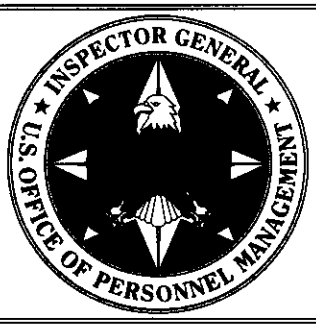

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT MEDCO HEALTH SOLUTIONS, INC.

Pharmacy Benefit Manager for:

- BlueCross BlueShield Federal Employee Program
- American Postal Workers Union Health Plan
- Government Employees Health Association
- SAMBA Federal Employee Benefit Association
- Foreign Service Benefit Plan

Report No. 1A-10-00-11-052

Date: March 14, 2012

--CAUTION--

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM

MEDCO HEALTH SOLUTIONS, INC.

Pharmacy Benefit Manager For:

BLUECROSS BLUESHIELD ASSOCIATION
CONTRACT 1039; CODES 104, 105, 111, 112
AMERICAN POSTAL WORKERS UNION HEALTH PLAN
CONTRACT 1370; CODES 471, 472, 474, 475
GOVERNMENT EMPLOYEES HEALTH ASSOCIATION
CONTRACT 1063; CODES 311, 312, 314, 315
SAMBA FEDERAL EMPLOYEE BENEFIT ASSOCIATION
CONTRACT 1074; CODES 441, 442, 444, 445
FOREIGN SERVICE BENEFIT PLAN
CONTRACT 1062; CODES 401, 402

Report No. 1A-10-00-11-052

Date: 03/14/12

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM

MEDCO HEALTH SOLUTIONS, INC.

Pharmacy Benefit Manager For:

BLUECROSS BLUESHIELD ASSOCIATION
CONTRACT 1039; CODES 104, 105, 111, 112
AMERICAN POSTAL WORKERS UNION HEALTH PLAN
CONTRACT 1370; CODES 471, 472, 474, 475
GOVERNMENT EMPLOYEES HEALTH ASSOCIATION
CONTRACT 1063; CODES 311, 312, 314, 315
SAMBA FEDERAL EMPLOYEE BENEFIT ASSOCIATION
CONTRACT 1074; CODES 441, 442, 444, 445
FOREIGN SERVICE BENEFIT PLAN
CONTRACT 1062; CODES 401, 402

Report No. 1A-10-00-11-052

Date: 03/14/12

This final report discusses the results of our audit of general and application controls over the information systems at Medco Health Solutions, Inc.

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for Medco, 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
Medco has established a comprehensive series of IT policies and procedures to create an awareness of IT security at the Plan. We also verified that Medco has adequate human resources policies related to the security aspects of hiring, training, transferring, and terminating employees.

Access Controls
We found that Medco has implemented numerous physical controls to prevent unauthorized access to its facilities, as well as logical controls to prevent unauthorized access to its information systems. However, we found that Medco's data center does not require two-factor authentication for access and that there is no documented review of system administrator activity.

Configuration Management
Medco has developed formal policies and procedures providing guidance to ensure that system software is appropriately configured and updated, controlling system software configuration changes, and monitoring configuration through vulnerability scanning.

Contingency Planning
We reviewed Medco's business continuity plans and concluded that they contained the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed, updated, and tested on a periodic basis.

Claims Adjudication
Medco has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we found that Medco does not use the Office of Personnel Management (OPM) debarred provider listing to update its master pharmacy database. We also recommend that Medco 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 Medco is not in compliance with the HIPAA security and privacy regulations.

Contents

I. Introduction

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

The audit was conducted pursuant to applicable FEHBP contracts; 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.

Medco is the pharmacy benefit manager responsible for processing prescription drug claims on behalf of the following FEHBP insurance carriers:

- Blue Cross Blue Shield (BCBS) Federal Employee Program - contract CS 1039;
- American Postal Workers Union Health Plan - contract CS 1370;
- Government Employees Health Association (GEHA) - contract CS 1063;
- SAMBA Federal Employee Benefit Association - contract CS 1074; and
- Foreign Service Benefit Plan (FSBP) - contract CS 1062.

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

All Medco 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 Medco'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 Medco'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 Medco'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 Medco'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 scope of this audit centered on the information systems used by Medco to process prescription benefit claims for FEHBP members. The business processes reviewed are primarily located in Medco's Franklin Lakes, New Jersey facility.

