will no longer provide support or distribute security patches for their products. In order to avoid the risk associated with operating unsupported software, organizations must have a process to anticipate end-of-life dates and phase out the deployment of such software prior to this window of exposure.

Sentara stated that it is aware of the unsupported operating systems in its environment and that those systems will be retired when the business no longer needs the hosted application. However, Sentara policy states any system or application that is no longer supported shall be removed from the network by the end-of-life date.

NIST SP 800-53, Revision 4, recommends that organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer … ." NIST SP 800-53, Revision 4, also states that "Unsupported components … provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components." Failure to upgrade system software leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 16

We recommend that Sentara implement a methodology to ensure that information systems are removed or upgraded to supported software versions prior to the end of vendor support.

E. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of Sentara's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to Optima business operations when disruptive events occur:

Sentara maintains thorough disaster recovery and business continuity plans.

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems."

The following sections describe areas for improvement related to Optima's contingency planning controls.

1) Business Impact Analysis

Sentara has not conducted a formal Business Impact Analysis (BIA) of the Optima organization. At the time of the audit, Sentara provided evidence that it is in the early stages of completing a BIA, and the BIA is scheduled to be completed at the end of calendar year 2018.

NIST SP 800-34, Revision 1, states that, "The BIA is a key step in implementing … the contingency planning process … ." Three steps involved in accomplishing a BIA include determining business processes and recovery criticality, identifying resource requirements, and identifying recovery priorities for system resources. Failure to conduct a BIA increases the risk that Optima will not be able to recover critical business operations in a timely manner.

Recommendation 17

We recommend that Sentara and Optima complete a formal Business Impact Analysis for Optima business processes and information systems. We further recommend that Sentara incorporate the results into its disaster recovery plan.

2) Backup Media Encryption

As part of its IT disaster recovery strategy, Sentara stores backup tapes onsite in a virtual library and offsite at a secure vendor facility. [redacted].

NIST SP 800-53, Revision 4, states the organization should protect "the confidentiality, integrity, and availability of backup information at storage locations. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes." [redacted]

Recommendation 18

We recommend that Sentara [redacted]

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting Optima's claims adjudication process. [redacted] We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

1) Application Configuration Management

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

Sentara has implemented a thorough process for managing software changes.

Sentara 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 approval of software modifications:

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

- Unit, integration, and user acceptance 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 adequate controls have not been implemented over the application configuration management process.

2) Claims Processing System

We evaluated the business process controls associated with Optima's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that Optima has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;

- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and

- Claims scheduled for payment are actually paid.

The sections below document areas for improvement related to Optima's claims adjudication processes.

Claims Input Reconciliation

A vendor is responsible for scanning all claim files received by mail into Optima's claims processing system. Currently, Optima does not have a reconciliation process in place to verify that all scanned claims have been received for processing.

Optima does not have procedures to verify the claims processing activities performed by vendors.

FISCAM states that "The entity should have policies and procedures in place to reasonably assure that all authorized source documents and input files are complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system." Failure to validate this process could lead to incomplete processing of properly submitted claims.

Recommendation 19

We recommend that Optima establish a reconciliation process to ensure that all claims are scanned and successfully transmitted to the claims systems by the vendor.

Output Reconciliation

Explanation of Benefits letters are printed by a vendor. Optima sends an electronic file to the vendor to notify them of what needs to be printed and mailed. However, there currently is no reconciliation process in place to ensure that all Explanation of Benefits have been printed and mailed.

FISCAM states that "Formal procedures should be established for data processing to help assure that … output control totals are accurate and are being verified, and the resulting information is distributed in a timely … manner … ." Failure to provide accountability over this process could lead to incomplete communication of benefit decisions with members.

Recommendation 20

We recommend that Optima establish a process to reconcile the print request files with the output produced by the vendor.

3) Enrollment

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

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

4) Debarment

Optima has documented procedures for reviewing the provider file for debarments and suspensions. Optima is notified by OPM when an update to the debarment list is available. An automated comparison of the OPM debarment list and providers within Optima's claims processing system generates reports that will flag debarred providers. If an active provider is determined to be debarred, Optima personnel will manually update the provider file within the claims processing system. Optima adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

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

APPENDIX

OptimaHealth

4417 Corporation Lane
Virginia Beach, VA 23462

February 13, 2018

[redacted]
Information Systems Auditor
Office of the Inspector General
U.S. Office of Personnel Management
Washington, D.C. 20415

Re: Report No. 1C-PG-00-17-045

Dear [redacted]:

I am in receipt of the above-referenced draft report, dated December 13, 2017, concerning the information technology audit of Optima Health Plan conducted by the Office of the Inspector General at the U.S. Office of Personnel Management. Thank you for allowing us the opportunity to review the draft report. Optima Health does not have any comments concerning the draft report. Optima Health has begun the process to implement the recommendations outlined in the draft report.

It has been a pleasure working with you and your colleagues on this important matter.

Sincerely,

[redacted]

Director, Information Technology

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