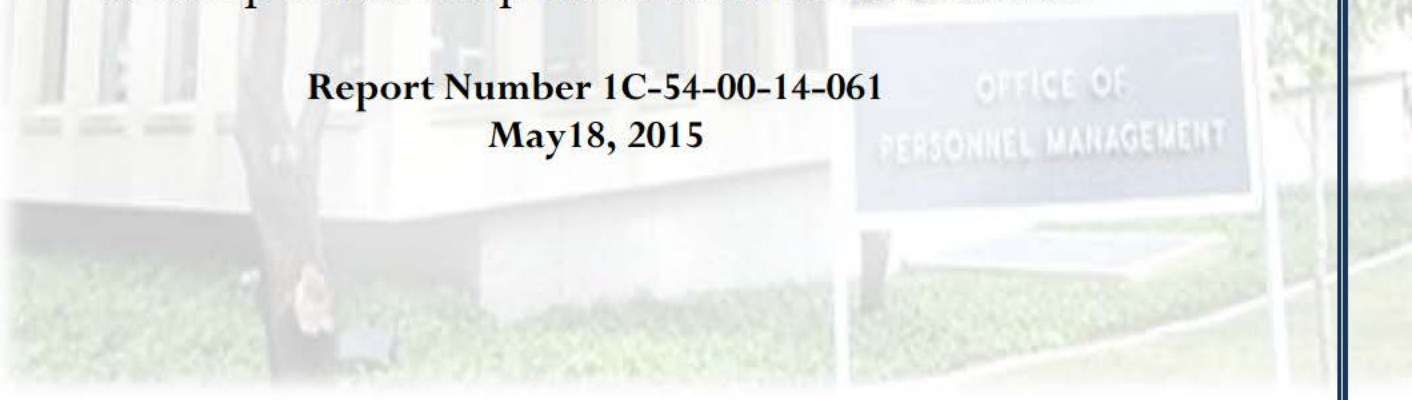
U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Audit of Information Systems General and Application Controls at Group Health Cooperative and KPS Health Plans

Report Number 1C-54-00-14-061
May18, 2015



-- CAUTION --

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Group Health Cooperative and KPS Health Plans

Report No 1C-54-00-14-061 **May 18, 2015**

Background

Group Health Cooperative (GHC) and KPS Health Plans (KPS) contract with the U.S. Office of Personnel Management (OPM) as part of the Federal Employees Health Benefits Program (FEHBP). KPS is a wholly owned subsidiary of GHC, and the companies share several IT resources and policies and procedures.

Why Did We Conduct the Audit?

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

What Did We Audit?

The scope of this audit centered on the information systems used by GHC and KPS to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit at GHC and KPS determined that:

- GHC has established an adequate security management program.
- GHC and KPS have implemented controls to prevent unauthorized logical access to its systems. However, we noted the following areas of concern related to GHC's physical access controls:
  - Physical access controls over general facility access could be improved, and
  - Physical access controls over data center access could be improved.
- We noted several areas of concern related to GHC's and KPS' network security controls:
  - A patch management policy is in place, but our test work indicated 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  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized;
  - Several servers were configured in an insecure manner; and
  - KPS does not have a formal firewall management policy.
- GHC has not developed formal configuration policies/baselines for all operating platforms used in its environment. Furthermore, GHC does not audit its configuration settings against documented baseline configurations.
- GHC's and KPS' business continuity and disaster recovery plans contain the key elements suggested by relevant guidance and publications.
- GHC has documented system development lifecycle procedures, however, the procedures are only guidelines and are not required for all system changes.
- GHC and KPS have implemented many controls in their claims adjudication processes to ensure that FEHBP claims are processed accurately. However, we noted several opportunities for improvement in GHC's and KPS' claims application controls.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
GHC	**Group Health Cooperative**
IT	**Information Technology**
HIO	**Healthcare and Insurance Office**
HIPAA	**Health Insurance Portability and Accountability Act**
KPS	**KPS Health Plans**
NIST	**National Institute of Standards and Technology**
SDLC	**System Development Life Cycle**
SP	**Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims by Group Health Cooperative (GHC) and KPS Health Plans (KPS).

