



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 THE  
GOVERNMENT EMPLOYEES HEALTH ASSOCIATION**

**Report No. 1B-31-00-11-066**

**Date: August 9, 2012**

**--CAUTION--**

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

## **Audit Report**

**FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM  
CONTRACT 1063  
THE GOVERNMENT EMPLOYEES HEALTH ASSOCIATION  
PLAN CODE 31  
LEE'S SUMMIT & INDEPENDENCE, MISSOURI**

**Report No. 1B-31-00-11-066**

**Date: August 9, 2012**



---

**Michael R. Esser  
Assistant Inspector General  
for Audits**

**--CAUTION--**

This audit report has been distributed to Federal and Non-Federal officials who are responsible for the administration of the audited contract. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

## **Executive Summary**

<p><b>FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM CONTRACT 1063 THE GOVERNMENT EMPLOYEES HEALTH ASSOCIATION PLAN CODE 31 LEE'S SUMMIT &amp; INDEPENDENCE, MISSOURI</b></p>
--

**Report No. 1B-31-00-11-066**

**Date: August 9, 2012**

This final report discusses the results of our audit of general and application controls over the information systems at the Government Employees Health Association (GEHA).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for GEHA, as well as the various processes and information technology (IT) systems used to support these applications. We also conducted a significant follow-up review of prior audit recommendations from our 2006 IT audit.

In 2006 a substantial number of recommendations were made that collectively identified a significant weakness in GEHA's management of IT security. GEHA lacked the critical policies and procedures necessary for an entity-wide security program. Furthermore, they did not have the appropriate resources, both tangible and personnel, to ensure the protection of member data and successful processing of FEHBP claims. During our follow-up review, we determined that these long standing weaknesses have not been addressed and prior audit recommendations had been prematurely closed by OPM. While the audit work conducted during this review showed very recent steps taken by GEHA management to develop an improved IT security program, currently there are significant weaknesses that still threaten the privacy and security of FEHBP

data and member PII. We documented controls in place and opportunities for improvement in each of the areas below.

### Security Management

GEHA has established a series of IT policies and procedures to create an awareness of IT security at the Plan. However, GEHA has not developed a Rules of Behavior agreement that all employees are required to sign.

### Access Controls

We found that GEHA has implemented numerous controls related to the process of granting physical access to its data center, as well as logical controls to encrypt sensitive information. However, we did note multiple opportunities for improvement related to GEHA's physical and logical access controls.

### Configuration Management

GEHA has developed formal policies and procedures providing guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes. However, we noted numerous weaknesses in GEHA's configuration management program. The weaknesses were severe enough to consider the program a significant deficiency in GEHA's ability to securely process sensitive FEHBP data.

### Contingency Planning

We reviewed GEHA's business continuity plans and concluded that they contained most of the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis. However, GEHA does not perform routine disaster recovery testing on its distributed server environment.

### Application Controls

GEHA has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we recommended that GEHA implement several system modifications to ensure that its claims processing systems adjudicate FEHBP claims in a manner consistent with the OPM contract and other regulations.

### Health Insurance Portability and Accountability Act (HIPAA)

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

# Contents

	<u>page</u>
Executive Summary .....	i
I. Introduction.....	1
Background.....	1
Objectives .....	1
Scope.....	2
Methodology.....	2
Compliance with Laws and Regulations.....	3
II. Audit Findings and Recommendations .....	4
A. Security Management .....	4
B. Access Controls.....	5
C. Configuration Management.....	13
D. Contingency Planning.....	18
E. Application Controls .....	20
F. Health Insurance Portability and Accountability Act.....	25
III. Major Contributors to This Report.....	26

Appendix: Government Employees Health Association's May 10, 2012 response to the draft audit report issued March 14, 2012.

## **I. Introduction**

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims at the Government Employees Health Association (GEHA).

The audit was conducted pursuant to FEHBP contract 1063; 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 last OIG audit of general and application controls at GEHA occurred in 2006. While the audit was closed in 2006 by the audit resolution group in OPM's Healthcare and Insurance Office, we did a full review of all recommendations from the 2006 audit. We determined that several recommendations were inappropriately closed and that numerous weaknesses were not remediated until after 2009. Several recommendations should still be open and have been rolled forward within this report.

The business processes related to the scope of this audit are primarily located at GEHA's Lee's Summit and Independence, Missouri facilities. GEHA has two data centers supporting FEHBP processes in the greater Kansas City, Missouri area. Employees responsible for processing FEHBP claims are predominantly located in Independence, Missouri. The majority of claim output is printed and mailed at a contractor facility in St. Louis, Missouri. Several PPO contractor networks are also utilized to perform functions related to both claims input and output.

All GEHA 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 GEHA's information technology (IT) environment.

These objectives were accomplished by reviewing the following areas:

- Security management;
- Access controls;
- Segregation of duties;
- Configuration management;
- Contingency planning;
- Application controls specific to GEHA's claims processing systems; and,
- HIPAA compliance.

## **Scope**

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, the OIG obtained an understanding of GEHA's 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 GEHA's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The OIG evaluated the confidentiality, integrity, and availability of GEHA's computer-based information systems used to process FEHBP claims, 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.

The scope of this audit centered on the [REDACTED] claims processing system (and the IT environment that supports it) used by GEHA to process FEHBP claims.

In conducting our audit, we relied to varying degrees on computer-generated data provided by GEHA. 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 audit was performed at GEHA offices in Lee's Summit, Missouri, and Independence, Missouri. These on-site activities were performed in September and October 2011. The OIG completed additional audit work before and after the on-site visits at OPM's 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 GEHA as of December 15, 2011.

## **Methodology**

In conducting this review the OIG:

- Gathered documentation and conducted interviews;
- Reviewed GEHA's business structure and environment;

- Performed a risk assessment of GEHA’s information systems environment and applications, and prepared an audit program based on the assessment and the Government Accountability Office’s (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, the auditors used judgmental sampling in completing their compliance testing.

Various laws, regulations, and industry standards were used as a guide in evaluating GEHA’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;
- 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 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 3, 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 GEHA’s practices were consistent with applicable standards. While generally compliant, with respect to the items tested, GEHA was not in complete compliance with all standards as described in the “Audit Findings and Recommendations” section of this report.



## **II. Audit Findings and Recommendations**

### **A. Security Management**

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

GEHA has implemented a series of formal policies and procedures that comprise a comprehensive security management program. GEHA's security management program is led by the company's IT professionals whose responsibilities include creating policies to protect against threats or improper use of sensitive data and HIPAA compliance. All policies and procedures are approved by an executive committee before they are published and posted on the company intranet. GEHA has also developed a thorough risk management methodology, and has procedures to document, track, and alleviate or accept identified risks.

We also reviewed GEHA's human resources policies and procedures related to hiring, training, transferring, and terminating employees. However, we found that GEHA has not developed a rules of behavior agreement for information and information system usage.

NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems (NIST SP 800-53) states that "The organization: Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system."

Without clearly defining their rules of behavior the organization increases the risk of employees sharing account access information, downloading malicious software, sharing personally identifiable information, and general improper use of information systems.

#### **Recommendation 1**

We recommend GEHA develop a rules of behavior agreement and require all employees to sign the document.

#### **GEHA Response:**

***"GEHA has an extensive orientation process where new hires are trained on various policies and procedures and are required to sign Acknowledgement of Responsibility forms. These acknowledgements encompass what one rules of behavior document would address."***

#### **OIG Reply:**

We have received evidence that this recommendation has been implemented; no further action is required.

## **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 GEHA's data centers, the Independence claims processing facility, and two Lee's Summit office buildings. We also examined the logical controls protecting sensitive data on GEHA's network environment and claims processing related applications.

In addition, we conducted a network topology scan to verify that all known assets were included within GEHA's system inventory list.