The on-site portion of this audit was performed in June and July of 2011. We completed additional audit work before and after the on-site visits 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 Medco as of September 9, 2011.

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

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

Various laws, regulations, and industry standards were used as a guide to evaluating Medco'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 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 Revision 1, 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, we performed tests to determine whether Medco's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Medco 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 Medco's overall IT security controls. We evaluated Medco's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Medco has implemented a series of formal policies and procedures that comprise a comprehensive security management program. Medco's security management program is developed, maintained, and annually reviewed by Medco Global Security; their responsibilities include creating policies to protect against threats or improper use of protected health information, HIPAA compliance, and to provide central governance and coordination. Medco has also developed a thorough risk management methodology, and has procedures to document, track, and alleviate or accept identified risks. We also reviewed Medco's human resources policies and procedures related to the security aspects of hiring, training, transferring, and terminating employees.

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

B. Access Controls

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

We examined the physical access controls of a Medco office complex and a separate data center facility, both in New Jersey. We also examined the logical controls protecting sensitive data in Medco's network environment and claims processing related applications.

The access controls observed during this audit included, but were not limited to:

- Procedures for granting and revoking physical access privileges to the data centers;
- Adequate intrusion detection and incident response capabilities;
- Controls over firewall configuration and security;
- Use of software tools to monitor and filter e-mail and Internet activity; and
- Strict identification and authentication requirements.

However, we did note several opportunities for improvement related to Medco's physical and logical access controls.

a) Data Center Access Controls

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

- [redacted]

[redacted]

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to Medco's data center and the sensitive resources and confidential data it contains. NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 1

We recommend that Medco improve the physical access controls at its data center. [redacted]

Medco Response:

"Medco appreciates the safety concerns raised regarding the access controls into the Data Center space. [redacted] ***Due to the small number of personnel who have access to the building and the computer room, as well as the security controls in place, the risk of "piggybacking" is controlled."***

OIG Reply:

[redacted]ls are the most basic form of physical access controls that are implemented at nearly all data centers of health insurance companies visited by the OIG. We believe that the controls at Medco's data center are substantially

weaker than industry standards, and we continue to recommend that Medco improve the physical access controls at its data center.

b) System Administrator Review

The Medco claims processing system resides on an [redacted] that utilizes the [redacted] tool to provide access control and auditing functionality for the operating system. [redacted] produces a variety of logs and reports, such as a daily activity report and a daily violation report, which are routinely reviewed by system administrators for suspicious activity.

Medco informed us that the activity of the system administrators is reviewed on a quarterly basis by an individual without administrator access. However, Medco was unable to produce any evidence indicating that this review takes place. Medco explained that a report detailing the system administrators' activity is placed in a shared folder on Medco's network and the individual responsible for reviewing these reports receives an email stating that the report is available. The individual reviews the activity, but does not document that the review has been conducted.

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 reviews could allow unintended or malicious activity to go undetected and increase system vulnerability.

Recommendation 2

We recommend that Medco maintain documentation indicating that system administrator activity is reviewed on a routine basis.

Medco Response:

"Medco notes that the [standard operating procedure] SOP for management of the privileged accounts on the [redacted] has been updated to include an explicit requirement for periodic review and signoff on the reports at the management level."

OIG Reply:

As part of the audit resolution process, we recommend that Medco provide OPM's Healthcare and Insurance Office (HIO) with a copy of the updated SOP and evidence that a management review of privileged accounts is occurring on a regular basis.

C. Configuration Management

Medco's claims processing applications are housed on a [redacted] with a [redacted] operating platform that is protected with [redacted] We evaluated Medco's management of the [redacted] configuration and determined that the following controls were in place:

- Policies and procedures for ensuring that operating platforms are securely configured;

- Controls for securely managing changes to the operating platform and claims processing application;
- Controls for monitoring privileged user activity on the operating platform;
- Procedures for routinely updating and patching the operating platforms; and
- Procedures for monitoring configuration through vulnerability scans.

Nothing came to our attention to indicate that Medco does not have adequate controls related to configuration management.

D. Contingency Planning

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

- Business continuity plans for several business units, data center operations, pharmacies, and customer service;
- Business continuity plans for the check writing facility;
- Disaster recovery plan for the claims processing system;
- Disaster recovery plan tests conducted in conjunction with the recovery site; and
- Emergency response procedures and training.