The audit was conducted pursuant to FEHBP contracts CS 1043 and CS 1767; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

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

This was our first audit of GHC's and KPS' information technology (IT) general and application controls. We also reviewed GHC's and KPS' compliance with the Health Insurance Portability and Accountability Act (HIPAA). We chose to review these two distinct health plans in one audit because KPS is a wholly owned subsidiary of GHC, and the companies share several IT resources and policies and procedures.

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

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

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

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to GHC's and KPS' claims processing system; and
- HIPAA compliance.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of GHC's and KPS' internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of GHC's and KPS' internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by GHC and KPS to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. GHC claims are processed through a claims adjudication system managed internally by the organization. KPS licenses its claims application from a third party vendor, [redacted]. The business processes reviewed are primarily located in Tukwila and Bremerton, Washington.

The on-site portion of this audit was performed from October through November 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 GHC and KPS as of November 2014.

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

In conducting this audit we:

- Gathered documentation and conducted interviews;
- Reviewed GHC's and KPS' business structure and environment;
- Performed a risk assessment of GHC's and KPS' information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and,
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating GHC's and KPS' control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the CFR;
- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, 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, 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 GHC's and KPS' practices were consistent with applicable standards. While generally compliant, with respect to the items tested, GHC and KPS were not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

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

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

GHC has implemented a series of formal policies and procedures that comprise its security management program. The GHC Chief Information Security Officer is responsible for creating, reviewing, editing, and disseminating IT security policies. GHC has developed a thorough risk management methodology, and has procedures to document, track, and mitigate or accept identified risk. We also reviewed GHC's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that GHC 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 of GHC's and KPS' facilities and data centers. We also examined the logical controls protecting sensitive data on GHC's network environment and claims processing related applications.

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

- Procedures for appropriately granting, revoking, and routinely auditing physical access to secure areas;
- Procedures for granting, adjusting, and auditing user access; and
- Procedures for removing network and application access for terminated employees.

The following section documents opportunities for improvement related to GHC's physical access controls.

1. **Facility Access**

Most GHC facility entrances are protected by either a locked door requiring an access badge or a security guard stationed at the entrance. However, we observed [redacted] at various times during business hours. GHC also does [redacted] into its facilities ([redacted]).

FISCAM states that "Access to facilities should be limited to personnel having a legitimate need for access to perform their duties." Physical controls vary, but include: manual door or cipher key locks, magnetic door locks that require the use of electronic keycards, biometrics authentication, security guards, photo IDs, entry logs, and electronic and visual surveillance systems.

FISCAM also states that "By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software."

We did not observe any opportunities for improvement related to facility access at any KPS facilities.

Recommendation 1

We recommend that GHC reassess its facilities' physical access management and implement controls that will ensure proper physical security.

GHC Response:

"Procedural changes have been deployed to eliminate gaps in lobby coverage. Further enhancements are being planned and will be deployed by 5/1/2015 to assure the posted security has better visual access to ID badges when persons enter through GH lobby areas.

Policy and training currently conveys the expectation that [redacted]. Improvement to verbiage on the badge, access policy and related training is being developed and will be deployed by 5/1/2015 to reinforce the expectation that all persons utilize badges for secure buildings and spaces. This will create a policy violation for [redacted]

OIG Reply:

As part of the audit resolution process, we recommend that GHC provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this report that GHC and KPS agree to implement.

2. Access to Data Center

The GHC data center has electronic card readers to control physical access. However, we expect all FEHBP contractors to also have multi-factor authentication at data center entrances. GHC has stated that they are in the process of moving their primary data center from the office complex location in [redacted], Washington to another facility with improved controls. GHC should ensure that the new facility contains the following common access controls that we typically see at other FEHBP carrier facilities:

Physical access controls at GHC's data center could be improved.

- Multi-factor authentication to enter the computer room (e.g., pin code or biometric device in addition to an access card);
- [redacted] alarms to enter the computer room [redacted]

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to the GHC data centers and the sensitive IT resources and confidential data they contain. NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," provides guidance for adequately controlling physical access to information systems containing sensitive data.

We did not observe any opportunities for improvement related to facility access at the KPS data center.

Recommendation 2

We recommend that GHC reassess its data centers' physical access management and implement controls that will ensure proper physical security. At a minimum, GHC should implement multi-factor authentication at data center entrances.

