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 EMBLEMHEALTH

Report No. 1D-80-00-12-045

Date: December 10, 2012

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 1056 & 2655

EMBLEMHEALTH

PLAN CODES 6V1 / 6V2 / X41 / X42 / 801 / 802
804 / 805 / 511 / 512 / 514 / 515

NEW YORK, NEW YORK

Report No. 1D-80-00-12-045

Date: December 10, 2012

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACTS 1056 & 2655

EMBLEMHEALTH

PLAN CODES 6V1 / 6V2 / X41 / X42 / 801 / 802
804 / 805 / 511 / 512 / 514 / 515

NEW YORK, NEW YORK

Report No. 1D-80-00-12-045

Date: December 10, 2012

This final report discusses the results of our audit of general and application controls over the information systems at EmblemHealth. EmblemHealth has separate plans that service federal employees: GHI Health Plan, GHI HMO Select Plans, and HIP Health of Greater New York.

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

Security Management

EmblemHealth has established a series of IT policies and procedures to create an awareness of IT security at the Plan. We also verified that EmblemHealth has adequate human resources policies related to the security aspects of hiring, training, transferring, and terminating employees.

Access Controls

EmblemHealth has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. However, we did note opportunities for improvement related to EmblemHealth's authentication controls over physical access to the data centers as well as the method for encrypting emails containing PII. EmblemHealth has since remediated all of these weaknesses.

Configuration Management

EmblemHealth has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes. However, we noted several weaknesses in EmblemHealth's configuration management program related to mainframe, server, and database system configurations. EmblemHealth has since remediated several of these weaknesses and is working to implement the necessary changes for the remaining vulnerabilities.

Contingency Planning

We reviewed EmblemHealth'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.

Claims Adjudication

EmblemHealth has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we recommended that EmblemHealth implement a tool to facilitate automation of its application configuration change process.

Health Insurance Portability and Accountability Act (HIPAA)

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

Contents

I. Introduction

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

The audit was conducted pursuant to FEHBP contracts CS 1056 and CS 2655; 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.

This was our first audit of EmblemHealth's general and application controls. We also reviewed EmblemHealth's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All EmblemHealth 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.

Objectives

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

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

Scope

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of EmblemHealth'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 EmblemHealth'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.

EmblemHealth has separate plans that service federal employees: two Health Maintenance Organization plans referred to as GHI-HMO and HIP-HMO; and a fee-for-service plan, GHI.

The scope of this audit centered on the information systems used by EmblemHealth to process medical insurance claims for FEHBP members, with a primary focus on their claims adjudication applications. Three separate systems are used to process claims at EmblemHealth: one for GHI professional claims, one for GHI facility claims, and a third for both GHI-HMO and HIP-HMO claims. The business processes reviewed are primarily located in EmblemHealth's New York, New York facilities.

The on-site portion of this audit was performed in April and May of 2012. 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 EmblemHealth as of May 2012.

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

Methodology

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed EmblemHealth's business structure and environment;
- Performed a risk assessment of EmblemHealth's information systems environment and applications, and prepared an audit program based on the assessment and the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and,
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing. Results of samples that are judgmentally or randomly selected cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

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

- Title 48 of the Code of Federal Regulations;
- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, 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 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 EmblemHealth's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, EmblemHealth 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 EmblemHealth's overall IT security controls. We evaluated EmblemHealth's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

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

B. Access Controls

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls at EmblemHealth's New York headquarters buildings and its data center. We also examined the logical controls protecting sensitive data on EmblemHealth's network environment and claims processing applications. Furthermore, we conducted an automated network topology scan to verify that all known assets were included within EmblemHealth's computer hardware inventory.

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 Windows/network access for terminated employees; and,
- Controls to monitor and filter email and Internet activity.

However, the following sections document several opportunities for improvement related to EmblemHealth's physical access and network environment controls.

