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 KAISER FOUNDATION HEALTH PLAN NORTHERN AND SOUTHERN CALIFORNIA REGIONS

Report No. 1C-59-00-09-002

Date: June 18, 2009

--CAUTION--

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

# Audit Report

## FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
## CONTRACT CS 1044

## KAISER FOUNDATION HEALTH PLAN
## NORTHERN AND SOUTHERN CALIFORNIA REGIONS
## PLAN CODES 59/62

[redacted]

**Report No. 1C-59-00-09-002**

**Date:** June 18, 2009

**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 CS 1044

## KAISER FOUNDATION HEALTH PLAN
## NORTHERN AND SOUTHERN CALIFORNIA REGIONS
## PLAN CODES 59/62

[redacted]

**Report No. 1C-59-00-09-002**

**Date:** June 18, 2009

This final report discusses the results of our audit of general and application controls over the information systems at the Northern and Southern California regions of Kaiser Foundation Health Plan (Kaiser).

Our audit focused on the information systems used to process data related to Kaiser members that are part of the Federal Employees Health Benefits Program (FEHBP). We documented controls in place and opportunities for improvement in each of the areas below.

Entity-wide Security Program

The policies and procedures that comprise Kaiser's entity-wide security program appear to provide an adequate foundation to protect the organization's information resources. However, we determined that neither the Northern nor Southern California regions of Kaiser are routinely conducting business impact analyses and risk assessments in accordance with company policy.

Access Controls

Kaiser has implemented a variety of controls to prevent or detect unauthorized access to its physical and logical resources. Such controls include: procedures for securely granting and removing access to networks and applications; the use of tools to detect unauthorized network activity; and controls to encrypt data at rest and data transferred via email. However, we also noticed several areas where Kaiser's access controls could be improved, including: physical access to its facilities; [redacted]; security of network incident logs; review of active user accounts; disabling inactive user accounts; and password controls.

Application Development and Change Control

Kaiser has adopted a traditional system development life cycle (SDLC) methodology that incorporates the use of formal change requests managed by a project tracking tool. Kaiser also uses a structured approval process for all changes to its applications.

System Software

Kaiser has implemented a thorough system software change control methodology. This process utilizes a change management tool to control and track changes and involves multiple levels of approvals. It was also noted that Kaiser has implemented policies and procedures for conducting emergency changes and limiting access to system software to the appropriate individuals.

Business Continuity

A Disaster Recovery (DR) Organization has been designated within Kaiser with the responsibility to develop, support, test, maintain, and execute disaster recovery plans. However, we determined that a thorough business continuity and disaster recovery plan has not been implemented for any of the six information systems reviewed during this audit.

Application Controls

Kaiser has implemented a variety of controls to ensure that electronic transactions related to member service encounters are valid, authorized, and processed accurately. However, we noted several weaknesses in the manner in which Kaiser's systems process FEHBP data. Kaiser's systems inappropriately processed several transactions presented by OIG auditors, including: an encounter with a procedure/diagnosis inconsistency; an encounter with a procedure/gender inconsistency; an encounter with a procedure/provider inconsistency; an encounter with non-covered benefits; an encounter with emergency room to hospital transfers; and an encounter with a procedure/age inconsistency.

Health Insurance Portability and Accountability Act (HIPAA)

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

# Contents

**Page**

# 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 data related to Federal Employees Health Benefits Program (FEHBP) members at the Northern and Southern California Regions of Kaiser Foundation Health Plan (referred to throughout this report as 'Kaiser').

The audit was conducted pursuant to Contract CS 1044; 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.

The [redacted] facilities supporting Kaiser's Northern California region are located in [redacted] and [redacted] and the [redacted] facilities supporting Kaiser's Southern California region are located in [redacted] A data center supporting the information systems listed above is located in [redacted]

This was the OIG's first audit of general and application controls at Kaiser.

All personnel that worked with the auditors were particularly helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

## Objectives

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

These objectives were accomplished by reviewing the following areas:

- Entity-wide security program;
- Access controls;
- Application development and change control;
- Segregation of duties;
- System software;
- Business continuity;

- Application controls specific to Kaiser's claims processing systems; and
- Health Insurance Portability and Accountability Act (HIPAA) compliance.

## Scope

Our performance audit was conducted in accordance with generally accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, the OIG obtained an understanding of Kaiser's internal controls through interviews and observations, as well as the inspection of various documents, including information technology and other organizational policies and procedures. This understanding of Kaiser'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.

We evaluated the confidentiality, integrity, and availability of Kaiser's computer-based information systems, and found that there are opportunities for improvement in the information systems' internal controls. These areas are detailed in the "Audit Findings and Recommendations" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on Kaiser's system of internal controls taken as a whole.

The scope of this audit centered on, but was not limited to, the information systems used by Kaiser to process and store data related to its Northern and Southern California FEHBP members, including:

- [redacted] – used by providers and hospitals to record the services provided to Kaiser members;
- [redacted] – Kaiser's membership system that stores data related to the Plan's enrollees;
- [redacted] – a series of analytical databases that store and format data critical to Kaiser's health plan and service delivery lines of business;
- [redacted] – uses data produced by the other systems to develop the adjusted community pricing rates for Kaiser's customers (e.g., OPM/FEHBP);
- [redacted] – adjudicates claims submitted by outside (non-Kaiser) providers for services rendered to Northern California Kaiser members; and
- [redacted] – adjudicates claims submitted by outside (non-Kaiser) providers for services rendered to Southern California Kaiser members.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Kaiser. 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.

The fieldwork portion of this audit was performed in [redacted] These on-site activities were performed in October and November 2008. The OIG completed additional audit work before and after the on-site visits at OPM's office in

Washington, D.C. The findings, conclusions, and recommendations outlined in this report are based on the status of information system general and application controls in place at Kaiser as of November 28, 2008.

## Methodology

In conducting this review the OIG:

- Gathered documentation and conducted interviews;
- Reviewed Kaiser's business structure and environment;
- Performed a risk assessment of Kaiser'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; and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, the auditors used judgmental sampling in completing their compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating Kaiser's control structure. This criteria includes, but is not limited to, the following publications:

- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's Federal Information System Controls Audit Manual;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and
- HIPAA Act of 1996.

## Compliance with Laws and Regulations

In conducting the audit, the OIG performed tests to determine whether Kaiser's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Kaiser 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. Entity-wide Security Program

The entity-wide security component of this audit examined the policies and procedures that are the foundation of Kaiser's overall IT security controls. The OIG evaluated Kaiser's ability to manage risk, develop security policies, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

The OIG also reviewed various Kaiser human resources (HR) policies and procedures to evaluate the controls in place regarding various HR functions such as hiring, terminations, transfers, conflicts of interest, training, and standards of conduct.

The policies and procedures that comprise Kaiser's entity-wide security program appear to provide an adequate foundation to protect the organization's information resources. However, the section below details one instance where Kaiser's policy related to risk assessment did not appear to be enforced.

### 1. Risk Assessment

Kaiser's Northern and Southern California regions have both developed a "Security Risk Management and Evaluation Policy" that details requirements for identifying and managing security incidents to reduce their harmful effects and prevent reoccurrence. The policy requires both regions to identify, assess, and mitigate risks related to the security of sensitive data.

In addition, according to Kaiser's "National Kaiser Business Continuity Management Policy," every department within the organization is required to identify critical business functions and work flow dependencies by performing a business impact analysis.

Based on interviews with Kaiser personnel and Kaiser's response to various documentation requests, the OIG determined the requirements described above are not being adhered to by either the Northern or Southern California regions of Kaiser.

HIPAA Security Rule 164.308(a)(1)(ii) requires all Plans to: "(A) . . . Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. . . (B) . . . Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level . . . ."

Additionally, NIST SP 800-30, Risk Management Guide for IT Systems, recommends that a risk assessment contain components such as risk identification, risk evaluation (probability and impact), and recommendations on how to manage and mitigate risks.