GHC Response:

"Group Health is [redacted] to a new primary data center, provided by data center designer, owner and operator, [redacted]

[redacted]. [redacted] ***provides multiple levels of physical and logical security for Group Health's data center environment including:***

- On-site security personnel 24 hours per day, 7 days per week
- Secure perimeter security setbacks, berms and fencing with intrusion detection
- Secure access checkpoint
- CCTV throughout campus
- Mantraps at building entrance
- Biometrics

To gain access to the Group Health data servers in the new data center environment, [redacted]

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.

We evaluated GHC's and KPS' network security program and also independently performed several automated vulnerability scans and compliance audits performed on GHC and KPS/[redacted] operating platforms during this audit. We noted the following opportunities for improvement related to network security controls.

1. Vulnerabilities Identified in Scans

System Patching

GHC has documented vulnerability management policies and procedures that establish timeframes for remediating weaknesses. However, the results of our vulnerability scans indicate that all critical patches, service packs, and hot fixes are not implemented in a timely manner.

[redacted] also conducts periodic vulnerability scanning on the technical environment supporting KPS. However, the results of our vulnerability scans on this environment also indicate that all critical patches, service packs, and hot fixes are not 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 the Plan 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 information could be stolen.

Recommendation 3

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

GHC Response:

"Group Health has established a monthly vulnerability scanning process that looks for the existence of current software and patches per its baseline.

Group Health has revised the operating system patching process and schedule to ensure monthly scanning will detect all current patches in the month they are released from the vendor. Group Health has also revised the technology platform used to deploy updates, conforming to industry best practices for efficient, effective patch deployment, as well as reporting.

A comprehensive plan for remediating production systems will be completed and validated by scans scheduled for 06/01/2015."

Recommendation 4

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

KPS Response:

"[redacted] represents that all servers in this environment will be replaced and put on a regular monthly patch schedule by 4/30/15. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA."

Noncurrent software

The results of the vulnerability scans of GHC and KPS/[redacted] also indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 5

We recommend that GHC implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

GHC Response:

"Leveraging the monthly vulnerability scanning and other IT processes and tools, Group Health will develop a process to remediate out of date or no longer supported software on production [redacted] servers by 3/31/2015. Group Health will also create a Plan to remediate, complete with timeline and completion date by 06/30/2015. The final completion date will be delivered as a component of the implementation plan itself by 06/30/2015."

Recommendation 6

We recommend that KPS require [redacted] implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

KPS Response:

"[redacted] represents that all servers in this environment will be replaced and put on a regular monthly patch schedule by 4/30/15. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA."

Insecure Operating System Configuration

The results of the vulnerability scans also indicated that several GHC and [redacted] servers contained insecure configurations that could allow hackers or unprivileged users to [redacted]. We were subsequently provided evidence that GHC has since remediated this vulnerability.

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 7

We recommend that KPS require [redacted] to remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

KPS Response:

"All servers in this environment will be replaced and put on a regular monthly patch schedule by the 4/30/15 date. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA."

2. Firewall Management

[redacted] has implemented firewalls to help secure the network environment supporting KPS. However, a firewall configuration/hardening policy has not been developed. [redacted] also has procedures in place to document and track firewall changes. However, there is no routine review of firewall settings because there are no approved settings to which to compare the actual settings.

NIST SP 800-41 Revision 1 states that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. . . . The policy should also include specific guidance on how to address changes to the rule set."

Failure to implement a thorough firewall configuration policy and continuously manage the devices' settings increases the organization's exposure to insecure traffic and vulnerabilities.

We did not observe any opportunities for improvement related to GHC's firewall management methodology.

Recommendation 8

We recommend that KPS require that [redacted] document a formal firewall management policy.

KPS Response:

"[redacted] represents that it is revising its firewall management policies and will have an approved policy in place by 04/30/2015. [redacted] and [redacted] have both been installed with full automation expected to be completed by the end of 4/30/15. Once

automation is complete, [redacted] will be conducting full reviews at least twice per year to ensure compliance with the established policy."

Recommendation 9

We recommend that KPS require that [redacted] implement a process to conduct routine configuration reviews on its network firewalls to ensure performance and security optimization, as defined by the firewall management policy.

KPS Response:

KPS provided the same response as for recommendation 8.

D. Configuration Management

The GHC claims processing application is housed [redacted]. The system includes many supporting applications and system interfaces. Additional supporting applications are hosted in data centers owned and operated by GHC. We evaluated GHC's management of the configuration of these platforms and determined that the following controls were in place:

- Documented build standards and procedures; and
- Thorough change management procedures for system software.

