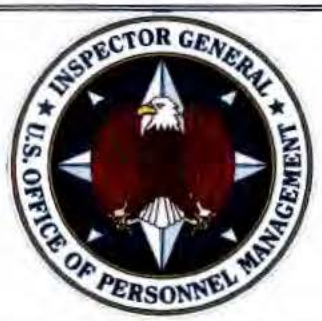

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT PREMERA BLUE CROSS

Report No. 1A-10-70-14-007

Date: November 28, 2014

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
PREMERA BLUE CROSS
PLAN CODES 10/11
MOUNTLAKE TERRACE, WASHINGTON

Report No. 1A-10-70-14-007

Date: November 28, 2014

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
PREMERA BLUE CROSS
PLAN CODES 10/11
MOUNTLAKE TERRACE, WASHINGTON

Report No. 1A-10-70-14-007

Date: November 28, 2014

This final report discusses the results of our audit of general and application controls over the information systems at Premera Blue Cross (Premera or Plan).

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

Security Management

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

Access Controls

Premera has implemented controls to grant or prevent physical access to its data center, as well as logical controls to protect sensitive information. However, Premera's data center did not contain controls we typically observe at similar facilities, such as multi-factor authentication and piggybacking prevention. Since the issuance of the draft report Premera has installed multi-

factor authentication, but has yet to implement piggybacking prevention. We also noted a weakness related to the password history configuration settings.

Network Security

Premera has implemented a thorough incident response and network security program. However, we noted several areas of concern related to Premera's network security controls:

- A patch management policy is in place, but current scans show that patches are not being implemented in a timely manner;
- A methodology is not in place to ensure that unsupported or out-of-date software is not utilized;
- Insecure server configurations were identified in a vulnerability scan.

Configuration Management

Premera has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured, updated, and changes are controlled. However, Premera has not documented formal baseline configurations that detail the approved settings for its server operating systems, and therefore cannot effectively audit its security configuration settings.

Contingency Planning

We reviewed Premera's business continuity and disaster recovery plans and concluded that they contained the key elements suggested by relevant guidance and publications. However, Premera does not perform a complete disaster recovery test for all information systems.

Claims Adjudication

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

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that Premera 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 Premera Blue Cross (Premera or Plan).

The audit was conducted pursuant to FEHBP contract CS 1039; 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.

All Premera 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 the security controls at Premera. We discussed the results of our audit with Premera representatives at an exit conference.

Objectives

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

Premera has a nationwide fee-for-service plan sponsored by the BlueCross and BlueShield Federal Employee Program (FEP).

The scope of this audit centered on the information systems used by Premera to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. Premera processes FEP claims through its local system and then through FEP Direct, the BlueCross BlueShield Association's (BCBSA) nationwide claims adjudication system. The business processes reviewed are primarily located in Premera's Mountlake Terrace, Washington facilities.

The on-site portion of this audit was performed in January and February of 2014. 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 Premera as of March 2014.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Premera. 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 Premera's business structure and environment;
- Performed a risk assessment of Premera'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 Premera'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 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Information Technology 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;
- NIST SP 800-61 Revision 2, 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 Premera's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Premera 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 an examination of the policies and procedures that are the foundation of Premera's overall IT security controls. We evaluated Premera's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Premera has implemented a series of formal policies and procedures that comprise its security management program. Premera has also developed a thorough risk management methodology. Premera conducts routine enterprise-wide risk assessments, which has allowed the Plan to document, track, and mitigate or accept identified risks in a timely manner. We also reviewed Premera's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Premera 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 Premera's facilities and data center located in Mountlake Terrace, Washington. We also examined the logical controls protecting sensitive data in Premera'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 facilities and data centers for terminated employees;
- Procedures for removing [redacted]/network access for terminated employees;
- Controls to monitor and filter email and Internet activity; and
- Procedures for recertifying employees' access to systems and applications.

However, the following section documents opportunities for improvement related to Premera's physical and logical access controls.

1. Facility and Data Center Physical Access Controls

The physical access controls in Premera's data center could be improved.

The Premera facilities we visited use electronic card readers to control access to the buildings. However, Premera's data center did not contain controls that we typically observe at similar facilities, including:

- Multi-factor authentication to enter the computer room (e.g., cipher lock or biometric device in addition to an access card); and
- Piggybacking prevention controls at the computer room entrance (e.g., alarm that sounds if more than one person walks past a sensor for each access card that is swiped or a turnstile that only allows one person to enter per card swipe).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to Premera's data center and the sensitive resources and data it contains. NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data (see control PE-3, Physical Access Control).