Failure to conduct thorough risk assessments increases the likelihood that system vulnerabilities may not be identified. Risk assessments and business impact analyses provide a basis for establishing appropriate security controls and selecting cost-effective techniques to implement these controls.

**Recommendation 1**

We recommend that Kaiser conduct periodic business impact analyses and risk assessments on its information systems in accordance with corporate policy, HIPAA requirements, and NIST guidelines.

***Kaiser Response:***

***"While the Carrier generally agrees with this finding of the Draft Report, the Carrier wishes to highlight the important programs in place to establish compliance with its security risk and business continuity management policies and prevailing standards. These programs have already developed significant processes that fulfill the requirements of the security risk management and business continuity management policies and, to the extent that gaps remain, these programs have already developed plans to address them. Most of the programs began in 2008. Because the Carrier believed the scope of the audit was the 2007 Contract Year, the Carrier did not provide the auditors with documents related to activities that occurred after 2007."***

See Appendix for Kaiser's full response to this recommendation.

**OIG Reply:**

The OIG issued a formal pre-audit request for documentation that asked for a copy of Kaiser's "current risk assessments." Nothing in this document indicated that the scope of the request was limited to the 2007 contract year. On September 15, 2008, Kaiser issued a written response to the OIG that stated that "the Carrier is currently planning a new risk assessment process to review all applications against updated security requirements and risk criteria. Since this assessment is in the planning stage, no risk assessment information is currently available."

However, we do acknowledge the steps that Kaiser is taking to become fully compliant with its security risk and business continuity management policies. As part of the audit resolution process, we recommend that Kaiser provide OPM's Center for Retirement and Insurance Services (CRIS) with appropriate supporting documentation of the actions it takes to address this audit recommendation.

## B. Access Controls

Access controls are the policies, procedures, and techniques an organization has put in place to prevent or detect unauthorized physical or logical access to sensitive resources.

The OIG examined the logical controls protecting Kaiser's network environment and the applications used to process or store data related to Kaiser's FEHBP members. During this review, the following controls were documented:

- Procedures for approving and securely granting access to networks and applications;
- Procedures for removing network and application access from individuals that no longer require access;
- The use of a variety of tools to detect and prevent unauthorized system access and intrusion attempts; and
- The use of tools to encrypt data at rest as well as data transferred via email.

The OIG also examined the physical controls of Kaiser's facilities in [redacted]

The following sections detail the opportunities for improvement that were noted for logical and physical access controls.

**1. Physical Access Controls**

Kaiser has implemented very strong interior and exterior physical access controls at its data center in [redacted] However, the physical access controls could be improved at two office buildings visited by the OIG.

OIG auditors visited three Kaiser office facilities and reviewed controls in place related to access to the facility, access to sensitive resources within the facility, and visitor access. The sections below detail the auditors' observations related to physical access controls at these locations.

[redacted]

A Kaiser facility in [redacted] contains office space for several companies in addition to Kaiser. All Kaiser employees in this building are provided with electronic access cards. An electronic access card reader located in the elevator will only allow employees to access floors owned by their respective company. Visitors are not provided with an access card and must be escorted by a Kaiser employee. The OIG did not detect any weaknesses of the physical access controls at this facility.

[redacted]

One of the [redacted] facilities used by Kaiser's Northern California region is located in [redacted] Access to the public areas of this building (hallways, lobbies, stairwells, elevators) is not restricted. Access to the office suites occupied by Kaiser is controlled by an electronic access card system; users must swipe an access card against an electronic reader to unlock the door. [redacted]

*Visitor Access*

Although the access card system limits physical access to Kaiser's office space, a weakness exists in Kaiser's procedures for distributing [redacted] cards. When a visitor requires access to Kaiser suites, they must check in at Kaiser's reception/security desk. After signing a visitor log, the visitor will be provided a [redacted] card that is valid for the remainder of that business day. Visitors to this building do not require an escort and are not required to show a photo ID before being provided with a temporary access card.

*Unlocked Conference Room*

The OIG observed that an access card reader was disabled on the door to a Kaiser conference room. Although a second (active) card reader prevented unauthorized access to the office space beyond the conference room, the room did contain an active network and telephone port.

[redacted] This building is occupied entirely by Kaiser, and only Kaiser employees and visitors are allowed access. A security guard is stationed in the main lobby of this building to verify that individuals entering the building have a valid Kaiser employee identification badge. Individuals without an ID badge are directed to a security desk located on the side of the lobby. At the security desk, visitors are required to sign in and indicate which room they will be visiting. However, after signing in, visitors are allowed unescorted access to the building, and no procedures exist to verify that a Kaiser employee is expecting a visitor. Furthermore, this building does not contain any internal access card readers or other mechanisms to prevent unauthorized access to various work spaces.

NIST SP 800-12, An Introduction to Computer Security, outlines the benefits of implementing strong physical security controls. Specifically, it describes how physical access controls can reduce the risk of interruptions to computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and physical theft.

The [redacted] controls described above increase the risk [redacted] his risk is further increased by [redacted]

**Recommendation 2**

We recommend that Kaiser improve the physical access controls at its [redacted] facilities.

***Kaiser Response:***

***"While the Carrier generally agrees with the Draft Report, it notes that significant positive security practices are already in place in these facilities in [redacted] [redacted] These practices, and the plans to improve them, are described more fully below. In addition, the [redacted] facility contains internal access card readers that protect critical areas, and, with regard to the card reader on the conference room in [redacted] the Carrier confirmed with building security that this reader had been intentionally deactivated. . . .***

***"Like the majority of office buildings nation-wide, the physical security program for the buildings in [redacted] [redacted] is intended to provide ready access to spaces within the building by authorized personnel and visitors. Positive surveillance practices are employed to screen and filter criminal opportunists. Employees are directed to immediately report suspicious activities to security. The program is also integrated with, and reliant upon, other security measures to manage the overall risks presented to the Carrier by access of unauthorized persons (e.g. mechanical locks, card key secured access, staffed reception areas, physical device security measures, network security protocols, etc.). In some instances, such as the [redacted] building, facilities are leased and operated by various landlords and/or property management firms. For these facilities, the owner and/or their representatives have implemented what they believe to be appropriate and reasonable office building protective requirements for their premises.***

***"At the time of the finding, the conference room utilized by the auditors was open for general use; the card reader's operation was intentionally suspended. The card reader is activated whenever limited access is requested by the tenant.***

***"Considering the above, the Carrier does not believe significant physical modifications to these facilities and/or major deployment of additional security technologies are warranted at this time. However, the findings do recognize opportunities to reinforce current physical security protocols. Accordingly, subject to budgetary constraints, the Carrier plans to take the following actions . . . ."***

See Appendix for Kaiser's full response to this recommendation.

**OIG Reply:**

The response to the draft audit report indicates that Kaiser considers its physical security program comparable to that of the majority of office buildings nation-wide. However, we continue to believe that Kaiser's physical access controls are substantially weaker than those implemented by the majority of health insurance carriers throughout the country that the OIG audit staff visits on a regular basis. For example, other carriers generally have controls in place that prevent unauthorized individuals from physically accessing an active network port (such as the one available in the unlocked conference room in [redacted]

However, we acknowledge the steps that Kaiser is taking or plans to take to improve its physical security program. As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with appropriate supporting documentation of the actions it takes to enhance physical access controls to its facilities.

### 3. Security of Network Incident Logs

Kaiser has implemented a [redacted] where individuals continuously monitor the performance of the various operating platforms and network environments that house the applications critical to Kaiser's business. The [redacted] operation facilitates many controls related to IT security monitoring and incident response. However, details of security incidents monitored by the [redacted] are published on a [redacted] that is accessible by anyone with access to [redacted].

NIST SP 800-61, Computer Security Incident Handling Guide, provides guidelines for securely documenting data related to security incidents. Specifically, it states that an "incident response team should take care to safeguard data related to incidents because it often contains sensitive information - for example, data on exploited vulnerabilities, recent security breaches, and users that may have performed inappropriate actions. To reduce the risk of sensitive information being released inappropriately, the team should ensure that access to incident data is restricted properly."