KPS' claims processing system is hosted and maintained by [redacted]. The claims processing application is housed in a distributed server environment. We evaluated [redacted] configuration management of the claims processing system and determined that the following controls were in place:

- Documented configuration baselines; and
- Thorough change management procedures for system software.

The sections below document areas for improvement related to GHC's and [redacted]' configuration management controls.

1. Baseline Configurations

GHC has created build standards and procedures for deploying new servers and databases. However, during the fieldwork phase of this audit, GHC had not documented baseline configurations for all operating platforms used by the organization. A baseline configuration is a formally approved policy or standard outlining how to securely configure an operating platform. We were subsequently provided evidence that baseline policies are in the process of being created for several operating platforms using Center for Internet Security standards. We were told that full implementation of the baselines is scheduled for February 2015.

GHC has not documented 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.

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

[redacted] has documented adequate baseline configurations for the operating platforms supporting KPS.

Recommendation 10

We recommend that GHC document approved baseline configurations for all [redacted].

GHC Response:

"Group Health has incorporated baseline configuration standards into the new production [redacted] build image; such that all new production [redacted] builds adhere to the desired configuration outcome. In addition, all new production [redacted] are also built with [redacted] installed to help ensure the desired configuration state is maintained over time.

Existing production [redacted] will be brought into compliance of the baseline security configuration standards by September 31, 2015."

2. Configuration Compliance Auditing

As noted above, GHC does not maintain approved operating platform secure configuration baselines for its [redacted]. Therefore, GHC cannot effectively audit the system's security settings (i.e., there are no approved settings to which to compare the actual settings). We were told that GHC is in the process of implementing tools to assist with configuration compliance auditing on existing [redacted], which will be complete in February 2015.

[redacted] has created baseline configuration policies for its servers and databases that process claims data. However, it does not routinely audit its configurations to ensure compliance. [redacted] has recently completed the installation of two tools that will allow it to review system configurations. However, full automation of these tools is not planned until the first quarter of 2015.

NIST SP 800-53 Revision 4 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system.

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 11

We recommend that GHC routinely audit all server, database, and mainframe security configuration settings to ensure they are in compliance with approved baselines.

GHC Response:

"All new production [redacted] are currently built with [redacted] installed to help ensure the desired configuration state is maintained over time. All existing production [redacted] will be retrofitted with [redacted] by [redacted]."

Recommendation 12

We recommend that KPS require [redacted] to routinely audit all server and database security configuration settings to ensure they are in compliance with the approved baselines.

KPS Response:

"[redacted] represents that it is revising its configuration management policy and will have an approved policy in place by [redacted]. [redacted] and [redacted] have both been installed with full automation expected to be completed by the end of [redacted]. Once automation is complete, [redacted] will be conducting full reviews at least twice per year to ensure they comply with the established policy.

[redacted] continues with ongoing change management procedures with respect to evaluations and approval of all applicable configuration changes for specific devices."

E. Contingency Planning

We reviewed the following elements of GHC's and KPS' contingency planning programs to determine whether controls were in place to prevent or minimize interruptions to business operations when disastrous events occur:

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

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." GHC and KPS have identified and prioritized the systems and resources that are critical to business operations, and have developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that GHC or KPS have not implemented adequate controls related to contingency planning.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting the GHC and KPS claims adjudication process. The following sections address both the GHC claims system, [redacted], and the KPS claims system hosted by [redacted].

1. Application Configuration Management

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

KPS and [redacted] have documented system development life cycle (SDLC) procedures that IT personnel follow during routine software modifications. All changes require approval and undergo testing prior to migration to the production environment. We do not have any concerns regarding KPS' application configuration management process.

GHC has also implemented procedures related to application configuration management, and has adopted an SDLC methodology. However, these SDLC procedures are "guidelines" and are not required for all application changes. We were told that a new SDLC methodology will be implemented in the future that will specify certain required items for medium to large system implementations.

GHC's SDLC process is not enforced on all application changes.

NIST SP 800-53 Revision 4, states that an organization must manage the information systems using a system development life cycle that incorporates information security considerations. Failure to enforce the SDLC procedure for all application changes increases the risk that changes could be made that are not approved and not adequately tested. This could increase the risk that defective or malicious code could be introduced into the production environment without management's knowledge.