1. Access to Data Center

EmblemHealth's primary data centers use stand-alone electronic card readers to control physical access. However, we expect all FEHBP contractors to also have multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at all data center entrances. In addition to this minimum requirement, the following list outlines physical access controls that are common at other FEHBP carrier facilities:

- Piggybacking alarms to enter the computer room (alarm that sounds if more than one person walks past a sensor for each access card that is swiped); and,
- "Man-trap" entrances (small space with two locking doors where the first door must close before the second opens).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to EmblemHealth's data centers and the sensitive IT resources and confidential data they contain. NIST SP 800-53 provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 1

We recommend that EmblemHealth reassess its data centers' physical access management and implement controls that will improve physical security. At a minimum, EmblemHealth should implement multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at data center entrances.

EmblemHealth Response:

"Dual input card readers, that require both an access card and a PIN, were installed for each entrance to the data center on September 12, 2012."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has implemented multi-factor authentication at data center entrances; no further action is required.

2. Email Encryption

We conducted a test of EmblemHealth's e-mail encryption program by asking an EmblemHealth employee to send us sample e-mails containing personally identifiable information (PII). We expected the encryption program to detect the PII and automatically encrypt the emails. However, the application did not encrypt any of the e-mails.

OMB Memorandum M-07-16 recommends "using encryption, strong authentication procedures, and other security controls to make [PII] . . . unusable by unauthorized individuals."

Failure to implement adequate e-mail encryption controls increases the risk that unauthorized individuals can access PII.

Recommendation 2

We recommend that EmblemHealth review its configuration settings for e-mail encryption to ensure that all PII is appropriately protected.

EmblemHealth Response:

"We have implemented the SSN lexicon for ZixSelect, the tool that we use to automatically encrypt e-mail containing PHI. A single SSN will force the encryption. We acknowledge the importance of the SSN as a key element of the e-mail and that it is PII vs. PHI . . . ."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has modified its e-mail encryption software to protect PII; no further action is required.

C. Configuration Management

EmblemHealth uses three claims adjudication applications: the GHI professional claims processing system (MCS), the GHI facility claims processing system (HCS), and the GHI HMO and HIP HMO claims processing system (QCare). We evaluated EmblemHealth's controls to securely configure the mainframe, databases, and servers that support these applications. We determined that the following controls are in place:

- Controls for securely managing changes to the operating platform and claims processing application;
- Controls for monitoring privileged user activity on the operating platform; and,
- Documented patch management procedures.

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

1. Mainframe System Configuration

EmblemHealth has a documented Mainframe Security Standard that outlines the approved configuration of its mainframe security software. However, our review of EmblemHealth's actual mainframe configuration identified several insecure settings. Although no settings directly violated the Security Standard, we believe that the policy is not comprehensive enough because it does not provide guidance on the specific settings in question. The problems that were detected were detailed in the draft report, but due to the sensitive nature of these findings, the specific settings in question will not be included in this report.

NIST SP 800-53 Revision 3 requires that the "organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system." The guidance also recommends that the organization review and update the baseline configuration at an organization-defined frequency, when required to under organization-defined circumstances, and as an integral part of the information system component installations and upgrades.

Failure to have appropriate security configurations based on common security practices increases the likelihood an attacker can gain access to sensitive data on the mainframe.

Recommendation 3

We recommend that EmblemHealth make the appropriate configuration changes related to the specific weaknesses identified during this audit.

EmblemHealth Response:

"We have implemented four of the recommended configuration changes and will implement an additional two on September 15, 2012. . . ."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has appropriately implemented several of the configuration changes we recommended.

However, several configuration changes still need to be implemented to fully address this recommendation. The details of the remaining weaknesses have been provided to EmblemHealth and OPM's HIO. We recommend that EmblemHealth update HIO on its progress to implement the remaining configuration settings.

Recommendation 4

We recommend that EmblemHealth update its Mainframe Security Standard to contain a detailed secure mainframe baseline configuration.

EmblemHealth Response:

"We updated the Mainframe Security Standard to include our approved baseline configuration."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has appropriately updated its Mainframe Security Standard to include its baseline configuration; no further action is required.