The [redacted] contains a significant volume of sensitive data such as server names and IP addresses. Access to this information increases the risk that an attacker could successfully gain unauthorized access to sensitive information or disrupt Kaiser's network environment and therefore its business processes. [redacted]

**Recommendation 4**

We recommend that Kaiser limit access to the [redacted] to employees whose job function requires access.

***Kaiser Response:***

***"This recommendation does not take into account that the [redacted] was specifically put in place to provide client transparency to real time incidents in progress, and for the Carrier's service desk to see a consolidated view of only high and critical incidents to provide quick real time status and service direction. The [redacted] currently averages close to [redacted] to the site Monday to Friday, and is used widely by clients and IT staff for information on High and Critical Incidents in progress. Because the Draft Report did not note this important function of the [redacted] its recommendation in this regard would significantly limit the utility and purpose of the [redacted]***

***"The Carrier intends to adjust its [redacted] to address these concerns. Within thirty (30) days of the Final Report, the Carrier will initiate the process to remove certain links from the [redacted] This will eliminate wide access to potentially sensitive infrastructure data and eliminate access to impact data and bridge call status.***

***"The Carrier believes this adjustment will generate additional status calls to the Help Desk. It will test to ensure the effectiveness of the adjustment. This process is expected to take at least thirty (30) days to implement."***

**OIG Reply:**

We acknowledge the steps that Kaiser is taking to limit access to the [redacted] to individuals whose job function requires access. We continue to assert that there are significant IT security risks inherent with the practice of allowing [redacted] access to any individual that can physically access one of Kaiser's [redacted]. As discussed in section B.1, above, we noted several instances where [redacted] were not adequately protected.

We understand the important functionality of the [redacted] as well as the need for IT clients and staff to have access to it. The audit recommendation does not suggest that Kaiser revoke [redacted] access to these individuals. Rather, we continue to recommend that Kaiser develop a methodology that allows appropriate access to the [redacted] while preventing unauthorized individuals from accessing this sensitive information.

As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with appropriate supporting documentation of the actions it takes to address this audit recommendation.

**4. Periodic Management Review of Active User Accounts**

As mentioned in the scope section of this report, OIG auditors reviewed the system access controls of six Kaiser applications that are used to process data relevant to Kaiser's FEHBP line of business. Although Kaiser has implemented a variety of controls to ensure that active user accounts on its applications are reviewed for appropriateness, [redacted]

NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule, states that organizations should develop "procedures for reviewing and, if appropriate, modifying access authorizations for existing users." Furthermore, NIST SP 800-12, An Introduction to Computer Security, states that access reviews should "examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth."

The procedures for reviewing user access were similar for the [redacted]. For several systems, Kaiser's [redacted] administrators assist in the process by providing the business unit that owns the application with a list of active users. However, in each case, it was the responsibility of the business unit to review active user accounts for appropriateness. [redacted]

This issue is further complicated by the fact that the business unit managers that approve access to this particular application are not involved in the process of removing user accounts. This creates a scenario where the approver only has a one-way view of accounts, and does not know which (or how many) of the accounts that they approved remain active, increasing the risk that user accounts exist for individuals that no longer require access to this application.

**Recommendation 5**

We recommend that Kaiser periodically review the active user accounts for all of its critical applications to verify that accounts exist only for active employees whose job function requires access to that application.

***Kaiser Response:***

***"In response to this concern, by the end of the Second Quarter of 2009, the designated business contact will work with the [redacted] administrators to develop an access review process, which will include a quarterly review of staffing changes."***

**OIG Reply:**

We acknowledge the steps that Kaiser is taking to address this recommendation. As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with appropriate supporting documentation of the actions it takes to improve controls related to the periodic review of active user accounts.

## 5. Disabling Inactive User Accounts

OIG auditors reviewed the user access controls of six Kaiser applications that are used to process data relevant to Kaiser's FEHBP line of business. Although Kaiser has implemented a variety of controls to ensure that user accounts are automatically disabled after a period of inactivity, there were no controls in place to automatically disable inactive accounts for one of the six systems reviewed.

NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, suggests that an information system automatically disable inactive user accounts after a predetermined period of inactivity.

The five systems that do have controls for automatically disabling inactive user accounts are housed in Kaiser's [redacted] environment. The one system that does not have similar controls is housed in an [redacted] environment. As mentioned in section B.4, Kaiser has implemented a process to manually review user accounts for appropriateness. However, implementing technical controls to automatically disable inactive user accounts for all systems further decreases the risk that user accounts exist for individuals that no longer require access to this application.

**Recommendation 6**

We recommend that Kaiser implement technical controls on all of its critical applications to automatically disable inactive user accounts after a predetermined period of inactivity.

***Kaiser Response:***

***"The design of the application noted in Recommendation 6 is based on multiple 'instances' which make truly automated disabling of access substantially more complex than the five [redacted] applications which did not contain exceptions.***

***"Because of these limitations on the automatic setting, the user security and processing team manually processes deactivation for non-use by extracting last login dates for all instances and specifically setting the account status to inactive on all instances, which fully deactivates the account, per the regional access termination documentation provided during the audit."***

**OIG Reply:**

If Kaiser determines that it is not cost or resource efficient to implement the audit recommendation, we recommend that it formally document its understanding and acceptance of the risks inherent with this decision. This documentation should be provided to OPM's CRIS in order to close the audit recommendation.

## 6. Password Controls

OIG auditors reviewed the authentication controls of six Kaiser applications that are used to process data relevant to Kaiser's FEHBP line of business. Although Kaiser has implemented a corporate password policy, as well as a variety of technical controls to enforce this policy, Kaiser has not implemented adequate password controls for one of the six systems reviewed.

The OIG identified three separate password settings that could be improved for this system. The specific settings were provided to Kaiser personnel during the fieldwork phase of the audit and will not be included in this report. One of the settings was in violation of Kaiser's corporate password policy. The other two settings, while compliant with Kaiser's policy, do not meet industry best-practice standards or the password attributes suggested in NIST SP 800-12, An Introduction to Computer Security.

Weak password requirements increase the risk that an unauthorized individual can gain access to Kaiser's sensitive IT resources and data.

**Recommendation 7**

We recommend that Kaiser update its corporate password policy and implement technical controls to enforce the policy on all of its critical applications.

***Kaiser Response:***

***"In 2008, the Carrier implemented a new enterprise password policy based on balancing existing policies, current industry best-practices, and the various risks and needs of its associates, which include care delivery personnel. The required password length was increased, and passwords were also forced to be made more complex.***

***"With these more stringent standards in place, the Carrier's decision to remove this control was made following a comprehensive analysis of the value of that control versus operational needs, particularly the needs of its care delivery personnel. It was determined that, given stronger rules for password complexity, the net effect would be equal security with less impact for the users.***

***"In light of these considerations, and the stringent controls already in place, the Carrier believes sufficient password controls are in place."***

**OIG Reply:**

If Kaiser determines that its current password policy is adequate, we recommend that it formally document its acceptance of the inherent risks associated with deviating from widely accepted password standards such as those outlined in NIST SP 800-12, An Introduction to Computer Security.

In addition, Kaiser's response did not address the password setting that was not compliant with the company's password policy. We continue to recommend that Kaiser configure its password settings in a manner that is compliant with its own corporate password policy.

## C. Application Development and Change Control

The OIG evaluated the policies and procedures governing software development and change control over Kaiser's [redacted] as well as its [redacted]

Kaiser has adopted a traditional system development life cycle (SDLC) methodology that incorporates the use of formal change requests managed by a project tracking tool. Kaiser also uses a structured approval process for change requests. The following controls related to testing and approvals of software modifications were observed:

- Testing activities are conducted at various stages of the SDLC;
- Appropriate levels of approval must be completed before the change is migrated into the production environment; and
- Procedures and controls are in place for emergency changes.

The OIG also observed the following controls related to software libraries:

- Kaiser has a software library management tool that provides sufficient control of application software;
- Application software is segregated among development, testing, and production regions; and

- There is a clear segregation of duties along organizational lines for all application software modifications.