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

- Procedures for appropriately granting physical access to facilities and data centers;
- Procedures for revoking access to data centers for terminated employees;
- Procedures for removing [REDACTED] network access for terminated employees; and,
- Controls to monitor and filter email and Internet activity.

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

### **1. Facility Physical Access Controls**

The physical access controls at GEHA's facilities could be improved.

All of the facilities we visited utilize some form of [REDACTED] to control access to the building during off-peak working hours. [REDACTED] during working hours. GEHA has a receptionist at each facility, but does not [REDACTED].

GEHA does not have any access controls to prevent [REDACTED]. [REDACTED] Employees are required to [REDACTED] but there are no physical controls in place to ensure that every individual follows this procedure.

We expect all FEHBP contractors to, at a minimum, have card reader controlled turnstile gates at facility entrances and multi-factor authentication at data center entrances (e.g., cipher lock or biometric device in addition to an access card). In addition to implementing [REDACTED], GEHA should analyze the benefit of implementing the common physical access controls listed below that we typically see at other FEHBP carrier facilities.

#### **Common Data Center Controls**

- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Common Office Building Controls

- [REDACTED], and
- [REDACTED]

FISCAM states that “Controls should accommodate employees who work at the entity’s facilities on an everyday basis; occasional visitors, such as employees of another entity facility or maintenance people; and infrequent or unexpected visitors. Physical security 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.”

In addition, NIST SP 800-53 provides guidance for adequately controlling physical access to information systems containing sensitive data (see control PE-3, Physical Access Control).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to GEHA facilities and the sensitive IT resources and confidential data they contain.

**Recommendation 2**

We recommend that GEHA reassess its facilities’ physical access management and implement controls that will ensure proper physical security. At a minimum, GEHA should implement [REDACTED] multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at data center entrances.

**GEHA Response:**

*“GEHA is currently reassessing facilities access at all of our locations and adding the following controls to increase physical security.*

1. [REDACTED] ...
2. ***Data Center – Multi-Factor Authentication at Entrance (COMPLETED) ...***
3. [REDACTED] ...
4. [REDACTED] ...
5. [REDACTED] ...”

**OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s Healthcare and Insurance Office (HIO) with evidence that it has fully implemented each of the changes to the physical security discussed in its response.

**2. Claim Storage Access Controls**

Paper claims containing sensitive information are stored [REDACTED]. However, GEHA does not separate access to [REDACTED]. The claims storage area is locked during non-business hours, but during the day there are no physical controls to separate the two areas.

FISCAM states that “Many of the control techniques for interior security are similar to those for perimeter and entry security (for example, locks, surveillance systems, as well as using and controlling badges, ID cards, smartcards, passkey, and other entry devices).”

Failure to restrict access to the claims storage area increases the risk that unauthorized employees can gain access to sensitive data contained within the room.

In addition, GEHA does not currently have a process in place to monitor claims file access. There is no employee stationed within this area and claim files can be removed for referencing. GEHA was unable to produce a claims file access log.

NIST SP 800-53 states that “The organization . . . Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk . . . .”

Failure to monitor and track access to claim files increases the risk that employees may manipulate, damage, or lose the claims.

**Recommendation 3**

We recommend that GEHA implement physical controls to prevent employees that only require access to the [REDACTED].

**GEHA Response:**

*“GEHA continues to keep this area locked during non-business hours and corrected this concern in October 2011 by installing a latching system on the inside of the storage area that prevents unsupervised access.”*

**OIG Reply:**

The intent of this recommendation is to ensure that claims are stored securely at all times, not just during non-business hours. As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with evidence that the claims are securely stored, preventing unauthorized access to claim files at all times.

#### **Recommendation 4**

We recommend that GEHA implement a process to monitor and track access to claim files.

#### **GEHA Response:**

*“The area where the claims are kept is separated from the [REDACTED] by a locked door. Access to this area is restricted to a limited number of claims clerical staff. There are no sign out procedures because claims leave this area only to be copied and immediately returned to the locked room.”*

#### **OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with the policy detailing the requirement to photocopy and immediately return claims to storage. Please also provide HIO with the policy which instructs GEHA employees to properly dispose of the claim form copies that contain PII.

### **3. Logical Access Controls**

When employees are terminated, GEHA’s policy is to remove their accounts from the [REDACTED] claims adjudication application.

We compared a list of recently terminated employees to the active [REDACTED] user list. We discovered that 20 terminated employees still had active accounts on [REDACTED] and that several of those employees had multiple active accounts.

Most of these individuals were terminated prior to 2010. Although GEHA’s current process appears to adequately remove [REDACTED] access for recently terminated users, it appears that there has never been an audit of old accounts to identify terminated users.

FISCAM states that “Inactive accounts and accounts for terminated individuals should be disabled or removed in a timely manner.”

#### **Recommendation 5**

We recommend GEHA conduct a detailed access review audit of [REDACTED] user accounts to identify accounts with inappropriate access.

#### **GEHA Response:**

*“GEHA Security Operations has taken multiple steps to better control [REDACTED] access. We have reviewed access for users with administrative access and have removed access that was inappropriate or no longer needed. To better establish and control access, we have developed a series of user templates that determine access by position. In doing so we have consulted with managers to verify access and remove any unneeded access. We have developed reporting from our payroll department that will allow us to better track users as they move within the organization or terminate. We have reviewed all previously terminated users to assure that all access has been removed. For auditing purposes it is necessary to leave IDs for terminated employees in place, however, all access to the ID is*

*removed, the account is locked, and the associated [REDACTED] user id is removed. This activity has been completed.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with:

- Samples of the user templates that determine access by position;
- Samples of the reports generated from the payroll department to track transferred and terminated employees;
- Evidence of the access review that took place to ensure terminated user access was appropriately removed; and,
- Evidence of the ongoing logical access auditing for a period of six months.

**4. Incident Response and Intrusion Detection**

GEHA has documented incident response procedures and has installed an intrusion detection system. However, the intrusion detection system has not been configured to optimize its security features. GEHA has recently installed next generation firewalls and monitoring software that has the ability to prevent and detect intrusions, however it is not configured for the GEHA environment. According to GEHA, a contractor will be going on-site in the near future to assist in configuring the tools and training employees.

FISCAM states that control techniques for an effective incident response program include “a means of prompt centralized reporting; active monitoring of alerts and advisories; [and] response team members with the necessary knowledge, skills, and abilities . . . .”

Failure to properly configure incident response and intrusion detection tools could allow incidents and intrusions to go unmonitored and unresolved. This could lead to a loss of sensitive resources.

**Recommendation 6**

We recommend that GEHA configure its intrusion detection tools to optimize their capabilities.

**GEHA Response:**

*“GEHA uses a [REDACTED] firewall that includes intrusion detection capabilities. The intrusion detection capabilities were recently activated and are being monitored to determine effectiveness in detecting known attacks. [REDACTED] are updated regularly to assure that detection capabilities are current. The Security Operations team will assist the Enterprise Architecture team in fine-tuning the detection capabilities as monitoring reveals changes that can be made to improve the system’s response. [REDACTED] [REDACTED]”*

**5. Remote Access Authentication**

GEHA does not require [REDACTED] to access its network from a remote location. Employees are required to use their [REDACTED] to remotely

authenticate to GEHA's network. [REDACTED] consist of a [REDACTED] [REDACTED]. GEHA plans to implement [REDACTED] in the future by requiring the [REDACTED]

NIST SP 800-53 Revision 3 states that information systems should use multifactor authentication for local and network access to privileged and non-privileged accounts.

Failure to implement adequate authentication controls increases the risk that unauthorized individuals can gain access to sensitive resources and confidential data.

### **Recommendation 7**

We recommend that GEHA implement [REDACTED].

#### **GEHA Response:**

*"GEHA has taken steps to purchase and implement [REDACTED] for remote access users. Remote web access to GEHA resources forces [REDACTED] to GEHA's [REDACTED] environment using [REDACTED] and [REDACTED]. This project has been completed for all users with remote access."*

#### **OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM's HIO with evidence when the [REDACTED] implementation is complete and [REDACTED] is required for all remote access users.