We determined that the service continuity documentation reviewed contained the critical elements suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems." Medco 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 Medco 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 Medco's claims adjudication process.

Application Configuration Management

The OIG evaluated the policies and procedures governing software development and change control of Medco's claims processing applications.

Medco has extensive policies and procedures related to application configuration management. Medco has adopted a traditional systems development lifecycle methodology that IT personnel follow during routine software modifications. The following controls related to testing and approvals of software modifications were observed:

- Medco 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
- Medco uses an automated tool to move the code between software libraries and ensure adequate segregation of duties.

Claims Processing System

We evaluated the input, processing, and output controls associated with Medco's claims adjudication systems. We determined that Medco 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 contracted mail room are tracked to ensure timely processing (aging reports).

Debarment

Medco employees download the Health and Human Services (HHS) OIG debarment list every month and compare it to the Medco pharmacy master database. Any debarred pharmacies that appear in Medco's pharmacy master database are promptly removed. Removing the pharmacy from the master database prevents claims submitted by that pharmacy from processing successfully during the claims adjudication process. However, Medco's procedures only consider the HHS debarment list and not the debarred provider listing maintained by the OPM OIG. Failure to update the debarment database with the OPM OIG exclusion list increases the risk that claims are being paid to providers that are debarred by OPM but not by HHS.

Recommendation 3

We recommend that Medco implement procedures to routinely update its pharmacy master database with OPM OIG's debarred provider listing.

Note: this recommendation does not apply to Medco's BCBS contract, as Medco does not process retail pharmacy claims for BCBS.

Medco Response:

"Medco notes that in addition to screening against the HHS OIG list referenced in the audit finding, Medco also checks the Excluded Parties List System (EPLS) maintained by the General Services Administration. It is Medco's understanding that all executive agencies of the federal government provide information relating to exclusion, debarment or suspension for inclusion on the EPLS. Medco notes that OPM is included in the list of agencies in EPLS. Medco believes that by screening against the EPLS, Medco meets OPMs requirements. Please refer to the attached monthly review memo (Attachment 1) that was provided to OPM OIG. The memo notes that the General Services Administration list is checked monthly."

OIG Reply:

Although the EPLS contains much of the same data as the OPM OIG's debarred provider listing, the EPLS is not acceptable for use by FEHBP contractors when making decisions that impact FEHBP members.

The EPLS is a public site that contains limited data regarding OPM suspended and debarred providers. It does not provide FEHBP contractors with all the data elements needed to make decisions regarding payment/nonpayment of FEHBP claims.

OPM requires its contracted insurance carriers to process all FEHBP claims against a sanctions database that is updated monthly with OPM's debarment and suspension data. OPM uses a secure webpage to electronically disseminate debarment/suspension/termination information to FEHBP carriers, and this webpage is OIG's exclusive method for distributing debarment and suspension data to FEHBP carriers.

OPM may also post messages on the secure webpage concerning debarment and suspension-related operational matters, as well as corrections to prior data. Therefore, it is important that contractors visit the webpage periodically between the regular postings.

We continue to recommend that Medco implement procedures to routinely update its pharmacy master database with OPM OIG's debarred provider listing.

Special Investigations and Fraud

The OIG evaluated the Medco policies and procedures governing special investigations and fraud. We determined that Medco has substantial policies and procedures in place to detect, manage, and report fraud. There were no opportunities for improvement noted during our review.

Application Controls Testing

We conducted a testing exercise on Medco's claims adjudication applications to validate the systems' claims processing controls. The exercise involved developing test claims designed with inherent flaws and evaluating the manner in which Medco's systems processed the claims.

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

a) Invalid Prescriber

Medco's claims processing applications do not have the ability to detect prescriptions containing invalid prescriber identifiers (identifiers not assigned to an active licensed provider).

We submitted test claims for prescriptions written by non-existent prescribers. The National Provider Identifier (NPI) numbers for these providers had a valid structure (last number was a correctly calculated check digit), but they were not assigned to a valid prescribing doctor. We also submitted test claims that contained an NPI number without an accurate check digit.

Medco's system appropriately suspended the claims containing NPI numbers with incorrect check digits. However, all claims with an accurate check digit were processed and paid without encountering any system edits or suspensions, even though the NPI numbers were not assigned to a valid prescriber.