2. Server and Database Configuration

EmblemHealth uses a third party vendor to periodically conduct vulnerability scans on its information systems. As part of this audit, we conducted our own automated vulnerability scans on a sample of EmblemHealth's systems (including 20 production servers and two databases) to identify security vulnerabilities. Our scans detected a variety of insecure configurations in EmblemHealth's environment. The list below outlines a high level description of the problems that were detected, but due to the sensitive nature of these findings, the details will not be included in this report. We determined that several servers and/or databases:

- Did not have critical patches, service packs, and hot fixes implemented in a timely manner;
- Are running operating systems and/or software that is no longer supported by the vendor;

- Do not have up-to-date antivirus software and/or virus definitions;
- Are running third party applications that were not appropriately updated or patched; and,
- Have password settings that are not in compliance with EmblemHealth's corporate password policy.

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." In addition, NIST SP 800-53 Revision 3 states that "The organization configures the information system to provide only essential capabilities. . . ." An organization should also review the information system to identify and eliminate unnecessary functions.

Failure to promptly install important updates, implement least functionality to an information system, and implement appropriate authentication controls can increase the amount of exposed vulnerabilities and methods an intruder can use to gain unauthorized access to the system.

Recommendation 5

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

EmblemHealth Response:

"We analyzed the server problems and determined that the tool we were using, Ecora, was not working as intended; we replaced this tool with ITCM and will monitor its effectiveness as we roll it out to the rest of the servers and databases. We have applied all of the fixes to the servers."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has appropriately patched the production servers; no further action is required.

Recommendation 6

We recommend that EmblemHealth implement appropriate procedures and controls to ensure that only current and supported versions of system software are installed on the production servers.

EmblemHealth Response:

"Several of our legacy in-house-developed applications are dependent on an older operating system. We are looking at new architecture to replace them. In the meantime,

we cannot upgrade the operating systems to supported versions because of the adverse impact that would have on our customers and our business."

OIG Reply:

As part of the audit resolution process, we recommend that EmblemHealth update OPM's HIO on its progress to implement new architecture and to ensure that only current and supported versions of system software are installed on the production servers.

Recommendation 7

We recommend that EmblemHealth implement appropriate procedures and controls to ensure that anti-virus software definitions are up-to-date on all production servers.

EmblemHealth Response:

"Information Security is now reviewing Anti-virus signatures on all servers via the EPO console on a daily basis. This task was added to the Daily Checklist."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has updated its procedures to ensure anti-virus definitions are current on all production servers; no further action is required.

Recommendation 8

We recommend that EmblemHealth review its current system configurations to ensure that only necessary software is installed on the production servers.

EmblemHealth Response:

"We have reviewed the Nessus reports and are in the process of identifying and removing unnecessary software. Going forward, we have a standard build for new servers to ensure that unnecessary software is not installed, and we will perform periodic reviews to ensure that we are at either emerging or current status for our operating systems."

OIG Reply:

As part of the audit resolution process, we recommend that EmblemHealth update OPM's HIO on its progress to identify and remove unnecessary software. EmblemHealth should also provide HIO with evidence of the first annual review.

Recommendation 9

We recommend that EmblemHealth implement appropriate controls to ensure that user accounts on system databases comply with corporate password policies.

EmblemHealth Response:

"Passwords on the database are now in compliance with EmblemHealth's Password Standard."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has appropriately changed its database settings to match their corporate password policy; no further action is required.

D. Contingency Planning

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

- Disaster response plan;
- Business continuity plan for data center operations;
- Business continuity plans for legacy GHI claims processing operations and claims support;
- Disaster recovery plan tests conducted in conjunction with the recovery site; and,
- Emergency response procedures and training.

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems." EmblemHealth has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that EmblemHealth has not implemented adequate controls related to contingency planning.

E. Claims Adjudication

The following sections detail our review of the applications and business processes supporting EmblemHealth's claims adjudication process.

1. Application Configuration Management

We evaluated the policies and procedures governing software development and change control of EmblemHealth's claims processing applications.

EmblemHealth has policies and procedures related to application configuration management. EmblemHealth has adopted a thorough system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- EmblemHealth has adopted practices that allow modifications to be tracked throughout the change process;
- Code, unit, system, and quality testing are all conducted in accordance with industry standards; and,
- EmblemHealth uses a separate business unit to move the code between development and production to ensure adequate segregation of duties.