## **6. Segregation of Duties**

GEHA does not enforce proper segregation of duties on its major applications. Currently, only one major application is monitored for proper segregation of duties. Furthermore, the process for monitoring segregation of duties is not documented.

FISCAM states that "Work responsibilities should be segregated so that one individual does not control critical stages of a process." FISCAM also states that "Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions."

Failure to implement adequate proper segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, or that computer resources could be damaged or destroyed.

### **Recommendation 8**

We recommend that GEHA document a process for ensuring application access is granted with proper segregation of duties and implement the process for all major applications.

**GEHA Response:**

*“GEHA has taken steps to identify duties within the claims processing area and has defined those activities that present a potential violation of the segregation of duties. [REDACTED] access has been reviewed and conflicting access removed. Other applications have initially been configured to reduce conflicts, but currently need to be reviewed and any conflicts removed. Expected completion of this activity is by the end of the fourth quarter of 2012.*

*“GEHA’s Internal Audit Department performs an annual audit of access rights on major applications for employees who have terminated or transferred positions.”*

**7. Logical Access Privileges Approval and Review**

GEHA does not routinely recertify that employee application access is appropriate for all major applications. Currently, only one application is subject to a full access recertification review by the system owners. GEHA’s Internal Audit Group does perform periodic application access reviews, but the review includes only a small sample of employees.

FISCAM states that “The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which they are responsible . . . . The owner should identify the nature and extent of access to each resource that is available to each user. [This includes the following types of access: read, update, delete, merge, and execute] Access may be permitted at the file, record, or field level. . . . Owners should periodically review access authorization listings and determine whether they remain appropriate. Access authorizations should be documented on standard forms and maintained on file.”

Failure to routinely recertify the appropriateness of application access could allow employees to perform functions or access sensitive information that they should not have approval to access.

**Recommendation 9**

We recommend that GEHA expand the access recertification process to all major applications.

**GEHA Response:**

*“The GEHA Security Operations team is in the process of working with managers to develop role based access templates for [REDACTED] and major applications. During the process we are aligning current access of individuals to templates created for the role or job title they hold. Managers are reviewing access changes to align with templates created. Going forward the Security Operations team will use this application reports and templates to verify with management the access of all employees at least annually.”*



## 8. Application Access Monitoring

GEHA does not adequately monitor user access to its applications. Weekly access violation reports are emailed to management, but the reports are not reviewed. GEHA is in the process of creating an Information Security Group that will take over security monitoring responsibilities for the entire company, including the review of access violation reports. Furthermore, GEHA does not monitor user activity within the claims processing application.

FISCAM states that “Audit and monitoring involves the regular collection, review, and analysis of indications of inappropriate or unauthorized access to the application.” Management should monitor access within the application (i.e., unauthorized access attempts, unusual activity, etc.).

Failure to monitor activity logs and violation reports could allow attempts to gain unauthorized access to sensitive computer resources to continue unnoticed.

### **Recommendation 10**

We recommend that GEHA implement a process to log and review user access to and activity within its applications.

### **GEHA Response:**

*“The Security Operations team has developed a daily process to review [REDACTED] violation reports. [REDACTED] Violation reports for [REDACTED]s and other applications are not available at this time. [REDACTED] reports are reviewed, users are contacted to respond to violations, and notations are made electronically on the report pdf file. The file is stored along with related correspondence. This process is currently implemented.”*

### **OIG Reply:**

The intent of this recommendation was not to simply monitor log-on violations at the [REDACTED] but also to audit user transactions within the claims processing system. As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with evidence of a solution to monitor the claims processing system’s user activity.

## 9. Claims Processing System Password Modification

GEHA uses a [REDACTED] when creating all new [REDACTED] user accounts or resetting the password of existing accounts. While GEHA requires that the temporary password be changed after the first login attempt, this is not a sufficient compensating control. The process for establishing and changing passwords for the claims processing system is less secure than other major applications at GEHA. For other applications, an email is automatically sent to the user with a randomly generated temporary password that they use to establish new accounts or unlock existing ones.

NIST SP 800-118 (draft) states that “Randomly generated or arbitrarily chosen [one time passwords], not default or patterned passwords (e.g., “NIST0722”), should be used during

account creation and password reset processes. This ensures that if the user does not promptly change the assigned password, that the password will not be easily guessable.”

Failure to use randomly generated temporary passwords increases the risk that a person could gain unauthorized access to the claims processing system by exploiting the default password.

### **Recommendation 11**

We recommend that GEHA program the new claims processing system to use randomly generated temporary passwords for users who need to establish new accounts and users who lock themselves out of the system. The passwords should be automatically emailed to the user requesting access.

### **GEHA Response:**

*“The Security Operations team will review current practices for creating [REDACTED] IDs and modify that process as necessary adding steps to require interaction with the Help Desk before a user id is activated for first use. The new claims system uses authentication based on [REDACTED] where users will automatically authenticate to [REDACTED] as they activate the application client. [REDACTED] password management will be reviewed and changes made as necessary to randomize initial passwords. A password self-service tool will be investigated to see if they provide a more secure method for changing initial or forgotten passwords. Changes to processes will be completed by the fourth quarter of 2012.”*

## **C. Configuration Management**

[REDACTED] is housed in a [REDACTED] with the [REDACTED] and access control managed by [REDACTED]. Additional applications supporting the claims adjudication process are housed in a [REDACTED] with the [REDACTED]. We evaluated GEHA’s management of this system software and have serious concerns regarding its overall configuration management program.

The sections below document areas for improvement related to GEHA’s configuration management controls. We believe that the severity of the weaknesses related to configuration management represents a significant deficiency in GEHA’s ability to securely process FEHBP data in its IT environment.

### **1. Baseline Configurations**

GEHA has not documented a secure baseline configuration for its servers or mainframe. New system software is currently configured using employees’ collective knowledge of best practices. However, no standard configuration documentation has been created for any system software used by the organization. In December 2011, GEHA created a Baseline Server Configuration and Maintenance Plan that details the new process for creating configuration baselines for three server operating systems. The actual baseline documents are scheduled for completion in 2012.

FISCAM states that “The entity should maintain current configuration information in a formal configuration baseline that contains the configuration information formally designated at a specific time during a product’s or product component’s life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. There should be a current and comprehensive baseline inventory of hardware, software, and firmware, and it should be routinely validated for accuracy.”

Failure to create baseline configurations increases the likelihood that newly implemented or modified hardware, software, and firmware will not be securely configured.

### **Recommendation 12**

We recommend that GEHA formally document baseline configurations for its hardware, software, and firmware.

#### **GEHA Response:**

*“GEHA is addressing secure baseline configuration in a three-phase approach. Each phase will document the system function, inventory, configurations and security hardening requirements. For the initial phase, GEHA is focusing on [REDACTED]*

*[REDACTED] The second phase will extend into higher levels of the architecture including but not limited to [REDACTED]. The final phase will be a granular view of the business applications that utilize the architecture detailed in the first two phases such as [REDACTED]*

## **2. Monitoring System Administrator Activity**

GEHA’s management does not monitor system administrator activity. GEHA currently employs two [REDACTED] administrators that have the authority to control security for the entire system. [REDACTED] has a reporting capability that documents any changes that the administrators make to the system. However, these reports are not currently reviewed.

NIST SP 800-53 Revision 3 requires that “The organization . . . Tracks and monitors privileged role assignments. . . Privileged roles include, for example, key management, network and system administration, database administration, [and] web administration.”

Failure to document and track system administrator activity could allow unintended or malicious events to go undetected and increase system vulnerability.

### **Recommendation 13**

We recommend that GEHA implement a process to routinely monitor system administrator activity.