Recommendation 13

We recommend that GHC update its SDLC policy to require all application changes go through the documented SDLC process.

GHC Response:

"Group Health will update the Change Management Policy to require all updates to the application portfolio to follow the SDLC process. In addition, Group Health has updated the SDLC process and related reference and training materials.

Throughout 2015, system implementations will go through a more robust Phase Gate Review process, tracking/monitoring tools and instructions on what steps and artifacts of the SDLC are required based on the type of project and risk profile Group Health expect that these changes should be fully implemented by 12/31/2015."

2. Claims Processing System

We evaluated the input, processing, and output controls associated with the GHC and KPS claims processing systems. We determined that GHC and KPS have implemented policies and procedures to help ensure that:

- GHC paper claims that are received in the mail room are tracked to ensure timely processing;
- Claims are monitored as they are processed through the systems with real time tracking of the system's performance; and,
- Claims scheduled for payment are actually paid.

While on-site at the KPS facility in Bremerton, Washington, we observed that incoming mail was not logged before being transferred to another location for processing. Failure to log incoming mail increases the risk that claims or checks could get lost during shipment. We subsequently received evidence that KPS has since remediated the weakness by implementing mail logging procedures.

Nothing else came to our attention to indicate that GHC or KPS have not implemented adequate controls over its claims processing systems.

3. Enrollment

We evaluated GHC's and KPS' procedures for managing their databases of member enrollment data. Enrollment information is received electronically or in paper format and entered into the claims processing system. Enrollment transactions are audited weekly to ensure information is entered accurately. We do not have any concerns regarding GHC's or KPS' enrollment policies and procedures.

4. Debarment

GHC and KPS have adequate procedures for updating their claims processing systems with debarred provider information. GHC and KPS download the OPM OIG debarment list every

month and make the appropriate updates to the provider databases. Any claim submitted for a debarred provider is flagged by GHC and KPS to prevent claims submitted by that provider from being processed successfully during the claims adjudication processes.

Nothing came to our attention to indicate that GHC or KPS have not implemented adequate controls over the debarment process.

5. Application Controls Testing

We conducted tests on both GHC's and KPS' claims processing applications to validate the systems' claims adjudication controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which the systems processed and adjudicated the claims. The test results from GHC and KPS are documented separately below.

Group Health Cooperative

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

- Exact duplicate claims;
- Gender / Procedure inconsistency;
- Facility / Procedure inconsistency;
- Invalid place of service;
- Catastrophic maximum;
- Eligibility;
- Surgeon / Assistant surgeon;
- Coordination of benefits;
- Bundling charges; and
- Timely Filing.

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

a. Medical Editing

Our claims testing exercise identified several scenarios where the GHC claims processing 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:

- [redacted]

- [redacted]
- [redacted]

The examples outlined above merely represent a small number of medically inconsistent scenarios that could be detected by comprehensive medical edits in the system. It is not intended to be an all-inclusive list, and GHC's efforts to address this finding should be focused on a comprehensive medical edit solution.

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

Recommendation 14

We recommend that GHC implement comprehensive medical edits in its claims adjudication application.

GHC Response:

"Group Health is improving the adjudication process by implementing the following medical edit updates:

[redacted]
- [redacted]
- [redacted]

[redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]
- [redacted]

- [redacted]
- [redacted]

OIG Reply:

While the [redacted] process may detect and deny some forms of [redacted] inconsistencies, we believe that an [redacted] would increase the likelihood of detecting and suspending these types of claims from processing. Therefore we continue to recommend that GHC implement comprehensive medical edits in its claims adjudication application.

b. Patient History

Our claims testing exercise identified several scenarios where the GHC claims processing did not adequately compare current claims to a patient's historical claims. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the issue:

- [redacted]
  - [redacted]
- [redacted]
  - [redacted]
  - [redacted]

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 duplicate claims or member history inconsistencies increases the risk that fraudulent or erroneous claims are paid.

Recommendation 15

We recommend GHC ensure the appropriate system modifications to ensure that claims are compared against historical claims data to identify potential duplicates.

GHC Response:

"Group Health is improving the adjudication process by implementing the following system modifications:

[redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]

c. *Benefit Structure*

Our claims testing exercise identified a scenario where the GHC claims processing system failed to apply the FEHBP benefit structure correctly.