## D. System Software

The system software that houses the production applications within the scope of this audit reside at Kaiser's data center in [redacted] Five of these applications are run on [redacted]

Kaiser has implemented a thorough system software change control methodology. This process utilizes a change management tool to control and track changes, and involves multiple levels of approvals.

It was also noted that Kaiser has implemented policies and procedures for conducting emergency changes and limiting access to system software to the appropriate individuals. The OIG reviewed several high level security settings of Kaiser's [redacted], and did not identify any weaknesses.

## E. Business Continuity

We reviewed Kaiser's service continuity program to determine if (1) procedures are in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan exists to recover critical operations should interruptions occur. The following section documents the results of the service continuity review and provides recommendations for improving Kaiser's service continuity program.

### 1. Disaster Recovery Plan

Based on interviews with Kaiser personnel and Kaiser's response to various documentation requests, the OIG determined that a thorough business continuity and disaster recovery plan has not been implemented for any of the six applications reviewed during this audit.

A Disaster Recovery (DR) Organization has been designated within Kaiser with the responsibility to develop, support, test, maintain and execute disaster recovery plans. The DR Organization has prepared a time line to establish a reasonable deadline for completing disaster recovery plans for its critical applications. However, as of November 2008, the disaster recovery plans are incomplete and Kaiser is still in the planning phase of its disaster recovery capability overhaul.

Furthermore, although Kaiser has implemented procedures for periodic testing of disaster recovery plans, a full scope disaster recovery test has yet to be conducted for Kaiser's critical applications.

A variety of criteria exists to emphasize the need for Kaiser to develop a thorough business continuity and disaster recovery capability, including:

- Kaiser's business continuity policy states that Kaiser will "develop and maintain business continuity plans to address the actions necessary to protect the security of its electronic information in the event of an emergency or disaster." Also, Kaiser will periodically test and update business continuity plans.
- Kaiser's corporate disaster recovery policy states that Kaiser will "develop and maintain a disaster recovery plan to address the actions to be taken to recover, as necessary, damage to computing or biomedical systems/devices containing its electronic information and/or lost KP electronic information in an emergency or disaster." In addition, the policy states Kaiser will periodically test and update disaster recovery plans.
- HIPAA Security Rule 164.308 (a)(7)(i) states that "a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures. . . . Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation."
- NIST SP 800-34, Contingency Planning Guide for IT Systems, states that "Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan."

Failure to adequately develop, maintain, and test business continuity and disaster recovery plans increases the risk that Kaiser will be unable to maintain critical business operations when unexpected events occur.

**Recommendation 8**

We recommend that Kaiser develop and implement business continuity and disaster recovery plans for all of its critical applications in accordance with company policy and other relevant criteria.

***Kaiser Response:***

***"The Carrier has made considerable investments in disaster recovery and business continuity, and has made significant strides in advancing its implementation and testing capability. For instance, the recent acquisition and integration of the new data center (NDC) required an enormous commitment of resources, represented great progress in the Carrier's disaster recovery and business continuity implementation efforts, and went a long way to ensuring the viability of critical systems in the event of a disaster.***

***As these and other efforts reflect, the Carrier understands the importance of disaster recovery and business continuity management, and is committed to completing the implementation of its programs within the timelines it has set for itself."***

See Appendix for Kaiser's full response to this recommendation.

**OIG Reply:**

We acknowledge the steps that Kaiser is taking to improve its disaster recovery and business continuity programs in a timely manner. As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with appropriate supporting documentation of the actions it takes to address this audit recommendation.

**Recommendation 9**

We recommend that Kaiser test its disaster recovery plans at least annually.

***Kaiser Response:***

See Kaiser Response to Recommendation 8

**OIG Reply:**

See OIG Reply to Recommendation 8

## F. Application Controls

The OIG evaluated the application controls of the information systems that Kaiser uses to adjudicate the data associated with an FEHBP member receiving services from a Kaiser professional provider or hospital ("encounters"). The systems included in the scope of this review include:

- [redacted] – used by providers and hospitals to record the services provided to Kaiser members;
- [redacted] – Kaiser's membership system that stores data related to the Plan's enrollees;
- [redacted] – a series of analytical databases that store and format data critical to Kaiser's health plan and service delivery lines of business; and
- [redacted] ([redacted] – uses data produced by the other systems to develop the adjusted community pricing rates for Kaiser's customers (e.g., OPM/FEHBP).

The OIG tested the controls of these systems by submitting a series of test encounters of FEHBP members into the systems' test environments. The test encounters were created with inherent flaws designed to evaluate the systems' ability to either correct the errors or prevent the erroneous data from being included in the calculation of the FEHBP's adjusted community rating (rating). OIG auditors worked with Kaiser employees ("testers") to enter the test encounters, consisting of both professional provider and hospital services, into the [redacted] system. The encounters were then processed through the [redacted]. A report was produced by [redacted] that detailed the final prices assigned to test encounters as it would be used in calculating the FEHBP's rating. The testers used the same system interfaces and had the same privileges that would be available in the system's production environment.

The testing exercise revealed that Kaiser's systems do have many controls in place including, but not limited to, the ability to:

- Detect duplicate encounters and prevent them from being submitted into the [redacted] (both hospital and professional encounters);
- Detect encounters for ineligible members and prevent them from being included in the rating calculation;
- Detect encounters with medical inconsistencies and prevent them from being included in the rating calculation (hospital encounters only); and
- Assign the appropriate price to various encounters based on the member's benefit level (standard or high).

However, the OIG identified several areas where Kaiser's system controls could be improved, as detailed in the sections below.

**1. Medical Edits for Professional Encounters**

Several professional encounters with medical inconsistencies were processed, priced, and inappropriately included in the FEHBP's rating.

**a) Procedure invalid for diagnosis.**

An encounter was processed for a member that received an [redacted] for a diagnosis of a [redacted]. The system did not produce any warning messages indicating that an inconsistency/conflict existed between the diagnosis and procedure, and the encounter was assigned a price and passed to the FEHBP's rating.

A second test encounter with a diagnosis/procedure inconsistency further verifies this system weakness. In the second case, a [redacted] was ordered for a diagnosis of a [redacted], and the encounter was assigned a price and passed to the FEHBP's rating.

After the testers entered the original diagnoses, the system did suggest a series of procedures related to that diagnosis. However, the OIG does not consider this to be an adequate compensating control, as the tester was able to manually search for and order an alternate procedure without significant additional effort.

**b) Procedure invalid for member's gender**.

An encounter for a [redacted] was processed for a [redacted]. Although this procedure is inconsistent with [redacted] anatomy, the encounter was assigned a price and passed to the FEHBP's rating. The system did not produce any warning messages indicating that there was a conflict between the member's gender and the ordered procedure.

**c) Procedure invalid for provider specialty.**

An encounter was processed for a [redacted] performed by an [redacted] is typically performed by an [redacted], and is outside of an

[redacted] specialty. The system did not produce any warning messages related to this inconsistency, and the encounter was assigned a price and passed to the FEHBP's rating. After the testers entered the provider's information, the system did display a series of procedures that would typically be performed by an [redacted]. However, the OIG does not consider this to be an adequate compensating control, as the tester was able to search a full list of procedure codes and select the [redacted] without significant additional effort.

Kaiser utilizes a third party software package that performs medical edits of hospital encounters. However, the results of the system testing indicate that similar controls are not in place for professional encounters. The lack of adequate medical edits in Kaiser's systems to identify anomalies like those listed above increases the risk that invalid professional encounters could be inadvertently or fraudulently processed and improperly included in the FEHBP rating calculation.

**Recommendation 10**

We recommend that Kaiser implement medical edits in its systems to evaluate the medical appropriateness of all encounters that will be included in the FEHBP rating calculation.