**GEHA Response:**

*“The Security Operations team has developed a daily process to review [REDACTED] administrator activity reports. The [REDACTED] reports are reviewed, users are contacted to respond to questionable activities, and notations are made electronically on the report pdf file. The file is stored along with related correspondence. The new claims processing system will require different tools to track administrative access because access will primarily be controlled through [REDACTED]. It may be possible to track administrative access within the new application but that is unknown at this time. A tool is being investigated that will track user data view and that tool may provide additional visibility within the new claims application. [REDACTED] administrator activity monitoring is currently implemented.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with samples of the reports generated to monitor [REDACTED] administrator activity as well as evidence of the review to routinely monitor system administrator activity.

**3. Configuration Auditing**

GEHA performs configuration audits of its [REDACTED] servers. However, they do not adequately use the results of the audits to enhance system security. The results of the audits revealed numerous configuration settings that were below industry standards. To confirm these results, we used an automated tool to conduct a compliance audit on over 150 production servers to determine if configuration settings were in compliance with HIPAA and industry standards. The results of the scan revealed major compliance issues in each server (the results of the scan were provided to GEHA but will not be detailed in this report due to the sensitive nature of the information).

FISCAM states “Current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. . . . Monitoring, sometimes called configuration audits, should be periodically conducted to determine the extent to which the actual configuration item reflects the required physical and functional characteristics originally specified by requirements.”

Failure to analyze the results of configuration audits and appropriately adjust software settings increases the risk of improper and less secure system software configuration.

**Recommendation 14**

We recommend that GEHA address the issues detected by the compliance audit and routinely monitor system software configuration to ensure compliance with established baselines.

**GEHA Response:**

*“The recent purchase of a security vulnerability scanning tool by the Security Operations team gives us the ability to scan configuration settings of individual [REDACTED] servers once*

*authenticated to the server. Security Operations will work with the Enterprise Architecture to assure that appropriate settings are routinely scanned and addressed. This recommendation should be completed by the end of the fourth quarter of 2012.”*

#### 4. Vulnerability Scanning and [REDACTED]

GEHA does not perform routine vulnerability scanning of its computer servers. We used an automated tool to conduct a vulnerability scan of GEHA’s server environment to determine if its servers were properly secured. We discovered numerous weaknesses related to [REDACTED] [REDACTED] (the results of the scan were provided to GEHA but will not be detailed in this report due to the sensitive nature of the information). GEHA has documented [REDACTED] procedures, but they are not being enforced.

We used another automated tool to conduct [REDACTED] scans on GEHA’s [REDACTED]. The [REDACTED] scan did not product any negative results. The [REDACTED] was terminated prematurely because it caused a disruption to GEHA’s production environment. However, the limited results that were returned from this scan indicated that the [REDACTED] may be vulnerable to [REDACTED]s (the results of the scan were provided to GEHA but will not be detailed in this report due to the sensitive nature of the information). We believe that the extent of the security weaknesses could be better evaluated by a third party company that specializes in [REDACTED].

FISCAM states that “Software should be scanned and updated frequently to guard against known vulnerabilities.” NIST SP 800-53 Revision 3 states “The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously.”

Failure to promptly install [REDACTED] increases the risk that vulnerabilities will not be remediated and unauthorized users could gain access to the system. Furthermore, the weakness within the [REDACTED] could be compromised, allowing unauthorized users access to PII.

#### **Recommendation 15**

We recommend that GEHA implement a process to conduct routine vulnerability scans and track any identified weaknesses until they are remediated.

#### **GEHA Response:**

*“A product to scan systems for vulnerabilities has recently been purchased and a project has been created to develop processes for scanning, notification of findings, risk assessment, remediation, and review. The project will focus on reducing the risk to the organization by implementing a routine vulnerability monitoring and remediation*

*program. This recommendation should be completed by the end of the fourth quarter of 2012.”*

**Recommendation 16**

We recommend that GEHA install the [REDACTED] that were identified in the scan results and, in the future, improve the patch management process to ensure that [REDACTED] are installed promptly.

**GEHA Response:**

*“GEHA recognizes the need and importance of developing and implementing a [REDACTED] to identify [REDACTED]s, determine applicability to GEHA systems, and distribute and implement on GEHA systems to prevent and minimize the risk of security breaches and losses. GEHA is initiating a formal [REDACTED] program to mitigate the risk presented by the [REDACTED]. The program will be a combination of technology in the form of [REDACTED] and deployment software and processes to identify, test and deploy software updates following a risk-based management approach. . . .”*

**Recommendation 17**

We recommend that GEHA contract with a third party vendor that specializes in [REDACTED] vulnerability assessments to conduct a thorough [REDACTED] vulnerability assessment of its [REDACTED].

**GEHA Response:**

*“GEHA is addressing [REDACTED] in two different ways. In late 2012, we engaged a third-party, [REDACTED] to conduct a comprehensive [REDACTED] assessment and [REDACTED]. The scope of the assessment included our [REDACTED]. Our IT and Security teams are actively remediating issues noted in that assessment. In addition, GEHA is currently redesigning our [REDACTED] and Security teams are involved in those discussions to ensure that any open vulnerabilities or concerns are addressed in the new design.*

*The second way we are addressing this issue is the purchase and implementation of [REDACTED]. Our Information Security Analysts have installed this solution and are currently conducting configuring and testing. This tool will be used on a continuous basis to assist security in identifying vulnerabilities affecting our infrastructure and will assist in the risk ranking of those vulnerabilities to drive remediation priorities. The solution will have the ability to not only alert security staff to vulnerabilities facing our [REDACTED], but also vulnerabilities on our [REDACTED]. We expect to have [REDACTED] deployed in our production environment and identifying vulnerabilities by Q3 of 2012.*

*We feel that it is important and we plan to continue engaging a third party to conduct an independent assessment, however due to the addition of our [REDACTED] tool and*

*vulnerability management processes, we will be reducing the frequency of those from annually to perhaps every other year.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with the following evidence: the [REDACTED] vulnerability assessment and penetration test results, evidence of the tracking and remediation of weaknesses, evidence of the implementation of [REDACTED] and the functionality of the tool.

**5. Updating System Software**

GEHA is currently running a version of [REDACTED], that is not supported by the vendor. GEHA has begun the process of upgrading to a supported operating system, but the upgrade is not complete.

FISCAM states that “Software should be scanned and updated frequently to guard against known vulnerabilities. In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats. Also, software releases should be adequately controlled to prevent the use of noncurrent software. . . . 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 use an operating system that is supported by the vendor increases the risk that the operating system contains vulnerabilities that cannot be fixed or patched.

**Recommendation 18**

We recommend that GEHA continue its efforts to upgrade the [REDACTED] operating system to a vendor-supported version.

**GEHA Response:**

*“GEHA is continuing the efforts to update the [REDACTED] me operating systems to vendor supported versions. We are working through the [REDACTED] and custom-developed application dependencies which require update before the [REDACTED] e operating systems can be updated. GEHA has also had to procure and implement a new [REDACTED] storage subsystem to allow for the increased capacity needs for the testing environments for process and inter-operability testing.”*

**D. Contingency Planning**

We reviewed GEHA’s service continuity program to determine whether controls were in place to prevent or minimize damage and interruptions to business operations when disastrous events occur.

We evaluated GEHA's contingency planning documentation to determine whether it outlined procedures for maintaining critical services for its members should business operations be disrupted. The following elements of GEHA's contingency planning program were reviewed:

- Business continuity plans for several major business units including claims, telecommunications/customer service, and check printing;
- Disaster recovery plan for the [REDACTED] claims processing system;
- Disaster recovery tests conducted in conjunction with an [REDACTED] recovery site; and,
- Emergency response procedures and training.

We determined that critical elements suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems," were addressed in the service continuity documentation reviewed. GEHA has identified which systems and resources are critical to business operations and how to recover those systems and resources.