- Timely filing (Professional & Facility) – the GHC claims processing system is not appropriately following the timely filing limit outlined in the FEHBP brochure. According the brochure, claims must be submitted by December 31 of the year after the year you received the service. Currently, GHC only allows one year from the end of the date of service to submit a claim, while OPM allows until the end of the calendar year after the year of the date of service.

We received evidence after the fieldwork phase of the audit indicating that GHC has since resolved this issue. The filing limit has been updated so that for FEHB members the timely filing limit is extended until the end of the year following the year when services were provided.

KPS Health Plans

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

- Exact duplicate claims;
- Gender / Procedure inconsistency;
- Facility / Procedure inconsistency;
- Invalid place of service;
- Catastrophic maximum;

- Eligibility;
- Surgeon / Assistant surgeon;
- Coordination of benefits; and
- Bundling charges.

The following section documents opportunities for improvement related to KPS' claims application controls:

a. Medical Editing

Our claims testing exercise identified several scenarios where the KPS claims processing 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:

- [redacted]
- [redacted]
- [redacted]

The examples outlined above merely represent a small number of medically inconsistent scenarios that could be detected by comprehensive medical edits in the system. It is not intended to be an all-inclusive list, and KPS' efforts to address this finding should be focused on a comprehensive medical edit solution.

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

Recommendation 16

We recommend that KPS work with [redacted] to implement comprehensive medical edits in its claims adjudication application.

KPS Response:

"KPS and [redacted] are working to improve the adjudication process by implementing the following medical edit updates:

[redacted]

[redacted]

[redacted]

b. *Benefit Structure*

Our claims testing exercise identified scenarios where the KPS claims processing system failed to detect benefit structure inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- [redacted]
- Timely filing (Professional & Facility) – KPS' claims processing system is not appropriately following the timely filing limit. According the FEHBP brochure, claims must be submitted by December 31 of the year after the year you received the service. Currently, KPS is only allowing for one year from the end of the date of service to submit a claim; and
- [redacted]

Failure to ensure the claims processing system is correctly following the benefit structure increases the risk that claims are being incorrectly paid.

Recommendation 17

We recommend that KPS work with [redacted] to implement the appropriate system modifications to ensure that claims are being appropriately processed according to the benefit structure.

KPS Response:

"KPS is improving the adjudication process by implementing the following system modifications:

[redacted]

- [redacted]

Timely Filing (Professional and Facility)

- ***Due to the variables in the number of days for timely filing, KPS modified the system with a 365-day timely filing indicator and a new report to verify that claims to potentially be denied due to the timely filing limitation are in fact beyond the timely filing limit. This will be a pre-check-run report. KPS re-tested claims after the change in the timely filing criterion and results were as expected. Report is currently in development and expected completion date is 04/01/2015***

[redacted]

- [redacted]

c. Patient History

Our claims testing exercise identified several scenarios where the KPS claims processing did not adequately compare current claims to a patient's historical claims. For the following scenarios, a test claim was processed and paid without encountering any edits detecting the issue:

- [redacted]
  - [redacted]
  - [redacted]

Failure to detect patient history issues increases the risk that fraudulent or erroneous claims are paid.

Recommendation 18

We recommend that KPS work with [redacted] to ensure the appropriate system modifications are made to prevent claims with patient history issues from processing.

KPS Response:

"KPS is improving the adjudication process by implementing the following system modification:

[redacted]

- [redacted]

[redacted]

G. Health Insurance Portability and Accountability Act

We reviewed GHC's and KPS' efforts to maintain compliance with the security and privacy standards of HIPAA. GHC created and maintains the HIPAA policies and procedures that KPS enforces.

GHC has implemented a collection of IT security policies and procedures to address the requirements of the HIPAA security rule. GHC has also developed a series of privacy policies and procedures that address requirements of the HIPAA privacy rule. GHC reviews its HIPAA privacy and security policies annually and updates when necessary. The GHC legal office oversees all HIPAA activities, and publishes and maintains corporate policies. Privacy and security training is provided periodically to all employees.