***Kaiser Response:***

***"The Carrier's internal delivery operations and its system are already designed to minimize risk and have established controls over how professional encounters are documented and captured. The nature of the Carrier's physician workflow and system functionality minimizes the risk of erroneous coding existing in the rating system data. As described during the onsite testing, because of the Carrier's unique arrangement with its contracted medical groups, individual physicians derive no direct financial benefit from the way a particular encounter is coded. In addition, three tools are built into the Carrier's clinical delivery application to drive a high level of consistency and accuracy:***

1) [redacted] ***that suggest to the provider appropriate diagnoses and procedures for their specialty;***
2) ***A decision tree based tool*** [redacted] ***that presents appropriate procedures based on the chief complaint from the patient; and***
3) ***Best practice help guides or*** [redacted] ***for ordering appropriate procedures based on the patient's condition.***

***"As with covered procedures, individual physicians have no direct financial incentive to inappropriately code services they provide. Although the existing rating data does not check benefit eligibility at a fine level of detail, benefit classes such as infertility treatments or cosmetic services are excluded in the rating data through benefit verification and exclusion logic in the rating data preparation and load process.***

[redacted]

[redacted]

***"To test the extent to which erroneous coding and non-covered services exist in the Carrier's rating data, it reviewed claims data for the existence of those conditions tested during the auditors' on-site visit. The Carrier tested twelve (12) months of data (10/2007 - 9/2008) for a representative sample of our largest commercial customers, representing 14,450,107 member months. These tests revealed no (0) cases of a [redacted] performed on [redacted]; no (0) cases of [redacted] and [redacted] in the same encounter; only three (3) cases of [redacted] during a [redacted]; and no (0) cases of [redacted] in the [redacted]. In addition, it tested twelve (12) months of paid claims data (10/2007 - 9/2008) for all members of the FEHBP, representing 2,147,696 member months, and found only 26 incidences of non-covered [redacted].***

***"This review of actual data indicates that the prevalence of these situations and the associated costs are negligible. The few erroneous codes that appear in the data are statistically insignificant and do not affect a group's premium rate outcome. As part of its regular data validation process, the Carrier will monitor the data for these specific irregularities and if the results should change, it will determine if adjustments are necessary. [redacted].***

***"Given the extremely low prevalence of these particular conditions in the existing data, the Carrier has determined that it is cost prohibitive to invest capital on any other interim solutions prior to [redacted]. Based on economic conditions, these plans may be subject to change."***

**OIG Reply:**

During the fieldwork phase of the audit, Kaiser personnel thoroughly described to OIG auditors the three tools [redacted] that are used to discourage erroneous coding for professional encounters. After receiving a demonstration of the capability of these controls, we concluded that they are not sufficient to prevent or detect fraudulent or accidental coding inconsistencies or the inclusion of non-covered benefits into the FEHBP rating. These tools simply act as guides for the coding process, and in no way prohibit erroneous activity.

Although similar tools exist for the processing of hospital encounters, Kaiser has determined that it is necessary to utilize a third party software package to perform medical edits of hospital encounters. Kaiser's response did not address this inconsistency, and we continue to recommend that Kaiser's professional encounters be processed through the same degree of

medical edits that its hospital encounters are subject to, and that it make system modifications to ensure that non-covered benefits are detected.

Kaiser's response to the draft report also summarized the results of its testing of 12 months of encounter data related to the specific anomalies identified during the OIG testing exercise. This test revealed that very few instances of these medical inconsistencies have been processed through Kaiser's production environment for FEHBP members. While we appreciate the efforts taken to produce this data, we believe that Kaiser's response did not address the intent of the audit recommendation. The OIG deliberately made the test cases obscure and improbable in an effort to emphasize the extent of the system weakness. Although there were only 3 incidents of a [redacted] during a [redacted] and 26 incidents of a [redacted], Kaiser's analysis did not consider the thousands of additional medical inconsistencies or non-covered services that could be affected by the system flaws identified during this audit.

**2. Non-covered benefit**

An encounter was processed for a non-covered [redacted] procedure. Kaiser's systems did not detect that this procedure is not covered by Kaiser's FEHBP benefit structure, and the encounter was assigned a price and passed to the FEHBP's rating.

A second test encounter with a non-covered benefit further verifies this system weakness. In the second case, a [redacted] was ordered, and the encounter was assigned a price and passed to the FEHBP's rating.

Kaiser professionals and hospitals could inadvertently or fraudulently order procedures that are not covered by the FEHBP benefit structure. The lack of system controls to detect such encounters increases the risk that they are being improperly included in the FEHBP ratings calculation.

**Recommendation 11**

We recommend that Kaiser implement the appropriate system modifications to ensure that non-covered benefits are not included in the FEHBP rating calculation.

***Kaiser Response:***

See Kaiser Response to Recommendation 10

**OIG Reply:**

See OIG Reply to Recommendation 10

**3. Emergency Room to Hospital Transfers**

An encounter was processed for a member who was transferred from an emergency room (ER) to a hospital. Kaiser's systems did not correctly apply the FEHBP benefit structure to this encounter, and the services were inaccurately priced and passed to the FEHBP rating.

According to Kaiser's FEHBP benefit structure, members must pay a $50 copay for ER visits, and a $250 copay for hospital visits. However, when an individual is transferred from the ER to a hospital, the $50 ER copay is waived, and the member is only responsible for the $250 hospital copay.

In the test encounter, the [redacted] appropriately generated a $250 bill for the member, but the [redacted] system indicated that the member was liable for $300. The overvaluation of member liability resulted in the price assigned to the services and passed to the rating to be undervalued by $50.

**Recommendation 12**

We recommend that Kaiser implement the appropriate system modifications to ensure that the FEHBP benefit structure (specifically, member copays) are appropriately factored into the pricing of encounters that are included in the FEHBP rating.

***Kaiser Response:***

***"The Carrier understands that this situation may have resulted in a negligible undercharge to the FEHBP, and appreciates the opportunity to adjust its systems. Development of the detailed requirements is currently in process. System modifications are targeted to be developed, tested and in production by December 31, 2009."***

**OIG Reply:**

We acknowledge the steps that Kaiser is taking address this recommendation. As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with appropriate supporting documentation of the actions it takes to ensure its systems appropriately factor the FEHBP benefit structure into the pricing of FEHBP encounters.

## 4. Pricing of Hospital Professional Services and Room and Board

The OIG processed an encounter for a [redacted], and expected the system to pend this encounter due to an [redacted] inconsistency.

Kaiser's systems appropriately split the hospital room/board and professional services into two line items to be evaluated for pricing. However, the systems automatically re-classified the [redacted] as [redacted] (a non-covered procedure). Furthermore, the [redacted] system inaccurately indicated that the member was 100% liable for the room and board charges, and inaccurately priced the [redacted] procedure and passed it to the FEHBP rating.

Kaiser representatives and system testers acknowledged that a "bug" in the system caused the erroneous results observed during the processing of this test encounter. Due to the scope and timeline limitations associated with the testing exercise, the OIG is unable to determine the full extent of this problem.

**Recommendation 13**

We recommend that Kaiser research the extent of the system bug identified during the processing of this test encounter, and implement the appropriate system modifications to correct the problem.

***Kaiser Response:***

***"The Carrier has researched this issue and found that this "bug" only appears when one of its source processing files is empty. This condition does not exist in normal production. It was a problem the Carrier subsequently identified with the FEHBP audit test data run in the test environment. The Carrier's current production validation process does account for this issue; therefore, the Carrier has determined that no further action is required."***

**OIG Reply:**

As part of the audit resolution process, we recommend that Kaiser provide OPM's CRIS with documentation supporting its position that this bug does not exist in the production environment.

## G. Health Insurance Portability and Accountability Act

The OIG reviewed Kaiser's efforts to maintain compliance with the security, privacy and national provider identifier standards of HIPAA. Nothing came to our attention that caused us to believe that Kaiser is not in compliance with the various requirements of these HIPAA regulations.

Kaiser has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. Kaiser has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. The documents related to the HIPAA privacy and security rules are readily available to all Kaiser employees via the company's Intranet. Kaiser employees receive privacy and security related training during new hire orientation, as well as periodic subsequent training as needed.