GEHA does not perform a complete disaster recovery test for all systems. We were provided evidence that GEHA routinely performs a disaster recovery test of the [REDACTED] at the recovery site. However, we learned that there is no routine testing of the [REDACTED] environment. While the claims processing system resides on the [REDACTED], the [REDACTED] environment supports other critical GEHA applications.

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

Failure to perform annual disaster recovery tests on the [REDACTED] decreases the likelihood that GEHA will be able to completely restore operations in the event of a disaster.

### **Recommendation 19**

We recommend that GEHA conduct and document an annual disaster recovery test for the [REDACTED].

#### **GEHA Response:**

*"GEHA has designed and implemented a secured off-site co-location facility that will function as the disaster recovery site for all [REDACTED] GEHA is currently replicating all [REDACTED] data to the site through the use of the [REDACTED] data protection platform.*

*GEHA is scheduled to perform disaster recovery testing in Q3 of 2012. We have hired a Manager of Enterprise Risk that will be responsible for working with IT to maintain/update our BCP/DR plans to reflect the above changes and to assist in coordinating testing exercises. This person is currently assisting on our claims system conversion and will be joining the Enterprise Security and Risk Management team in Q3 of 2012. His focus will be BCP/DR and other Enterprise Risk Management initiatives."*



## **E. Application Controls**

### ***Application Configuration Management***

We evaluated the policies and procedures governing software development and change control of GEHA's [REDACTED] claims processing application.

GEHA has a series of policies and procedures related to application configuration management. GEHA has adopted a traditional system development life cycle methodology that IT personnel follow during routine software modifications. The following controls related to testing and approvals of software modifications were observed:

- GEHA has implemented change tracking software and correlating business practices that allow modifications to be tracked throughout the change process; and,
- Code, unit, system, and quality testing are all conducted in accordance with industry standards.

### ***Claims Processing System***

We evaluated the input, processing, and output controls associated with [REDACTED]. In terms of input controls, we documented the policies and procedures adopted by GEHA to help ensure that: 1) there are controls over the inception of claims data into the system; 2) the data received comes from the appropriate sources; and, 3) the data is entered into the claims database correctly. We also reviewed GEHA's quality assurance methods for reconciling processing totals against input totals and for evaluating the accuracy of its processes. Finally, we examined the security of physical input and output (paper claims, checks, explanation of benefits, etc.).

GEHA informed us that they are in the initial development phase of implementing a new claims processing system, [REDACTED]. This is scheduled for completion by the end of 2012.

### ***Provider Networks Involvement in Claims Processing***

GEHA utilizes PPO Contractor Networks (Network) that perform functions related to claims input and clinical editing. One Network, [REDACTED], has responsibilities for input, clinical edits, and output processes. During the course of our audit, we toured the facilities responsible for both the input and output of GEHA's UHC claims. We determined that there are sufficient processes in place to ensure the effective input of claims data.

GEHA sends [REDACTED] then prints provider checks from a GEHA bank account. However, GEHA and [REDACTED] do not reconcile the quantity and dollar amount of checks printed to the original submission by GEHA.

Without a reconciliation of the actual checks printed by [REDACTED] to those submitted by GEHA, there is an increased likelihood that improper claim payments will go undetected.

### **Recommendation 20**

We recommend that GEHA, in collaboration with [REDACTED] develop a process to reconcile printed checks.

**GEHA Response:**

***“We have initiated a project with our Project Management Department and have assembled a team to address this recommendation. We plan to coordinate with [REDACTED] and have a reconciliation process implemented once we have identified and created the necessary internal reporting.”***

***Enrollment***

We evaluated GEHA’s procedures for managing its database of member enrollment data. GEHA receives its enrollment data via fax, mail, and electronic update files. The majority of enrollment information is received electronically (about 70%) and is inputted into the database automatically. Enrollment information is otherwise inputted manually into the database. Information that is manually entered into the system is audited by enrollment specialists. Daily error reports are generated for managers to view as a part of the employee performance evaluation as well as used during the audit process by the enrollment specialists.

GEHA receives an e-mail attachment containing the quantity and type of enrollment file transmissions; however, at the time of the audit GEHA did not have a process to reconcile what is sent and what is actually received. As a result of our audit GEHA stated that it will begin a reconciliation process using the e-mail attachment and the files received.

There were no further concerns regarding GEHA’s enrollment policies, process and procedures.

***Debarment***

GEHA has adequate procedures for updating its claim system with debarred provider information, but it does not routinely audit its debarment database for accuracy.

GEHA downloads the OPM OIG debarment list every month and compares it to its provider maintenance file. Any debarred providers that appear in GEHA’s provider master database are flagged to prevent claims submitted by that provider from being processed by the claims processing system.

However, this process is done manually, and GEHA does not do a full reconciliation of the debarment list with its provider master database.

Failure to audit the accuracy of the debarment file increases the risk that claims are being paid to providers that are debarred.

**Recommendation 21**

We recommend that GEHA implement an audit process for the full debarment file.

**GEHA Response:**

***“GEHA does currently perform a monthly 3% audit on our full debarment file. However, based on the recommendation of OPM, we have increased the audit to 100% of the full debarment file effective April 15, 2012.”***

## **OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM's HIO with evidence of the monthly audit of the debarment file for a period of three months.

### ***Application Controls Testing***

To validate claims processing controls, a testing exercise was conducted on the GEHA [REDACTED] system. This test was conducted at GEHA's Independence, Missouri facility with the assistance of GEHA personnel. The exercise involved processing claims designed with inherent flaws in the test environment of the claims adjudication application. Upon conclusion of the testing exercise, the expected results were compared with the actual results obtained during the exercise.

The sections below document the opportunities for improvement that were noted related to application controls. GEHA intends to replace [REDACTED] with a new claims processing system called [REDACTED]. The recommendations contained within this section are directed toward this new system.

#### **1. Clinical Edits**

We submitted a hospital claim for a male with a diagnosis of postmenopausal bleeding and a procedure code for a total abdominal hysterectomy. This claim was processed and paid without encountering any system edits, despite the fact that this procedure could not be performed on a male. We were informed by GEHA that [REDACTED] does not have any clinical edits in place for hospital claims. This was a prior recommendation in 2005.

This system weakness increases the risk that benefits are being paid for procedures associated with a diagnosis that may not warrant such treatment.

#### **Recommendation 22**

We recommend that GEHA ensure that comprehensive medical edits are incorporated into the development of the new [REDACTED] claims processing system.

#### **GEHA Response:**

*“Our review of the [REDACTED] System and the new clinical editor has shown that [REDACTED] does not currently have edits for inpatient hospital claims. This specific claim example would not be captured in any of the edits. We will investigate the system capabilities of creating the configuration to assist in up front identification of these claims. There are [REDACTED] edits for outpatient hospital claims.*

*For the professional claim example, we have test cases developed to review diagnosis to procedure code edits. The system can then be coded to pend, deny, or use a warning message.*

*We have not received the latest version of [REDACTED] to test at this time. We will add these examples to our requirements and set up specific test cases to test capabilities to ensure accurate processing . . . .”*

**OIG Reply:**

The lack of clinical edits in GEHA’s claims processing system extends back to a prior OPM OIG audit from 2005. Clinical edits are a necessary element of implementing a new claims processing system. We continue to recommend that GEHA make the appropriate system modifications to ensure clinical edits are implemented for both professional and facility claims. As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with appropriate supporting documentation indicating its progress in successfully implementing these modifications.

**2. Therapy Visit Counter**

Procedure codes for therapy visits indicate a specific length of time of the services provided. The benefit structure only allows 2 hours per visit in addition to limiting the number of visits per year to 60. GEHA is not appropriately calculating the length of time per visit.

The OIG submitted a series of claims to test [REDACTED] ability to limit physical and occupational therapy visits to 60 per calendar year. While the system is configured to stop paying claims after 60 visits, we submitted a visit for 2.25 hours, and it was counted as 1 visit rather than two.