Recommendation 1

We recommend that Premera improve the physical access controls at its data center. At a minimum, the computer room entrance should require multi-factor authentication and have controls to prevent piggybacking.

Premera Response:

"In response to this recommendation, Premera has installed a multi-factor authentication key pad requiring staff to enter a unique pin number. . . .

Premera previously had the following controls in place:

- ***Restricted badge access to limited personnel who have management approval for Data Center access.***
- ***Visitor sign in at the main reception in building 4, as well as at the Data Center by authorized Data Center personnel with badge access.***
- ***Video camera surveillance triggered by motion detectors at the Data Center door. The camera data is monitored by security personnel."***

OIG Reply:

The evidence provided by Premera in response to the draft audit report indicates that the Plan has implemented multi-factor authentication. However, the Plan has not implemented controls to prevent piggybacking. As part of the audit resolution process, we recommend Premera provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation in regards to piggybacking prevention.

2. Password History Configuration

Premera has implemented a corporate password policy that is applicable to all information systems on the network. However, we performed automated configuration compliance scans that indicated that several systems did not limit the time between password changes.

This configuration would allow users to circumvent Premera's password history requirement by changing their password multiple times within a short time period and then reuse their initial password.

Recommendation 2

We recommend that Premera reconfigure its information systems to ensure compliance with the corporate approved password policy.

Premera Response:

"In response to this recommendation, Premera agrees to investigate and remediate as appropriate by December 31, 2014."

OIG Reply:

As part of the audit resolution process, we recommend that Premera provide OPM's HIO with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this audit report that the Plan agrees to implement.

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.

Premera has implemented a thorough incident response and network security program. We worked with Premera employees to conduct automated vulnerability scans on a sample of servers and databases. We noted several opportunities for improvement related to Premera's network security controls.

1. System Patching

Premera 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 states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 states that organizations must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly.

Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached.

Recommendation 3

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

Premera Response:

"In response to this recommendation, Premera agrees to implement procedures and controls for appropriate deployment of service packs and hotfixes by December 31, 2014.

However, Premera respectfully disagrees with the section of the recommendation related to patches as it believes deployment of critical security patches is in compliance with the documented patch management policy provided to the OPM Audit Staff in Information request 13."

OIG Reply:

The results of the vulnerability scans performed during the fieldwork phase of this audit indicated that Premera was not in compliance with its policy for deploying patches within a specific timeframe based on criticality. As part of the audit resolution process, we recommend that Premera provide OPM's HIO with evidence that it has adequately implemented this recommendation.

2. 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 4

We recommend that Premera implement a methodology to ensure that only current and supported versions of system software are installed in its network environment.

Premera Response:

"In response to this recommendation, Premera agrees to investigate noted (Audit Inquiry 04) applications in the environment to ensure compatibility and supportability and will remediate appropriately by December 31, 2014."

3. Insecure Operating System Configuration

The results of the vulnerability scans also indicated that several servers contained insecure configurations that could allow hackers or unprivileged users to insert code that would result in privilege escalation. The escalated privileges could grant the hackers unauthorized access to sensitive and proprietary information.

NIST SP 800-53 Revision 4 states that the Plan must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 5

We recommend that Premera remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Premera Response:

"In response to this recommendation, Premera agrees to investigate the noted technical weaknesses (Audit Inquiry 04), and will remediate appropriately by December 31, 2014."

D. Configuration Management

Premera's claims processing application is a commercial product from [redacted]. This application is housed [redacted]. The platform includes many supporting applications and system interfaces. We evaluated Premera's management of the configuration of the system software hosting [redacted] and determined that the following controls were in place:

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

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

1. Server and Database Baseline Configurations

Premera has created a corporate configuration policy to establish configuration management responsibilities within its IT functional areas. However, Premera has not created baseline configurations for its [redacted].

NIST SP 800-53 Revision 4 states that an organization must develop, document, and maintain a current baseline configuration of the information system. NIST SP 800-53 Revision 4 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 analyze the baseline and current configuration of the hardware, software, and firmware that comprise the information system.

Premera cannot effectively audit its server and database security settings without an approved baseline, as a baseline configuration is the benchmark for comparison.

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

Recommendation 6

We recommend that Premera document approved [redacted] baseline configurations for all versions of those platforms utilized in its network environment.