However, the configuration management process relies heavily on manual effort and could be improved with the implementation of automated tools. EmblemHealth has explored the option of implementing a change management tool and is considering a second pilot. The tool would force all steps in the change management process to occur in order with all required documentation and approvals in place before moving code into production. An automated tool would reduce the risk of human error and the movement of code without approved and complete change packages.

Recommendation 10

We recommend that EmblemHealth install and implement an automated tool to facilitate the application configuration management process.

EmblemHealth Response:

"We are in the process of customizing [redacted] for EmblemHealth's environment for implementation in 2013. In the meantime, we have implemented an additional tool to replace part of our existing mainframe implementation process and continue to be very diligent about our manual procedures."

OIG Reply:

As part of the audit resolution process, we recommend that EmblemHealth update OPM's HIO on its progress to implement a change management tool.

2. Claims Processing System

We evaluated the input, processing, and output controls associated with EmblemHealth's claims adjudication systems. We determined that EmblemHealth has implemented policies and procedures to help ensure that:

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

We do not have any concerns regarding EmblemHealth's claims processing policies and procedures.

3. Enrollment

We evaluated EmblemHealth's procedures for managing its database of member enrollment data. Changes to member enrollment information are primarily received via an encrypted electronic transmission. Changes to enrollment are predominately automated. Exceptions that require manual processing are identified during an overnight batch process that generates a report of manual enrollment changes. These updates are then manually entered into the enrollment system. EmblemHealth has an audit function for each step of the enrollment process that requires manual data manipulation.

We do not have any concerns regarding EmblemHealth's enrollment policies and procedures.

4. Debarment

EmblemHealth has adequate procedures for updating its claim system with debarred provider information, and the Plan routinely audits its debarment database for accuracy.

EmblemHealth downloads the OPM OIG debarment list every month and compares it to its provider maintenance file. Any debarred providers that appear in EmblemHealth's provider master database are flagged to prevent claims submitted by that provider from processing successfully during the claims adjudication process.

However, EmblemHealth's debarment procedures do not comply with OPM's "Guidelines for Implementation of FEHBP Debarment and Suspension Orders." EmblemHealth's claim payment guidelines state that "All claims will be denied the first day following the date of the debarment/mandatory termination." OPM's Guidelines for Implementation of FEHBP Debarment and Suspension Orders state that claims should be paid during a 15 day "grace period" after members have been notified that a doctor has been debarred.

Recommendation 11

We recommend that EmblemHealth make the appropriate changes to its debarment policies and procedures to comply with OPM's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.

Recommendation 12

We recommend that EmblemHealth make the appropriate changes to their claims processing systems to ensure FEHBP claims are processed in accordance with OPM's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.

EmblemHealth Response:

"We are in agreement with both recommendations. Based on these recommendations EmblemHealth has taken the opportunity to reinforce the policies and procedures followed in support of the Guidelines.

All of the necessary and appropriate protocols specified in the FEHB contract are now in place. These important functions have been reviewed in detail to make sure all of the specific responsibilities are appropriately applied to all FEHBP claims. Comprehensive policies and procedures have been implemented to provide a seamless member transition from debarment of health care providers by OPM."

OIG Reply:

The evidence provided by EmblemHealth in response to the draft audit report indicates that the Plan has appropriately updated its policies and procedures and made the system

modification to ensure compliance with OPM guidelines; no further action is required for either recommendation 11 or 12.

5. Special Investigations and Fraud

The OIG evaluated the EmblemHealth policies and procedures governing special investigations and fraud. We determined that EmblemHealth has substantial policies and procedures in place to detect, manage, and report fraud.

There were no areas of improvement noted during our review.

6. Application Controls Testing

We conducted a test on EmblemHealth's claims adjudication applications to validate the systems' claims processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which EmblemHealth's systems adjudicated the claims. Test claims were submitted for MCS, HCS, and QCare.