This system weakness increases the risk that providers are paid for rendering non-covered services.

**Recommendation 23**

We recommend that GEHA ensure that the appropriate system modifications be incorporated into the [REDACTED] claims processing system to ensure that therapy benefits are limited in accordance with the plan brochure.

**GEHA Response:**

*“GEHA agrees with the recommendation to ensure this is addressed in the conversion to [REDACTED] However, between now and the time of conversion to [REDACTED] we have implemented interim procedures in the Claims Department to adjudicate claims correcting the calculation of time per visit.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that GEHA provide OPM’s HIO with supporting documentation for the interim process showing that therapy claims are automatically detected for manual review/calculation. Furthermore, we recommend GEHA provide evidence of the implementation of these edits in place in the [REDACTED] claims processing system.

### 3. Overlapping Hospital Stays

The [REDACTED] system paid duplicate room and board charges on test claims for a member with two overlapping hospital stays.

The system does not have edits in place to prevent both room and board and intensive care charges for the same time period. We submitted a claim for an intensive care room and a subsequent claim for a semi-private room at the same facility on the same day. We were informed by GEHA representatives that [REDACTED] only looks at the revenue code for duplicate billing. As long as different revenue codes are used, the system will never detect multiple claims containing overlapping dates of service for hospital stays.

This system weakness increases the risk that hospitals are being paid for duplicate room and board expenses.

#### **Recommendation 24**

We recommend that GEHA ensure that the appropriate system configurations are made to [REDACTED] to prevent duplicate payments for claims with overlapping dates of service.

#### **GEHA Response:**

*“GEHA agrees with the recommendation and will explore the system configuration available in [REDACTED] to ensure accurate claim processing.”*

### 4. OBRA 90 PRICER

GEHA is pricing OBRA90 claims with outdated versions of the [REDACTED] program.

We entered several test claims subject to OBRA90 pricing into the [REDACTED] system. The system suspended all of the claims for OBRA90 pricing (also referred to as diagnosis-related group or DRG pricing), and the GEHA claims adjudicator priced each claim using the [REDACTED].

We also independently priced each claim using the most recent versions of the [REDACTED] programs, and compared the Medicare DRG amount produced to that calculated by the GEHA adjudicator. All of the test claims processed by GEHA were priced accurately, however we received screenprints of the [REDACTED] from GEHA which indicated GEHA was not using the most current version of the [REDACTED].

Failure to promptly provide claims adjudicators with updated versions of the [REDACTED] program increases the risk that GEHA is pricing OBRA90 claims incorrectly.

#### **Recommendation 25**

We recommend that GEHA implement procedures to ensure that OBRA90 claims are priced with the correct version of the [REDACTED].

**GEHA Response:**

*“GEHA agrees with the recommendation and is taking steps to ensure that the adjusters have access to the most current version of the OBRA 90 Pricer before claims processing. This will include working more closely with the IT area to ensure timely loading of the current version, while considering whether claims may need to be held in the interim to prevent claim payment issues.”*

**5. Manual Processing of Claims**

A significant portion of claims processed by GEHA are processed manually, including all hospital, anesthesiology, and renal failure claims.

The amount of manual effort required by adjudicators to process claims greatly increases the risk that these claims are processed incorrectly.

**Recommendation 26**

We recommend that GEHA ensure that the appropriate system configurations are made to [REDACTED] to ensure that a reduced manual effort is required by claims adjudicators to process claims.

**GEHA Response:**

*“GEHA is exploring every opportunity to reduce manual processes. Conversion to the [REDACTED] system will facilitate our goals in this area. While our conversion to [REDACTED] is still in the ‘build’ phase, we have already identified several areas of opportunity where reduced manual effort will be realized . . . . ”*

**F. Health Insurance Portability and Accountability Act**

The OIG reviewed GEHA’s efforts to maintain compliance with the security and privacy standards of HIPAA.

GEHA has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. GEHA has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. The plan has a designated Privacy Official who has the responsibility of ensuring compliance with HIPAA Privacy and GEHA’s HIPAA Privacy policies. GEHA employees receive HIPAA-related training during new hire orientation, as well as annual refresher training.

Nothing came to our attention that caused us to believe that GEHA is not in compliance with the various requirements of HIPAA regulations.

### **III. Major Contributors to This Report**

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

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

## Appendix



The Benefits of Better Health

May 10, 2012

██████████  
Auditor in Charge

Information Systems Audits Group Office of the Inspector General  
1900 E Street, NW Room 6400  
Washington, DC 20415-1100

Dear ██████████

We have completed our review of the report for the Audit of Information Systems General and Application Controls at Government Employees Health Association (GEHA) dated March 14, 2012. The following are our responses for each recommendation that was presented in the report.

### Recommendation 1

We recommend GEHA develop a rules of behavior agreement and require all employees to sign the document.

### **GEHA Response**

GEHA has an extensive orientation process where new hires are trained on various policies and procedures and are required to sign Acknowledgement of Responsibility forms. These acknowledgements encompass what one rules of behavior document would address.

1. Acknowledgement of GEHA Code of Ethics.
  - a. Confidentiality Agreement which is required upon hire and annually thereafter. The Confidentiality agreement ensures the employee to keep GEHA proprietary and health information confidential and to report any accidental or intentional disclosure.
  - b. HR policy 5-05 – Code of Ethics which includes a section on 'compromising computer security'
2. Acknowledgement of Responsibility for HIPAA confidentiality of patient information. This is required upon hire and thereafter when additional training is given.
  - a. HIPAA Policy 210 – Confidentiality and Security of Patient Information-Employee Breach and Disciplinary Action.
  - b. HIPAA Policy 215 - Breach Reporting, Investigation and Notification Requirements.
3. Acknowledgement of GEHA Information Protection Policy.

**Government Employees Health Association, Inc.**

P.O. Box 4665 • Independence, MO 64051-4665 • Telephone (800) 821-6136

[www.geha.com](http://www.geha.com)



- a. HR Policy 5-35 – Information Protection. This policy covers all information in any form and from any system.
- b. HIPAA Policy 840 – Internet and Software Acceptable Use Policy

**Recommendation 2**

We recommend that GEHA reassess its facilities' physical access management and implement controls that will ensure proper physical security. At a minimum, GEHA should implement [REDACTED]  
[REDACTED] t data center entrances.

**GEHA Response**

GEHA is currently reassessing facilities access at all of our locations and adding the following controls to increase physical security.

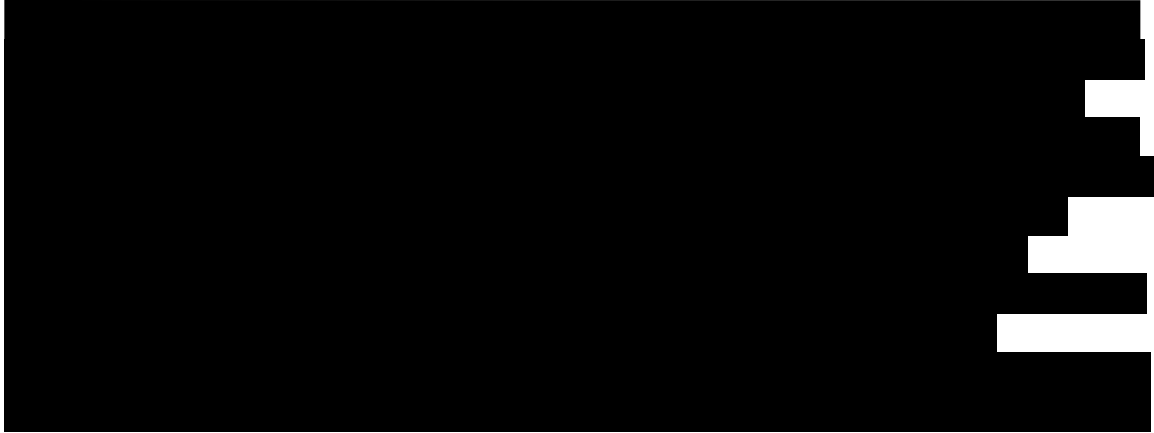
[REDACTED]

**2) Data Center – Multi-Factor Authentication at Entrance (COMPLETED)** - Access to GEHA's data center at our 310 building requires both an access badge as well as the code to a cipher lock built into the door. The addition of the cipher lock was completed in September of 2011.