In addition, the OIG documented that Kaiser has adopted the national provider identifier as the standard unique health identifier for health care providers, as required by HIPAA.

# III. Major Contributors to This Report

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

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted] Auditor-In-Charge
- [redacted], IT Auditor
- [redacted], IT Auditor

# Appendix

March 13, 2009

Mr. [redacted]
Auditor-in-Charge
Information Systems Audits Group
U.S. Office of Personnel Management
Office of the Inspector General
1900 E Street N.W., Room 6400
Washington, D.C. 20415

Re: Kaiser Foundation Health Plan, Inc. - Northern California Region
Kaiser Foundation Health Plan, Inc. - Southern California Region
Response to Draft of a Proposed Report 1C-59-00-09-002 (January 12, 2009)

Dear Mr. [redacted]:

This letter responds to your correspondence of January 12, 2009, which enclosed a Draft of a Proposed Report (Draft Report) based on "the audit of general and application controls over the information systems responsible for processing data related to Federal Employees Health Benefits Program (FEHBP) members at the Northern and Southern California Regions of Kaiser Foundation Health Plan" (Carrier). Draft Report, p. 1. This response addresses the recommendations in the Draft Report. Where appropriate, it also outlines the corrective actions that have been taken or will be taken by the Carrier based on the recommendations.

As you requested, we are submitting copies of this document both electronically and in hard copy.

## SUMMARY OF DRAFT REPORT FINDINGS

As described in the Draft Report, OIG identified several opportunities for improvement and made thirteen (13) recommendations with regard to the information systems subject to audit. In brief, the Draft Report made findings and recommendations in the following areas:

1) "[C]onduct periodic business impact analyses and risk assessments on its information systems" in accordance with company policy and other standards;
2) Improve physical access controls in non-data center office buildings;

3) [redacted]
4) Limit access to network incident logs;
5) Periodically review active user logs for critical applications;
6) Implement technical controls on critical applications to automatically disable inactive user accounts;
7) Update its corporate password policy and implement technical controls on critical applications;
8) “Develop and implement business continuity and disaster recovery plans for all of its critical applications”;
9) “Test its disaster recovery plans at least annually”;
10) “Implement medical edits in its systems to evaluate the medical appropriateness of all encounters that will be included in the FEHBP rating calculation”;
11) “Implement the appropriate system modifications to ensure that non-covered benefits are not included in the FEHBP rating calculation”;
12) “Implement the appropriate system modifications to ensure that the FEHBP benefit structure (specifically, member copays) are appropriately factored into the pricing of encounters”; and
13) “Research the extent of the system bug identified during the processing of this test encounter, and implement the appropriate system modifications to correct the problem.”

## RESPONSE TO DRAFT REPORT FINDINGS

The Carrier generally applauds the many positive observations and findings in the Draft Report, and views these as affirmation of the significant expenditures of time, effort and resources that the Carrier has undertaken to develop, build, and secure its information technology environment. In several instances, the Draft Report has helped the Carrier to identify opportunities to improve the programs, processes, systems and plans it already has in place.

In addition however, Carrier wishes to reiterate or identify additional facts which we believe clarify or place in context a number of the findings in the Draft Report. With regard to many of the opportunities for improvement identified in the Draft Report, the Carrier already has addressed or is in the process of implementing plans to address these opportunities and has provided additional details in the discussion below. The continued development and implementation of these programs may depend on budgetary constraints. We would be pleased to provide any additional information that would help satisfy the concerns noted in the Draft Report.

**Recommendation 1 (A. Entity-Wide Security Program):**

***The Carrier believes that activities begun in 2008 are intended to address HIPAA requirements by conducting periodic business impact analyses and risk assessments on its information systems. These address the implicit risks in Recommendation 1.***

With regard to the Carrier's enterprise-wide security program, the Draft Report indicated that the Carrier was not adhering to its own policies regarding security risk management and evaluation and business continuity management. Draft Report, p. 4. Based on these findings, the Draft Report recommended that the Carrier conduct periodic business impact analyses and risk assessments on its information systems.

While the Carrier generally agrees with this finding of the Draft Report, the Carrier wishes to highlight the important programs in place to establish compliance with its security risk and business continuity management policies and prevailing standards. These programs have already developed significant processes that fulfill the requirements of the security risk management and business continuity management policies and, to the extent that gaps remain, these programs have already developed plans to address them. Most of the programs began in 2008. Because the Carrier believed the scope of the audit was the 2007 Contract Year, the Carrier did not provide the auditors with documents related to activities that occurred after 2007.

**1. The Carrier's risk assessment program for HIPAA privacy and security already conducts periodic risk assessments in compliance with policy and prevailing standards.**

Prior to this audit, to ensure compliance with the risk assessment requirements of HIPAA, the Carrier conducted a privacy and security compliance risk assessment, developed a mitigation plan, and established a two year cycle for future risk assessments. Related documents are available for review upon request.

In 2008, the Kaiser Permanente National Privacy and Security Compliance Office (NPSCO) and the Regional Privacy and Security Officers (RPSOs) conducted a privacy and security compliance risk assessment in accordance with the National Compliance security policy, *Security Risk Management and Evaluation NATL.NCO.ISP.040*. The scope of the risk assessment encompassed all eight regions and was based on the HIPAA privacy and security requirements. Kaiser Permanente's Information Security Office (ISO) purchased [redacted], the assessment tool, and provided technical support during the process.

[redacted] assesses the level of privacy and security compliance and calculates inherent risk by adding the likelihood of risk to risk impact. An initial baseline of 560 questions was identified in [redacted]. NPSCO and ISO filtered the 560

questions into 77 targeted questions based upon the HIPAA Privacy and Security Rule and CMS audit interests.

During the planning phase of the assessment process, RPSOs were designated as the regional subject matter experts and facilitators. NPSCO and the RPSOs met on a weekly basis for most of 2008. During that time the following parameters were agreed upon:

- Use of the [redacted] tool to conduct the assessment and generate findings
- Agreement on [redacted] questions and risk criteria
- Identification of senior leaders to sponsor the project and sign off on findings and risk mitigation plans
- Identification of regional governance committees that would assess risk and determine risk management decisions
- Definition of policy and procedure implementation
- Agreement to target critical and high risks for mitigation

The assessment was conducted and mitigation plans were developed in 2008. Mitigation plans will be measured and reported in 2009 on a quarterly basis.

NPSCO and RPSOs have agreed upon a two year cycle for privacy and security compliance risk assessments. Planning is already underway for the implementation of the 2010 risk assessment. The Carrier is focusing on:

- Scope
- Methodology and tools
- Updating communication, training, documentation, and mitigation tools
- Timelines

**Recommendation 2 (B. Access Controls; 1. Physical Access Controls):**

***While the Carrier has implemented numerous physical access controls at its [redacted] facilities, the Carrier plans to further improve its access controls at these facilities to fully address the localized items noted in Recommendation 2.***

With regard to physical access controls, the Draft Report found that visitors to one building in [redacted] were not required to show photo identification or to have an escort, and that the access card reader to a conference room had been disabled. It also found that in one building in [redacted], although visitors must sign in, they do not need an escort, and "this building does not contain any internal access card readers or other mechanisms to prevent unauthorized access to various work spaces." Draft Report, p. 4. Based on these findings, the Draft Report recommended that the Carrier improve its physical access controls at these facilities.

While the Carrier generally agrees with the Draft Report, it notes that significant positive security practices are already in place in these facilities in [redacted]. These practices, and the plans to improve them, are described more fully below. In addition, the [redacted] facility contains internal access card readers that protect critical areas, and, with regard to the card reader on the conference room in [redacted], the Carrier confirmed with building security that this reader had been intentionally deactivated.