Premera Response:

"In response to this recommendation, Premera agrees to establish baseline configuration documentation for all supported [redacted] by December 31, 2014."

Recommendation 7

We recommend that Premera routinely audit all [redacted] security configuration settings to ensure they are in compliance with the approved baseline.

Premera Response:

"In response to this recommendation, Premera agrees to remediate appropriately to ensure compliance with approved and documented baselines by December 31, 2014."

E. Contingency Planning

We reviewed the following elements of Premera'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 an 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 Revision 1, Contingency Planning Guide for Federal Information Systems. Premera 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, Premera's contingency planning program could be improved. Premera does not perform a complete disaster recovery test for all information systems. The Plan conducts an annual business impact analysis and assigns a criticality tier from one to four for all applications (one being the most critical). However, only applications in tiers one and two are subject to annual disaster recovery testing; tiers three and four are not subject to routine testing.

FISCAM states that "Testing contingency plans is essential to determining whether they will function as intended in an emergency situation. . . . The most useful scenarios involve simulating a disaster situation to test overall service continuity."

Failure to perform annual disaster recovery tests on all applications decreases the likelihood that Premera will be able to completely restore operations in the event of a disaster.

Premera also does not have a contract in place to guarantee generator fuel delivery in the event of a prolonged power outage at its primary data center. The Plan has a back-up generator and enough fuel on-site to sustain data center operations for approximately three days. Any outage lasting longer than three days would require additional fuel from an outside source. We were informed that Premera has "preferred" customer status with its fuel vendor; however, this status does not guarantee delivery priority over other companies that may also be "preferred" customers.

NIST SP 800-53 Revision 4 states that an organization should provide "a long-term alternate power supply for the information system that is . . . Capable of maintaining minimally . . . required operational capability . . . in the event of an extended loss of the primary power source."

Failure to ensure a long-term power capability increases the risk of data loss and inhibits the plans ability to meet contractually obligated minimum service levels.

Recommendation 8

We recommend that Premera implement a methodology to ensure that all applications are subject to routine disaster recovery testing.

Premera Response:

"Premera respectfully disagrees with this recommendation as it believes that the recommendation is focused on Premera's low impact systems (i.e., Tier 3 and 4 systems).

The strategy and solution for the recovery of Tier 3 and 4 applications and services, include regularly scheduled data replication for availability at the recovery facility with build following the declaration of a major event or disaster. In addition, on an annual basis, the solution, restoration and recovery procedures of selected Tier 3 and 4 applications and services will be exercised via stand-alone tests to validate recoverability within their defined RTO (recovery time objectives). Tabletop reviews will be performed following the development or revisions of recovery documents.

Premera believes we meet the NIST SP 800-34 Section 3.5.3 guidance which states 'for low impact systems, a tabletop exercise at an organization-defined frequency is sufficient.'

Please see information request 2 section 7.2 (IT Disaster Recovery Plan) provided to the OPM Audit staff."

OIG Reply:

We have reviewed documentation provided, and agree that it outlines procedures on how to perform disaster recovery testing for low impact systems. However, this documentation is not

sufficient evidence to indicate routine disaster recovery testing of these systems has actually occurred.

As part of the audit resolution process, we recommend that Premera provide OPM's HIO with evidence of routine disaster recovery testing for low impact systems.

Recommendation 9

We recommend that Premera reevaluate its fuel delivery situation and determine if a contract with a fuel vendor would improve its disaster recovery program.

Premera Response:

"In response to this recommendation, Premera has obtained a memorandum from our fuel vendor acknowledging that Premera has priority delivery as a Preferred Customer."

OIG Reply:

The evidence provided by Premera in response to the draft audit report indicates that the Plan is recognized as a priority along with hospitals and other healthcare facilities in the event of an emergency; no further action is required.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting Premera's claims adjudication process. Premera processes all FEP claims through its local system and then through the BCBSA's FEP Direct nationwide claims adjudication system.

1. Application Configuration Management

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

Premera 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:

- Premera 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
- Premera 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 Premera 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 Premera's claims processing system. We have determined the following controls are in place over Premera's claims adjudication system:

- Routine audits are conducted on Premera's front-end scanning vendor for incoming paper claims;
- Claims are monitored as they are processed through the systems with real time tracking of the system's performance; and
- Claims output files are fully reconciled.

Nothing came to our attention to indicate that Premera has not implemented adequate controls over the claims processing system.