**3)** [REDACTED]

**4)** [REDACTED]

5)



**Recommendation 3**

We recommend that GEHA implement physical controls to prevent employees that only require access to the [REDACTED]

**GEHA Response**

GEHA continues to keep this area locked during non-business hours and corrected this concern in October 2011 by installing a latching system on the inside of the storage area that prevents unsupervised access.

**Recommendation 4**

We recommend that GEHA implement a process to monitor and track access to claim files (in the mail sort room).

**GEHA Response**

The area where the claims are kept is separated from the [REDACTED] by a locked door. Access to this area is restricted to a limited number of claims clerical staff. There are no sign out procedures because claims leave this area only to be copied and immediately returned to the locked room.

**Recommendation 5**

We recommend GEHA conduct a detailed access review audit of [REDACTED] user accounts to identify accounts with inappropriate access.

**GEHA Response**

GEHA Security Operations has taken multiple steps to better control [REDACTED] access. We have reviewed access for users with administrative access and have removed access that was inappropriate or no longer needed. To better establish and control access, we have developed a series of user templates that determine access by position. In doing so we have consulted with managers to verify access and remove any unneeded access. We have developed reporting

from our payroll department that will allow us to better track users as they move within the organization or terminate. We have reviewed all previously terminated users to assure that all access has been removed. For auditing purposes it is necessary to leave IDs for terminated employees in place, however, all access to the ID is removed, the account is locked, and the associated [REDACTED] user id is removed. This activity has been completed.

**Recommendation 6**

We recommend that GEHA configure its intrusion detection tools to optimize their capabilities.

**GEHA Response**

GEHA uses a [REDACTED] firewall that includes intrusion detection capabilities. The intrusion detection capabilities were recently activated and are being monitored to determine effectiveness in detecting known attacks. [REDACTED] are updated regularly to assure that detection capabilities are current. The Security Operations team will assist the Enterprise Architecture team in fine-tuning the detection capabilities as monitoring reveals changes that can be made to improve the system's response. [REDACTED]  
[REDACTED]

**Recommendation 7**

We recommend that GEHA implement [REDACTED] for remote access.

**GEHA Response**

GEHA has taken steps to purchase and implement [REDACTED] for remote access users. Remote web access to GEHA resources forces [REDACTED] to GEHA's [REDACTED] environment using [REDACTED]. This project has been completed for all users with remote access.

**Recommendation 8**

We recommend that GEHA document a process for ensuring application access is granted with proper segregation of duties and implement the process for all major applications.

**Response**

GEHA has taken steps to identify duties within the claims processing area and has defined those activities that present a potential violation of the segregation of duties. [REDACTED] access has been reviewed and conflicting access removed. Other applications have initially been configured to reduce conflicts, but currently need to be reviewed and any conflicts removed. Expected completion of this activity is by the end of the fourth quarter of 2012.

GEHA's Internal Audit Department performs an annual audit of access rights on major applications for employees who have terminated or transferred positions.

### **Recommendation 9**

We recommend that GEHA expand the access recertification process to all major applications.

#### **Response**

The GEHA Security Operations team is in the process of working with managers to develop [REDACTED] and major applications. During the process we are aligning current access of individuals to templates created for the role or job title they hold. Managers are reviewing access changes to align with templates created. Going forward the Security Operations team will use this application reports and templates to verify with management the access of all employees at least annually.

### **Recommendation 10**

We recommend that GEHA implement a process to log and review user activity within its applications.

#### **Response**

The Security Operations team has developed a daily process to review [REDACTED] violation reports. [REDACTED]. Violation reports for [REDACTED] and other applications are not available at this time. [REDACTED] reports are reviewed, users are contacted to respond to violations, and notations are made electronically on the report pdf file. The file is stored along with related correspondence. This process is currently implemented.

### **Recommendation 11**

We recommend that GEHA program the new claims processing system to use randomly generated temporary passwords for users who need to establish new accounts and users who lock themselves out of the system. The passwords should be automatically emailed to the user requesting access.

#### **Response**

The Security Operations team will review current practices for creating [REDACTED] IDs and modify the process as necessary adding steps to require interaction with the Help Desk before a user id is activated for first use. The new claims system uses authentication based on [REDACTED] where users will automatically authenticate to [REDACTED] as they activate the application client. [REDACTED] password management will be reviewed and changes made as necessary to randomize initial passwords. A password self-service tool will be investigated to see if they provide a more secure method for changing initial or forgotten passwords. Changes to processes will be completed by the fourth quarter of 2012.

### **Recommendation 12**

We recommend that GEHA formally document baseline configurations for its hardware, software, and firmware.

### **Response**

GEHA is addressing secure baseline configuration in a three-phase approach. Each phase will document the system function, inventory, configurations and security hardening requirements. For the initial phase, GEHA is focusing on [REDACTED].

The second phase will extend into higher levels of the architecture including but not limited to [REDACTED]. The final phase will be a granular view of the business applications that utilize the architecture detailed in the first two phases such as [REDACTED].

### **Recommendation 13**

We recommend that GEHA implement a process to routinely monitor system administrator activity.

### **Response**

The Security Operations team has developed a daily process to review [REDACTED] administrator activity reports. The [REDACTED] reports are reviewed, users are contacted to respond to questionable activities, and notations are made electronically on the report pdf file. The file is stored along with related correspondence. The new claims processing system will require different tools to track administrative access because access will primarily be controlled through [REDACTED]. It may be possible to track administrative access within the new application but that is unknown at this time. A tool is being investigated that will track user data view and that tool may provide additional visibility within the new claims application. [REDACTED] administrator activity monitoring is currently implemented.

### **Recommendation 14**

We recommend that GEHA address the issues detected by the compliance audit and routinely monitor system software configuration to ensure compliance with established baselines.

**Response** - The recent purchase of a security vulnerability scanning tool by the Security Operations team gives us the ability to scan configuration settings of individual [REDACTED] servers once authenticated to the server. Security Operations will work with the Enterprise Architecture to assure that appropriate settings are routinely scanned and addressed. This recommendation should be completed by the end of the fourth quarter of 2012.

### **Recommendation 15**

We recommend that GEHA implement a process to conduct routine vulnerability scans and track any identified weakness until they are remediated.

**Response**

A product to scan systems for vulnerabilities has recently been purchased and a project has been created to develop processes for scanning, notification of findings, risk assessment, remediation, and review. The project will focus on reducing the risk to the organization by implementing a routine vulnerability monitoring and remediation program. This recommendation should be completed by the end of the fourth quarter of 2012.

**Recommendation 16**

We recommend that GEHA install the [REDACTED] that were identified in the scan results and, in the future, improve the [REDACTED] management process to ensure that [REDACTED] are installed promptly.

**Response**

GEHA recognizes the need and importance of developing and implementing a [REDACTED] to identify [REDACTED], determine applicability to GEHA systems, and distribute and implement on GEHA systems to prevent and minimize the risk of security breaches and losses. GEHA is initiating a formal [REDACTED] to mitigate the risk presented by the [REDACTED]. The program will be a combination of technology in the form of [REDACTED] and deployment software and processes to identify, test and deploy software updates following a risk-based management approach. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**Recommendation 17**

We recommend that GEHA contract with a third party vendor that specializes in [REDACTED] vulnerability assessments to conduct a thorough [REDACTED] vulnerability assessment of its [REDACTED].