Our test results indicate that all three systems have controls and system edits in place to identify the following scenarios:

- Gender/Procedure inconsistencies;
- Provider/Procedure inconsistencies;
- Timely filing;
- Enrollment inconsistencies;
- Invalid date of service;
- Overlapping hospital stays; and,
- Duplicate and near duplicate claims.

F. Health Insurance Portability and Accountability Act

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

EmblemHealth has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. EmblemHealth has also developed a series of privacy policies and procedures that address all requirements of the HIPAA privacy rule. EmblemHealth uses HIPAA regulations as the baseline for the creation of its policies. The plan has designated a Privacy Official who is responsible for ensuring EmblemHealth's compliance with HIPAA Privacy and Security regulations. EmblemHealth employees receive annual compliance training that encompasses HIPAA regulations.

We do not have any concerns regarding EmblemHealth's 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

EmblemHealth®

55 Water Street, New York, New York 10041-8190

September 14, 2012

[redacted]
Office of the Inspector General
U. S. Office of Personnel Management
1900 E St. NW – Suite 6400
Washington, DC 20415

Dear [redacted]

Enclosed is EmblemHealth's response to The Draft Audit Report of Information Systems General and Application Controls for EmblemHealth. The report contains six findings and twelve recommendations. We have responded to each recommendation and where applicable have already implemented new protocols and/or software to address the concerns expressed by OIG.

We ask that you review our responses to your recommendations as well as all supporting documentation before preparing the final report. It is our goal to be in full compliance with the FEHB contract at all times as we believe you will see through our immediate action to your recommendations. As you are aware, some of the recommendations will require significant testing and a long term implementation plan, however all items that could be addressed immediately have been and are already operational.

Should you have any questions regarding this response to your audit report, please feel free to contact me at [redacted]

Sincerely,

[redacted]
Director Account Management

Recommendation #1

We recommend that EmblemHealth reassess its data centers' physical access management and implement controls that will improve physical security. At a minimum, EmblemHealth should implement multi-factor authentication (e.g., cipher lock or biometric device in addition to an access card) at data center entrances.

Response #1

Dual input card readers, that require both an access card and a PIN, were installed for each entrance to the data center on September 12, 2012.

Recommendation #2

We recommend that EmblemHealth review its configuration settings for e-mail encryption to ensure that all PII is appropriately protected.

Response #2

We have implemented the SSN lexicon for ZixSelect, the tool that we use to automatically encrypt e-mail containing PHI. A single SSN will force the encryption. We acknowledge the importance of the SSN as a key element of the e-mail and that it is PII vs. PHI. We cannot move beyond that to encrypt mailing address, zip codes and/or state names because doing so would cause all e-mails with address information in the signature section to be encrypted.

Recommendation #3

We recommend EmblemHealth make the appropriate configuration changes related to the specific weaknesses identified during this audit.

Response #3

We have implemented four of the recommended configuration changes and will implement an additional two on September 15, 2012.

**** REDACTED BY OPM/OIG DUE TO THE SENSITIVE NATURE OF THE INFORMATION****

Recommendation #4

We recommend that EmblemHealth update its Mainframe Security Standard to contain a detailed secure RACF baseline configuration.

Response #4
We updated the Mainframe Security Standard to include our approved baseline configuration.

Recommendation #5
We recommend EmblemHealth implement appropriate procedures and controls to ensure that production servers are installed with appropriate patches, service packs, and hotfixes on a timely basis.
Response #5
We analyzed the server problems and determined that the tool we were using, Ecora, was not working as intended; we replaced this tool with ITCM and will monitor its effectiveness as we roll it out to the rest of the servers and databases. We have applied all of the fixes to the servers.

Recommendation #6
We recommend EmblemHealth implement appropriate procedures and controls to ensure that only current and supported versions of system software are installed on the production servers.
Response #6
Several of our legacy in-house-developed applications are dependent on an older operating system. We are looking at new architecture to replace them. In the meantime, we cannot upgrade the operating systems to supported versions because of the adverse impact that would have on our customers and our business.

Recommendation #7
We recommend EmblemHealth implement appropriate procedures and controls to ensure that anti-virus software definitions are up-to-date on all production servers.
Response #7
Information Security is now reviewing Anti-virus signatures on all servers via the EPO console on a daily basis. This task was added to the Daily Checklist.