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

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge
[redacted], IT Auditor
[redacted], IT Auditor
[redacted], IT Auditor

[redacted], Group Chief

GroupHealth®

Date: 03/30/2015

To: [redacted], U.S. Office of Personnel Management
From: Robert O'Brien, Executive Vice President; Health Plan Division, Group Health Cooperative and Jim Page, KPS President; KPS Health Plans

Re: GHC & KPS Health Plan IT General and Application Controls Audit 2014; findings and recommendations

This memorandum is provided in response to findings and recommendations noted on OIG's draft audit report issued on 01/29/2015. Group Health Cooperative and KPS have reviewed the OIG's findings and recommendations and provide the following response.

Recommendation 1 – Facility Access for GHC

We recommend that GHC reassess its facilities' physical access management and implement controls that will ensure proper physical security.

Comment: Procedural changes have been deployed to eliminate gaps in lobby coverage. Further enhancements are being planned and will be deployed by 5/1/2015 to assure the posted security has better visual access to ID badges when persons enter through GH lobby areas.

Policy and training currently conveys the expectation that [redacted]. Improvement to verbiage on the badge, access policy and related training is being developed and will be deployed by 5/1/2015 to reinforce the expectation that all persons utilize badges for secure buildings and spaces. This will create a policy violation for [redacted].

Recommendation 2 – Access to Data Center for GHC

We recommend that GHC reassess its data centers' physical access management and implement controls that will ensure proper physical security. At a minimum, GHC should implement multi-factor authentication at data center entrances.

Comment: Group Health is [redacted] to a new primary data center, provided by data center designer, owner and operator, [redacted]. [redacted] provides multiple levels of physical and logical security for Group Health's data center environment including:

- *On-site security personnel 24 hours per day, 7 days per week*
- *Secure perimeter security setbacks, berms and fencing with intrusion detection*
- *Secure access checkpoint*
- *CCTV throughout campus*
- *Mantraps at building entrance*
- *Biometrics*

To gain access to the Group Health data servers in the new data center environment, [redacted].

Recommendation 3 – Network Security – System Patching for GHC

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

Comment: Group Health has established a monthly vulnerability scanning process that looks for the existence of current software and patches per its baseline.

Group Health has revised the operating system patching process and schedule to ensure monthly scanning will detect all current patches in the month they are released from the vendor. Group Health has also revised the technology platform used to deploy updates, conforming to industry best practices for efficient, effective patch deployment, as well as reporting.

A comprehensive plan for remediating production systems will be completed and validated by scans scheduled for 06/01/2015.

Recommendation 4 – Network Security – System Patching for KPS

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

Comment: [redacted] represents that all servers in this environment will be replaced and put on a regular monthly patch schedule by 4/30/15. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA

Recommendation 5 – Network Security – Non-Current Software for GHC

We recommend that GHC implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

Comment: Leveraging the monthly vulnerability scanning and other IT processes and tools, Group Health will develop a process to remediate out of date or no longer supported software on production [redacted] servers by 3/31/2015. Group Health will also create a Plan to remediate, complete with timeline and completion date by 06/30/2015. The final completion date will be delivered as a component of the implementation plan itself by 06/30/2015.

Recommendation 6 – Network Security – Non-Current Software for KPS

We recommend that KPS require [redacted] implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

Comment: [redacted] represents that all servers in this environment will be replaced and put on a regular monthly patch schedule by the 4/30/15 date. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be

placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA

Recommendation 7 – Network Security – Insecure Operating System Configuration for KPS

We recommend that KPS require [redacted] to remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Comment: All servers in this environment will be replaced and put on a regular monthly patch schedule by the 4/30/15 date. [redacted] is completing a planned migration of all physical servers to [redacted] and bringing all [redacted] operating systems up to [redacted] and using [redacted] for automated patching on a regularly scheduled basis. All systems will then be placed on a lifecycle with plans to upgrade as soon as new OS/app versions are validated by QA

Recommendation 8 & 9 Network Security – Firewall Management for KPS

We recommend that KPS require that [redacted] to document a formal firewall management policy.

We recommend that KPS require that [redacted] implement a process to conduct routine configuration reviews on its network firewalls to ensure performance and security optimization, as defined by the firewall management policy.

Comment: [redacted] represents that it is revising its firewall management policies and will have an approved policy in place by 04/30/2015. [redacted] and [redacted] have both been installed with full automation expected to be completed by the end of 4/30/15. Once automation is complete, [redacted] will be conducting full reviews at least twice per year to ensure compliance with the established policy.