**Response**

GEHA is addressing [REDACTED] vulnerabilities in two different ways. In late 2012, we engaged a third-party, [REDACTED] to conduct a comprehensive [REDACTED] vulnerability assessment and penetration test. The scope of the assessment included our [REDACTED] [REDACTED]. Our IT and Security teams are actively remediating issues noted in that assessment. In addition, GEHA is currently redesigning our [REDACTED] and Security teams are involved in those discussions to ensure that any open vulnerabilities or concerns are addressed in the new design.

The second way we are addressing this issue is the purchase and implementation of [REDACTED]. Our Information Security Analysts have installed this solution and are currently conducting configuring and testing. This tool will be used on a continuous basis to assist security in identifying vulnerabilities affecting our infrastructure and will assist in the risk ranking of those vulnerabilities to drive remediation priorities. The solution will have the ability to not only alert security staff to vulnerabilities facing our [REDACTED], but also vulnerabilities on our [REDACTED]. We expect to have [REDACTED] fully deployed in our production environment and identifying vulnerabilities by Q3 of 2012.

We feel that it is important and we plan to continue engaging a third party to conduct an independent assessment, however due to the addition of our [REDACTED] tool and vulnerability management processes, we will be reducing the frequency of those from annually to perhaps every other year.

#### **Recommendation 18**

We recommend that GEHA continue their efforts to upgrade the [REDACTED] operating system to a vendor-supported version.

#### **Response**

GEHA is continuing the efforts to update the [REDACTED] operating systems to vendor-supported versions. We are working through the [REDACTED] and custom-developed application dependencies which require update before the [REDACTED] operating systems can be updated.

GEHA has also had to procure and implement a new [REDACTED] storage subsystem to allow for the increased capacity needs for the testing environments for process and inter-operability testing.

#### **Recommendation 19**

We recommend that GEHA conduct and document an annual disaster recovery test for the [REDACTED].

#### **Response**

GEHA has designed and implemented a secured off-site co-location facility that will function as the disaster recovery site for all [REDACTED]. GEHA is currently replicating all [REDACTED] data to the site through the use of the [REDACTED] data protection platform.

GEHA is scheduled to perform disaster recovery testing in Q3 of 2012. We have hired a Manager of Enterprise Risk that will be responsible for working with IT to maintain/update our BCP/DR plans to reflect the above changes and to assist in coordinating testing exercises. This person is currently assisting on our claims system conversion and will be joining the Enterprise Security and Risk Management team in Q3 of 2012. His focus will be BCP/DR and other Enterprise Risk Management initiatives.



### **Recommendation 20**

We recommend that GEHA, in collaboration with [REDACTED], develop a process to reconcile printed checks.

### **Response**

We have initiated a project with our Project Management Department and have assembled a team to address this recommendation. We plan to coordinate with [REDACTED] and have a reconciliation process implemented once we have identified and created the necessary internal reporting.

### **Recommendation 21**

We recommend that GEHA implement an audit process for the full debarment file.

### **Response**

GEHA does currently perform a monthly 3% audit on our full debarment file. However, based on the recommendation of OPM, we have increased the audit to 100% of the full debarment file effective April 15, 2012.

### **Recommendation 22**

We recommend that GEHA ensure that comprehensive medical edits are incorporated into the development of the new [REDACTED] claims processing system.

### **Response**

Our review of the [REDACTED] System and the new clinical editor has shown that [REDACTED] does not currently have edits for inpatient hospital claims. This specific claim example would not be captured in any of the edits. We will investigate the system capabilities of creating the configuration to assist in up front identification of these claims. There are [REDACTED] edits for outpatient hospital claims.

For the professional claim example, we have test cases developed to review diagnosis to procedure code edits. The system can then be coded to pend, deny, or use a warning message.

We have not received the latest version of [REDACTED] to test at this time. We will add these examples to our requirements and set up specific test cases to test capabilities to ensure accurate processing.

The OIG finding included the following information – “GEHA informed us that for professional claims, clinical edits produce warning messages rather than having hard edits in place to prevent the claim from processing. If these claims are submitted electronically, they could be batched and subsequently processed and paid without a processor ever seeing that warning message.”

GEHA response - GEHA does not allow claims with these Clinicallogic warning messages to pass through batch, rather they are pending to the adjustor for additional review.

**Recommendation 23**

We recommend that GEHA ensure that the appropriate system modifications be incorporated into the [REDACTED] claims processing system to ensure that therapy benefits are limited in accordance with the plan brochure.

**Response**

GEHA agrees with the recommendation to ensure this is addressed in the conversion to [REDACTED]. However, between now and the time of conversion to [REDACTED] we have implemented interim procedures in the Claims Department to adjudicate claims correcting the calculation of time per visit.

**Recommendation 24**

We recommend that GEHA ensure that the appropriate system configurations are made to [REDACTED] to prevent duplicate payments for claims with overlapping dates of service.

**Response**

GEHA agrees with the recommendation and will explore the system configuration available in [REDACTED] to ensure accurate claim processing.

**Recommendation 25**

We recommend that GEHA implement procedures to ensure that OBRA90 claims are priced with the correct version of the [REDACTED]

**Response**

GEHA agrees with the recommendation and is taking steps to ensure that the adjusters have access to the most current version of the OBRA 90 Pricer before claims processing. This will include working more closely with the IT area to ensure timely loading of the current version, while considering whether claims may need to be held in the interim to prevent claim payment issues.

**Recommendation 26**

We recommend that GEHA ensure that the appropriate system configurations are made to [REDACTED] to ensure that a reduced manual effort is required by claims adjudicators to process claims.

## Response

GEHA is exploring every opportunity to reduce manual processes. Conversion to the [REDACTED] system will facilitate our goals in this area. While our conversion to [REDACTED] is still in the "build" phase, we have already identified several areas of opportunity where reduced manual effort will be realized

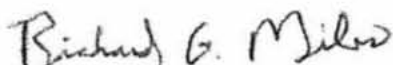
- With the addition of [REDACTED] we expect improvements in automated hospital and anesthesia processing.
- We will be using revenue coding which is required by some PPO networks. This will be loaded from the electronic claim and added to the processes in our data entry area. With this information, pricing can be applied through [REDACTED] allowing more claims to auto-adjudicate.
- For PPO USA hospitals and facilities that use a complex rate, they will be priced with [REDACTED] and auto-adjudicated.
- Authorizations for hospital stays will be loaded into [REDACTED] and then matched to the specific claim they represent. This will reduce manual review of the authorization and allow auto-adjudication of hospital stays and outpatient services.
- ASA codes and the associated units are also being loaded into the pricing software, as well as configuration of the time units, so that auto-calculation can be performed.
- National Contracts pricing is also loaded in [REDACTED] reducing the manual pricing that is required today.

## Conclusion

We are disappointed in the results of the audit, however we were making progress to update and improve our information systems infrastructure. We have filled several key positions within the last year to expand our expertise and have added staff to address weaknesses that were noted in the OIG's report. Prior to the start of the audit we formed an Enterprise Security and Risk Management Department that is independent of the IT Department and reports directly to me. The Enterprise Security and Risk Management Department is responsible for establishing security policies, assessing vulnerabilities and working with Information Systems management to remediate weaknesses in internal controls.

We thank you and your staff for your assistance in identifying the areas needing improvement and we are working diligently to resolve these issues.

Sincerely,



Richard G. Miles  
President

Attachments: Audit Report Draft

CC: [REDACTED], Chief of Health Insurance II Insurance Operations  
[REDACTED], Chief of Program Planning and Evaluation  
Eileen Hutchinson, GEHA VP - CFO  
[REDACTED] GEHA VP – Claims  
[REDACTED] GEHA VP – Enterprise Security and Risk Management  
[REDACTED] GEHA Manager of Internal Audit