3. Debarment

Premera has adequate procedures for updating its claims system with debarred provider information. Premera receives the OPM OIG debarment list every month and makes the appropriate updates to the FEP Direct claims processing system. Any claim submitted for a debarred provider is flagged by Premera to adjudicate through the OPM OIG debarment process to include initial notification, a 15 day grace period, and then denial.

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

4. Application Controls Testing

We conducted a test on Premera's claims adjudication application to validate the system's claims processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which the [redacted] and FEP Direct systems processed and adjudicated the claims. All claims are pre-priced in [redacted] and adjudicated in FEP Direct.

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

- Member eligibility;
- Coordination of benefits;
- Bundling charges;
- Overlapping hospital stays;
- Timely filing; and
- Chiropractic benefits.

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

Medical Editing

Our claims testing exercise identified several scenarios where Premera's claims system failed to detect medical inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- Diagnosis / Procedure – claims were submitted for [redacted] procedures where the diagnose codes corresponded to a [redacted];
- Provider / Procedure – claims were submitted for a [redacted] performing [redacted] and a [redacted] performing [redacted], and a [redacted];
- Place of Service / Procedure – a claim was submitted for a [redacted] performed in a [redacted];
- [redacted] / Procedure Inconsistency – a claim was submitted for a [redacted] receiving a [redacted]; and
- Member Age / Procedure Inconsistency – a claim was submitted for a [redacted].

Failure to detect these system weaknesses increases the risk that benefits are being paid for procedures that were not actually performed.

The BCBSA has a long standing corrective plan in place to incrementally implement medical edits into FEP Direct. The current monthly update from BCBSA to OPM indicated that a new release for FEP Direct is scheduled for April of 2014. These controls will be evaluated again during subsequent audits of the FEP Direct system.

Duplicate Claims

Two separate test claims were processed for the same patient, procedure code, diagnosis code, service date and billed amounts, but using different providers.

Due to the potential fraudulent nature of this scenario, we expected the system to suspend these claims for further review; however, no edit was generated by the system. Failure to detect potentially duplicate claims increases the risk that fraudulent or erroneous claims are paid.

Recommendation 10

We recommend that Premera ensure the appropriate system modifications are made to prevent duplicate claims from processing without proper verification.

Premera Response:

"In response to this recommendation, the Plan submitted the enhancement requests to the FEP Operations Center on March 6, 2014 and copies were sent to the OPM OIG Audit Staff on March 19, 2014 (folder name was Test Claim Follow-up). See Attachment E, Request # 20141648 and 20141651. The Plan will provide an update on this recommendation once feedback on the request is received."

OIG Reply:

As part of the audit resolution process, we recommend that Premera provide OPM's HIO with evidence when the response from the FEP Operations Center to the request has been received.

G. Health Insurance Portability and Accountability Act

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

Premera has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. Premera has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. Premera reviews its HIPAA privacy and security policies annually and updates when necessary. Premera's Privacy Office oversees all HIPAA activities, and helps develop, publish, and maintain corporate policies. Each year, all employees must complete compliance training which encompasses HIPAA regulations as well as general compliance.

Nothing came to our attention to indicate that Premera is not in compliance with the various requirements of HIPAA regulations.

III. Major Contributors to This Report

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

- [redacted] Group Chief
- [redacted] Lead IT Auditor-In-Charge
- [redacted] Lead IT Auditor
- [redacted] IT Auditor
- [redacted] IT Auditor
- [redacted] IT Auditor

Appendix

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans
Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

June 30, 2014

[redacted] Group Chief
Claims & IT Audits Group,
U.S. Office of Personnel Management
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT AUDIT REPORT
Premera Blue Cross IT Audit
Plan Code 430
Audit Report Number 1A-10-70-14-007
(Dated April 17, 2014 and received April 18, 2014)

The following represents the Plan's response as it relates to the recommendations included in the draft report.

Note: Premera is requesting wording changes to clarify or correct information in the draft report as indicated in Attachment A.

A. Security Controls

No Recommendations

B. Access Controls

1. Facility and Data Center Physical Access Controls

Recommendation 1

We recommend that Premera improve the physical access controls at its data center. At a minimum, the computer room entrance should require multi-factor authentication and have controls to prevent piggybacking.

Plan Response

In response to this recommendation, Premera has installed a multi-factor authentication key pad requiring staff to enter a unique pin number. Please see Attachments B and C.