Recommendation 10 – Configuration Management – Baseline Configuration for GHC

We recommend that GHC document approved baseline configurations for all [redacted]

Comment: Group Health has incorporated baseline configuration standards into the new production [redacted] build image; such that all new production [redacted] builds adhere to the desired configuration outcome. In addition, all new production [redacted] are also built with [redacted] installed to help ensure the desired configuration state is maintained over time.

Existing production [redacted] will be brought into compliance of the baseline security configuration standards by September 31, 2015.

Recommendation 11 – Configuration Management – Configuration Compliance Auditing for GHC

We recommend that GHC routinely audit all server, database, and mainframe security configuration settings to ensure they are in compliance with approved baselines.

Comment: All new production [redacted] servers are currently built with [redacted] installed to help ensure the desired configuration state is maintained over time. All existing production [redacted] servers will be retrofitted with [redacted] by [redacted]

Recommendation 12 – Configuration Management – Configuration Compliance Auditing for KPS

We recommend that KPS require [redacted] to routinely audit all server and database security configuration settings to ensure they are in compliance with the approved baselines.

Comment: [redacted] represents that it is revising its configuration management policy and will have an approved policy in place by 4/30/15. [redacted] and [redacted] have both been installed with full automation expected to be completed by the end of 4/30/15. Once automation is complete, [redacted] will be conducting full reviews at least twice per year to ensure they comply with the established policy.

[redacted] continues with ongoing change management procedures with respect to evaluations and approval of all applicable configuration changes for specific devices.

Recommendation 13 – Application Configuration Management for GHC

We recommend that GHC update its SDLC policy to require all application changes go through the documented SDLC process.

Comment: Group Health will update the Change Management Policy to require all updates to the application portfolio to follow the SDLC process. In addition, Group Health has updated the SDLC process and related reference and training materials.

Throughout 2015, system implementations will go through a more robust Phase Gate Review process, tracking/monitoring tools and instructions on what steps and artifacts of the SDLC are required based on the type of project and risk profile Group Health expect that these changes should be fully implemented by 12/31/2015.

Recommendation 14 – Claims Adjudication – Medical Editing for GHC

We recommend that GHC implement comprehensive medical edits in its claims adjudication application.

Comment: Group Health is improving the adjudication process by implementing the following medical edit updates:

[redacted]

[redacted]

Recommendation 15 – Claims Adjudication – Patient History for GHC
We recommend GHC ensure the appropriate system modifications to ensure that claims are compared against historical claims data to identify potential duplicates.

Comment: Group Health is improving the adjudication process by implementing the following system modifications:

[redacted]

Recommendation 16 – Claims Adjudication – Medical Editing for KPS
We recommend that KPS work with [redacted] to implement comprehensive medical edits in its claims adjudication application.

Comment: KPS and [redacted] are working to improve the adjudication process by implementing the following medical edit updates:

[redacted]

[redacted]

Recommendation 17 – Claims Adjudication – Benefit Structure for KPS
We recommend that KPS work with [redacted] to implement the appropriate system modifications to ensure that claims are being appropriately processing according to benefit structure.

Comment: KPS is improving the adjudication process by implementing the following system modifications:

[redacted]

Timely Filing (Professional and Facility)

- *Due to the variables in the number of days for timely filing, KPS modified the system with a 365-day timely filing indicator and a new report to verify that claims to potentially be denied due to the timely filing limitation are in fact beyond the timely filing limit. This will be a pre-check-run report. KPS re-tested claims after the change in the timely filing criterion and results were as expected. Report is currently in development and expected completion date is 04/01/2015*

[redacted]

Recommendation 18 – Claims Adjudication – Patient History for KPS
We recommend that KPS work with [redacted] to ensure the appropriate system modifications are made to prevent claims with patient history issues from processing.

Comment: KPS is improving the adjudication process by implementing the following system modification:

Member History

- [redacted] *is configured to pend professional claims for the same scenario but not hospital claims. A request for a new pre-check run report to capture data prior to final adjudication of hospital claims for this type of scenario has been submitted to [redacted] with a completion date of 04/01/2015.*

If you have any questions or concerns, please let us know.

Robert O'Brien, Executive Vice President
Health Plan Division, Group Health Cooperative

Jim Page, KPS President
KPS Health Plans

Report Fraud, Waste, and Mismanagement

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

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

By Phone:

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

By Mail:

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