**1. Although the Carrier's program of physical access already provides physical access controls equal to those in similar facilities, the Carrier plans to further reinforce its current security protocols.**

Like the majority of office buildings nation-wide, the physical security program for the buildings in [redacted] is intended to provide ready access to spaces within the building by authorized personnel and visitors. Positive surveillance practices are employed to screen and filter criminal opportunists. Employees are directed to immediately report suspicious activities to security. The program is also integrated with, and reliant upon, other security measures to manage the overall risks presented to the Carrier by access of unauthorized persons (e.g. mechanical locks, card key secured access, staffed reception areas, physical device security measures, network security protocols, etc.). In some instances, such as the [redacted] building, facilities are leased and operated by various landlords and/or property management firms. For these facilities, the owner and/or their representatives have implemented what they believe to be appropriate and reasonable office building protective requirements for their premises.

At the time of the finding, the conference room utilized by the auditors was open for general use; the card reader's operation was intentionally suspended. The card reader is activated whenever limited access is requested by the tenant.

Considering the above, the Carrier does not believe significant physical modifications to these facilities and/or major deployment of additional security technologies are warranted at this time. However, the findings do recognize opportunities to reinforce current physical security protocols. Accordingly, subject to budgetary constraints, the Carrier plans to take the following actions:

1. It will reinforce the current visitor authorization program through staff training and written communication. Visitors to these buildings will be required to show government issued picture ID. Target implementation date: 3rd Quarter 2009.

2. Where not already in place, arrangements will be made [redacted] Target implementation date: 3rd Quarter 2009.

3. Signage in the lobbies of the buildings noted in the audit will be reviewed to ensure that visitors are aware of these requirements immediately upon entering the building. Target implementation date: 3rd Quarter 2009.

4. Approximately [redacted] of the [redacted] building is secured during normal business hours to protect critical or confidential functions. Access to these secured spaces requires an access code or separate access cards. Plans are underway to expand this secured space to a total of approximately[redacted]. Target implementation date: March 2010.

5. A pilot project that involves [redacted] is underway in [redacted] buildings. Technology costs for this program are estimated at between $5,000 and $10,000 per installation. The pilot will be evaluated at the end of the 2nd Quarter of 2009 and, if deemed successful, capital funds will be requested from the regions to expand implementation. Target implementation date: December 2009.

[redacted]

**Recommendation 4 (B. Access Controls; 3. Security of Network Incident Logs):**

***Recommendation 4 concerning the Carrier's network incident logs did not take into account an important function of its logs which would prevent IT internal clients and staff from accessing important information regarding priority incidents.***

With regard to security of network incident logs, the Draft Report raised concerns around the Carrier's practice of communicating specific details of incidents via an Intranet website known as the [redacted] which currently is accessible by anyone with access to [redacted]. It recommended that the Carrier Limit access to the [redacted] to employees whose job function requires access for the information or general status. Draft Report, pp. 7-8.

This recommendation does not take into account that the [redacted] was specifically put in place to provide client transparency to real time incidents in progress, and for the Carrier's service desk to see a consolidated view of only high and critical incidents to provide quick real time status and service direction. The [redacted] currently averages close to [redacted] to the site Monday to Friday, and is used widely by clients and IT staff for information on High and Critical Incidents in progress. Because the Draft Report did not note this important function of the [redacted], its recommendation in this regard would significantly limit the utility and purpose of the [redacted].

The Carrier intends to adjust its [redacted] to address these concerns. Within thirty (30) days of the Final Report, the Carrier will initiate the process to remove certain links from the [redacted]. This will eliminate wide access to potentially

sensitive infrastructure data and eliminate access to impact data and bridge call status.

The Carrier believes this adjustment will generate additional status calls to the Help Desk. It will test to ensure the effectiveness of the adjustment. This process is expected to take at least thirty (30) days to implement.

**Recommendation 5 (B. Access Controls; 4. Periodic Management Review of Active User Accounts):**

***With regard to Recommendation 5, the Carrier is developing an access review process for the application identified in the Draft Report.***

With regard to periodic management review of active user accounts, the Draft Report found [redacted] It recommended that the Carrier implement periodic reviews of active user accounts for critical applications to verify that only active employees whose jobs require them to access an application actually have access. Draft Report, pp. 8-9.

In response to this concern, by the end of the Second Quarter of 2009, the designated business contact will work with the [redacted] administrators to develop an access review process, which will include a quarterly review of staffing changes.

**Recommendation 6 (B. Access Controls; 5. Disabling Inactive User Accounts):**

***The application containing the exception referenced in Recommendation 6 contains architectural elements which preclude utilization of similar auto-disable capabilities used on other applications noted in the Draft Report. The Carrier believes the manual controls implemented on this application adequately address access risks.***

With regard to disabling inactive user accounts, the Draft Report reviewed the user access controls for six applications used to process data relevant to the FEHBP line of business. Although it found that the Carrier has in place "a variety of controls to ensure that user accounts are automatically disabled after a period of inactivity," one system had manual controls to disable inactive user accounts, but had no automatic controls in place. The Draft Report recommended that the Carrier implement automatic controls to disable accounts on this application after a period of inactivity. Draft Report, p. 9.

The design of the application noted in Recommendation 6 is based on multiple "instances" which make truly automated disabling of access substantially more complex than the five [redacted] applications which did not contain exceptions.

Because of these limitations on the automatic setting, the user security and processing team manually processes deactivation for non-use by extracting last login dates for all instances and specifically setting the account status to inactive on all instances, which fully deactivates the account, per the regional access termination documentation provided during the audit.

**Recommendation 7 (B. Access Controls; 6. Password Controls):**

***The Carrier updated its password policy in 2008 based on balancing industry best practices against the risks and needs of its associates, which include care delivery personnel. As such, the Carrier believes sufficient password controls are in place.***

The Draft Report indicated that while five out of six of the applications reviewed have adequate password controls, it believed that three separate password settings on the remaining system could be improved. The Draft Report recommended that the Carrier change these three settings. Draft Report, pp. 9-10.

In 2008, the Carrier implemented a new enterprise password policy based on balancing existing policies, current industry best-practices, and the various risks and needs of its associates, which include care delivery personnel. The required password length was increased, and passwords were also forced to be made more complex.

With these more stringent standards in place, the Carrier's decision to remove this control was made following a comprehensive analysis of the value of that control versus operational needs, particularly the needs of its care delivery personnel. It was determined that, given stronger rules for password complexity, the net effect would be equal security with less impact for the users.

In light of these considerations, and the stringent controls already in place, the Carrier believes sufficient password controls are in place.

**Recommendations 8 and 9 (E. Business Continuity):**

***The Carrier will continue efforts already underway to address the disaster recovery and business continuity risks included in Recommendations 8 and 9.***

With regard to disaster recovery and business continuity management, the Draft Report noted that the Carrier has built a disaster recovery organization with a timeline for completing and testing disaster recovery plans for critical applications. It asserted that "the disaster recovery plans are incomplete" and that no "full scope disaster recovery test has yet to be conducted." Draft Report, p. 11. It recommended that the Carrier "develop and implement business

continuity and disaster recover plans for all of its critical applications" and test these plans at least annually. Draft Report, p. 12.

The Carrier has made considerable investments in disaster recovery and business continuity, and has made significant strides in advancing its implementation and testing capability. For instance, the recent acquisition and integration of the new data center (NDC) required an enormous commitment of resources, represented great progress in the Carrier's disaster recovery and business continuity implementation efforts, and went a long way to ensuring the viability of critical systems in the event of a disaster.

As these and other efforts reflect, the Carrier understands the importance of disaster recovery and business continuity management, and is committed to completing the implementation of its programs within the timelines it has set for itself.

**1. To augment the progress already made, the Carrier is supplementing its disaster recovery program for its mainframe applications.**

Prior to the audit, the Carrier had reviewed and begun to revamp its Disaster Recovery program. As part of this effort, the entire suite of applications was reviewed to determine those that provide mission critical functionality to the organization. For those applications deemed in scope for the new program, disaster recovery requirements were gathered to determine how quickly various applications need to be available. [redacted]

The Carrier has also put in place plans to remediate the rest of the application suite starting with the [redacted] applications running in WCDC. [redacted]

In addition, as part of its plan to further improve its disaster recovery environment, the Carrier is creating and implementing a National Disaster Recovery policy along with an implementation plan by year end (2009) to address the recovery of [redacted] applications not addressed in the current disaster recovery program. This policy and plan will supplement existing efforts by addressing the recovery of [redacted] applications not covered in the current disaster recovery program. The implementation plan will contain a complete timeline and ensure that recovery plans align with business defined objectives. These objectives correspond to the Disaster Recovery (DR) Class of Service that appears on Table 1 below.