Premera previously had the following controls in place:

- Restricted badge access to limited personnel who have management approval for Data Center access.

- Visitor sign in at the main reception in building 4, as well as at the Data Center by authorized Data Center personnel with badge access.
- Video camera surveillance triggered by motion detectors at the Data Center door. The camera data is monitored by security personnel.

2. Password Configuration Settings

Recommendation 2

We recommend that Premera reconfigure its information systems to ensure compliance with the corporate approved password policy.

Plan Response

In response to this recommendation, Premera agrees to investigate and remediate as appropriate by December 31, 2014.

C. Network Security

1. System Patching

Recommendation 3

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

Plan Response

In response to this recommendation, Premera agrees to implement procedures and controls for appropriate deployment of service packs and hotfixes by December 31, 2014.

However, Premera respectfully disagrees with the section of the recommendation related to patches as it believes deployment of critical security patches is in compliance with the documented patch management policy provided to the OPM Audit Staff in Information request 13.

2. Noncurrent Software

Recommendation 4

We recommend that Premera implement a methodology to ensure that only current

and supported versions of system software are installed in its network environment.

Plan Response

In response to this recommendation, Premera agrees to investigate noted (Audit Inquiry 04) applications in the environment to ensure compatibility and supportability and will remediate appropriately by December 31, 2014.

3. Insecure operating system configuration

Recommendation 5

We recommend that Premera remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Plan Response

In response to this recommendation, Premera agrees to investigate the noted technical weaknesses (Audit Inquiry 04), and will remediate appropriately by December 31, 2014.

D. Configuration Management

1. Server and Database Baseline Configurations

Recommendation 6

We recommend that Premera document approved [redacted] *baseline configurations for all versions of those platforms utilized in its* network environment.

Plan Response

In response to this recommendation, Premera agrees to establish baseline configuration documentation for all supported [redacted] by December 31, 2014.

Recommendation 7

We recommend that Premera routinely audit all [redacted] security configurations settings to ensure they are in compliance with the approved baseline.

Plan Response:

In response to this recommendation, Premera agrees to remediate appropriately to ensure compliance with approved and documented baselines by December 31, 2014.

E. Contingency Planning

1. Contingency Planning

Recommendation 8

We recommend that Premera implement a methodology to ensure that all applications are subject to routine disaster recovery testing.

Plan Response

Premera respectfully disagrees with this recommendation as it believes that the recommendation is focused on Premera's low impact systems (i.e., Tier 3 and 4 systems).

The strategy and solution for the recovery of Tier 3 and 4 applications and services, include regularly scheduled data replication for availability at the recovery facility with build following the declaration of a major event or disaster. In addition, on an annual basis, the solution, restoration and recovery procedures of selected Tier 3 and 4 applications and services will be exercised via stand-alone tests to validate recoverability within their defined RTO (recovery time objectives). Tabletop reviews will be performed following the development or revisions of recovery documents.

Premera believes we meet the *NIST SP 800-34 Section 3.5.3* guidance which states "for low impact systems, a tabletop exercise at an organization-defined frequency is sufficient."

Please see information request 2 section 7.2 (IT Disaster Recovery Plan) provided to the OPM Audit staff.

Recommendation 9

We recommend that Premera reevaluate its fuel delivery situation and determine if a contract with a fuel vendor would improve its disaster recovery program.

Plan Response

In response to this recommendation, Premera has obtained a memorandum from our fuel vendor acknowledging that Premera has priority delivery as a Preferred Customer. See Attachment D

F. Claims Adjudication

1. Application Controls Testing - Duplicate Claims

Recommendation 10

We recommend that Premera ensure the appropriate system modifications are made to prevent duplicate claims from processing without proper verification.

Plan Response

In response to this recommendation, the Plan submitted the enhancement requests to the FEP Operations Center on March 6, 2014 and copies were sent to the OPM OIG Audit Staff on March 19, 2014 (folder name was Test Claim Follow-up). See Attachment E, Request # 20141648 and 20141651. The Plan will provide an update on this recommendation once feedback on the request is received.

Thank you for the opportunity to provide an update to the Final Report. If you have any questions in the interim, please contact [redacted] at [redacted] or at [redacted]

Sincerely,

[redacted]

[redacted], CISA, CRSA
Managing Director, FEP Program Assurance

Attachments

cc: [redacted] OPM
[redacted] Premera
[redacted] FEP
[redacted] FEP