Recommendation #8
We recommend EmblemHealth review their current system configurations to ensure that only necessary software is installed on the production servers.
Response #8
We have reviewed the Nessus reports and are in the process of identifying and removing unnecessary software. Going forward, we have a standard build for new servers to ensure that unnecessary software is not installed, and we will perform periodic reviews to ensure that we are at either emerging or current status for our operating systems.

Recommendation #9
We recommend EmblemHealth implement appropriate controls to ensure that user accounts on system databases comply with corporate password policies.
Response #9
We plan to implement Oracle's OVD solution for the provider database. This will provide single-sign-on functionality for the application users, and Active Directory will enforce compliance with corporate password policies. For the DBA accounts that cannot function

properly without direct access, we will use Oracle's native 10.g password options to enforce compliance with corporate password policies.

10/12/12 Updated Response
Passwords on the database are now in compliance with EmblemHealth's Password Standard.

Recommendation #10
We recommend EmblemHealth install and implement an automated tool to facilitate the application configuration management process.
Response #10
We are in the process of customizing [REDACTED] for EmblemHealth's environment for implementation in 2013. In the meantime, we have implemented an additional tool to replace part of our existing mainframe implementation process and continue to be very diligent about our manual procedures.

Recommendation #11
We recommend that EmblemHealth make the appropriate changes to its debarment policies and procedures to comply with all OPM's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.
Recommendation #12
We recommend that EmblemHealth make the appropriate changes to their claims processing systems to ensure FEHBP claims are processed in accordance with OPM's Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders.
Response #11 and #12:
We are in agreement with both recommendations. Based on these recommendations EmblemHealth has taken the opportunity to reinforce the policies and procedures followed in support of the Guidelines.

All of the necessary and appropriate protocols specified in the FEHB contract are now in place. These important functions have been reviewed in detail to make sure all of the specific responsibilities are appropriately applied to all FEHBP claims. Comprehensive policies and procedures have been implemented to provide a seamless member transition from debarment of health care providers by OPM.

Expanded Protocols
The review resulted in expanded policies and procedures that more effectively support the specific carrier responsibilities outlined in the Guidelines. These expanded protocols reinforce our obligations and have been successfully implemented. Also, the involved staff has been fully trained on the newly expanded policies and procedures and the existing protocols have been reinforced. Policies and procedures that have been implemented, reinforced and expanded for all FEHBP claims include the following:

- Securing the monthly OIG Debarment and Suspension lists.

- Identifying providers located in the Emblem Health FEHBP service area.

- Requesting any necessary information missing from the OIG listings so that authoritative matches can be made.

- Match all FEHBP claims of medical service and items against the continuously updated OIG Debarment and Suspension list database. The FEHBP claims are automatically matched against the database. Upon a match, one of three situation-appropriate notices containing the required information is promptly issued to enrollees who receive services from Debarred and Suspended providers. The following steps are also taken:

  - Apply a 15-day grace period following the issuance of the notice and continue to pay items and services provided during this time. A 30-grace period is applied to facility claims if the member was not properly notified of debarment before the service occurred.

  - Payments are not made for items or services rendered more than 15 days after the date of the notice to the enrollee.

  - Exceptions that are sanctioned, approved or requested by OPM will be handled as instructed.

  - Deny further payments of claims after the date of debarment and suspension and applicable grace periods.

  - All information on the debarred and suspended providers, matched claims, issued notices and related matters is available in corporate repositories accessible to Customer Service representative to respond to any inquiries from providers, FEHBP members and other involved parties.

- FEHBP Claims are rejected if the claims for items or services are furnished more than 15 days after the date of enrollee notice unless the enrollee can demonstrate that they had not received the notice when the items/services were furnished or Emblem Health knows that the enrollee was specifically aware/notified of the provider's debarment or suspension.

- Reports will continue to be issued to OIG in the prescribed format and schedule.

EmblemHealth recognizes the importance of following the Debarment and Suspension Orders Guidelines and we continue our commitment to effectively administer all of the related activities.