As an interim step, by year end 2009, the Carrier will select the DR Class of Service 1 [redacted], provide up-to-date DR plans for them and test them [redacted] The implementation plan to be provided with the national policy will include the roadmap to [redacted] provide recovery appropriate to the DR Class of Service assigned.

Because of the size of the current portfolio of applications, it is not feasible for the Carrier to test all of these annually. However, the Carrier expects to test all DR Class of Service 1 and 2 applications annually after they are migrated to the new national policy requirements. Lower classes of service will be tested on a less frequent basis. Testing criteria will be outlined in the national policy being developed.

The following chart (Table 1) shows the recovery time objectives, recovery point objectives, and recovery method for each DR Class of Service:

| Class of Service | Recovery Time Objective | Recovery Point Objective | Recovery Method |
|---|---|---|---|
| 0* | 0 hours | 0 hours | Continuous Availability |
| 1 | ≤4 hours | ≤ 2 hours | Advanced Recovery |
| 2 | ≤24 hours | ≤ 8 hours | |
| 3 | ≤72 hours | ≤ 48 hours | |
| 4 | ≤1 week | ≤ 72 hours | Standard Revocery |
| 5 | ≤2 weeks | Last Safe Offsite Backup | |
| 6 | ≤1 month | Last Safe Offsite Backup | |
| 7 | Best Effort | Best Effort | |
| 8 | No recovery | No Recovery | No Recovery |

**Table 1.**

[redacted] This will be outlined in the implementation timeline that supports the adoption of the new national policy on disaster recovery.

**2. The Carrier is also supplementing its current business continuity efforts in the departments reviewed in the audit.**

The rating workflow process utilizes applications on the Carrier's standard data storage and computers and therefore, will rely on the Carrier's overall IT disaster recovery plans. To supplement these plans, by the end of the Second Quarter 2009, the unit that supports these applications will document a business continuity plan to be triggered in the event of a disaster. The plan will cover:

1) A command center with a list of contact and telephone numbers in order of management hierarchy;
2) Staff procedures to be followed; and
3) A formal communication plan.

**Recommendations 10 and 11 (F. Application Controls; 1. Medical Edits for Professional Encounters, and 2. Non-covered Benefit):**

***With regard to the medical edits of professional encounters (Recommendation 10) and processing of non-covered services (Recommendation 11), the Carrier already has in***

***place several levels of controls to prevent errors, and already had plans to further supplement these efforts.***

The Draft Report found that, although the Carrier uses "a third party software package" to perform medical edits of internal hospital encounters, it does not use similar controls for its internal professional encounters. Draft Report, p. 14. It recommended that the Carrier modify its systems to implement these edits for internal professional encounters. Draft Report, p. 14.

In addition, the Draft Report found that, in the test environment, it was possible to process two internal encounters for non-covered services, with the cost of these services passed into the FEHBP's rates. It recommended that the Carrier implement "appropriate system modifications" to ensure that internal services not covered by FEHBP did not pass into the FEHBP's rates. Draft Report, p. 14.

However, the Carrier's internal delivery operations and its system are already designed to minimize risk and have established controls over how professional encounters are documented and captured. The nature of the Carrier's physician workflow and system functionality minimizes the risk of erroneous coding existing in the rating system data. As described during the onsite testing, because of the Carrier's unique arrangement with its contracted medical groups, individual physicians derive no direct financial benefit from the way a particular encounter is coded. In addition, three tools are built into the Carrier's clinical delivery application to drive a high level of consistency and accuracy:

1) [redacted] that suggest to the provider appropriate diagnoses and procedures for their specialty;
2) A decision tree based tool [redacted] that presents appropriate procedures based on the chief complaint from the patient; and
3) Best practice help guides or [redacted] for ordering appropriate procedures based on the patient's condition.

As with covered procedures, individual physicians have no direct financial incentive to inappropriately code services they provide. Although the existing rating data does not check benefit eligibility at a fine level of detail, benefit classes such as [redacted] are excluded in the rating data through benefit verification and exclusion logic in the rating data preparation and load process.

[redacted]

To test the extent to which erroneous coding and non-covered services exist in the Carrier's rating data, it reviewed claims data for the existence of those conditions tested during the auditors' on-site visit. The Carrier tested twelve (12) months of data (10/2007 - 9/2008) for a representative sample of our largest commercial customers, representing 14,450,107 member months. These tests revealed no (0) cases of a [redacted] performed on a [redacted]; no (0) cases of [redacted] in the same encounter; only three (3) cases of [redacted]during a

[redacted]; and no (0) cases of[redacted]in the [redacted] department. In addition, it tested twelve (12) months of paid claims data (10/2007 - 9/2008) for all members of the FEHBP, representing 2,147,696 member months, and found only 26 incidences of [redacted]

This review of actual data indicates that the prevalence of these situations and the associated costs are negligible. The few erroneous codes that appear in the data are statistically insignificant and do not affect a group's premium rate outcome. As part of its regular data validation process, the Carrier will monitor the data for these specific irregularities and if the results should change, it will determine if adjustments are necessary. [redacted]

Given the extremely low prevalence of these particular conditions in the existing data, the Carrier has determined that it is cost prohibitive to invest capital on any other interim solutions prior to [redacted]. Based on economic conditions, these plans may be subject to change.

**Recommendation 12 (F. Application Controls; 3. Emergency Room to Hospital Transfers):**

***Recommendation 12 concerning emergency room transfers correctly identified a situation in which the Carrier was undervaluing the cost of covered services provided to FEHBP members.***

The Draft Report found that Carrier's pricing system inadvertently undervalued by $50 the price assigned to services provided when an FEHBP member was transferred from the emergency room to the hospital. It recommended that the Carrier modify its systems to correct this issue. Draft Report, p. 15.

The Carrier understands that this situation may have resulted in a negligible undercharge to the FEHBP, and appreciates the opportunity to adjust its systems. Development of the detailed requirements is currently in process. System modifications are targeted to be developed, tested and in production by December 31, 2009.

**Recommendation 13 (F. Application Controls; 4. Pricing of Hospital Professional Services and Room and Board):**

***Recommendation 13, concerning the pricing of internal professional services and room and board, reflected a system error that existed only in the test environment.***

In testing the Carrier's controls for age/procedure inconsistency, the Draft Report acknowledged that a system "bug" caused the system to automatically re-classify a procedure as a non-covered service, inaccurately charge the member for room

and board, inaccurately price the non-covered procedure, and pass it to the FEHBP rating. The Draft Report recommended further research on this issue. Draft Report, p. 15.

The Carrier has researched this issue and found that this "bug" only appears when one of its source processing files is empty. This condition does not exist in normal production. It was a problem the Carrier subsequently identified with the FEHBP audit test data run in the test environment. The Carrier's current production validation process does account for this issue; therefore, the Carrier has determined that no further action is required.

## ***III. CONCLUSION***

We appreciate this opportunity to respond to the Draft Report, and urge OPM to give due consideration to the information provided in this letter.

This response contains commercial and financial information that is proprietary and confidential to the Carrier. Disclosure of this information would cause substantial harm to the Carrier's competitive position. OPM is requested to treat this document as confidential. This material is exempt from disclosure under Section 552(b)(4) of Title 5 of the United States Code.

Please do not hesitate to contact me if you have any questions or need any additional information. You can reach me at [redacted]. Thank you.

Sincerely,

[redacted]
Vice President, FEHBP Line of Business

cc: [redacted]
Chief, Insurance Group III
OPM Insurance Program Services