Although retail pharmacies should validate prescribers before submitting a prescription claim, we believe that it is the responsibility of Medco to verify that prescriptions are written by valid prescribers prior to authorizing a claim for payment. A centralized method of verifying NPI numbers would be more efficient than relying on the efforts of various pharmacies whose processes Medco cannot control, and would also provide Medco assurance all claims are verified with consistent quality.

The weakness in the current control structure could be exploited by individuals submitting fraudulent prescriptions from an invalid prescriber. If the pharmacist filling the prescription does not detect the anomaly, Medco will pay benefits for the claim and the individual will gain unauthorized access to prescription drugs. This risk of fraudulent activity is even greater for mail order claims, where Medco is also the pharmacy filling the prescription and there is no second level of control added from a retail pharmacist. Medco confirmed that the only validation it does of prescriber identifiers on both retail and mail order claims is to validate the NPI check digit and verify that the prescriber is not on the OIG debarred provider list.

Recommendation 4

We recommend that Medco make the appropriate system modifications in order to detect claims being processed with invalid prescriber identifiers. Prescriber identifiers include: NPI, Drug Enforcement Agency (DEA) number, Unique Provider Identification Number (UPIN), or state license number.

Claims that do not contain a valid prescriber identifier should not be rejected at the point of sale, but Medco should attempt to retroactively obtain a valid identifier for these claims. When unable to obtain a valid prescriber identifier, Medco should pursue reimbursement from the pharmacy or member that submitted the claim. All funds recovered should be returned to OPM via the FEHBP carriers.

Medco Response:

"Medco notes that each plan determines the edits that are in place for that plan. Currently, no plan has requested the type of edit described above. Moreover, the recommendation, if implemented by the plans, will result in patients not obtaining drugs from prescribers who are licensed prescribers. This is because not all prescribers have NPI numbers at this time. Furthermore, while the above recommendation directs Medco to the CMS file, it does not take into account that the CMS file (1) is furnished only every 4-6 weeks, and

thus does not provide current information; (2) does not require that the prescriber register using the exact name that might be on the patient's prescription; (3) does not provide all the addresses at which a prescriber practices (it only has one location); (4) does not provide termination dates for NPI numbers; and (5) does not provide clear practice area information. Thus, relying on this database would result in legitimate claims being rejected at point of sale. The recommendation also does not take into account instances where, for example, a vaccine is administered at a pharmacy so the NPI number for the prescriber could be the same as the NPI of the pharmacy.

For 2012, CMS continues to instruct plans not to reject a claim at point of sale for invalid NPI numbers, so OPM's recommendation runs counter to CMS's requirement and will result in patients not receiving drugs to which they are entitled that are prescribed by licensed prescribers. However, if the plans choose to implement this recommendation, Medco will implement it."

Additional comments from Medco's FEHBP clients:

GEHA: "We concur with Medco's response and would not want to implement an edit that would prevent enrollees from receiving medications to which they are entitled."

OIG Reply:

Medco is correct that for 2012, the Department of Health and Human Services (HHS) Center for Medicare and Medicaid Services (CMS) instructed plans not to reject Medicare Part D claims at a point of sale for invalid NPI numbers. The 2012 CMS Final Call Letter to all Medicare prescription drug plan sponsors states that "sponsors should not reject a pharmacy claim solely on the basis of an invalid prescriber identifier unless the issue can be resolved at point-of-sale." However, this same document referenced by Medco also states that Prescription Drug Event (PDE) records submitted to CMS must contain one of four types of prescriber identifiers (including NPI), and that plans must ensure that these identifiers are active and valid. Therefore, if a valid prescriber ID is not included on the Part D claim, the sponsor must retroactively acquire a valid ID before submitting the PDE to CMS. The Call Letter also states that CMS is considering limiting acceptable prescriber identifiers to NPIs in 2013.

Furthermore, an audit report from the Inspector General at HHS recommended that Part D plans "institute procedures to (1) identify invalid identifiers in the prescriber identifier field on Part D drug claims and (2) flag for review Part D drug claims that contain invalid identifiers in the prescriber identifier field[1]."

Our draft audit report recommended that Medco make the appropriate system modifications in order to detect claims being processed with invalid NPIs. In order to be consistent with HHS, we modified the recommendation so that it does not explicitly require NPI numbers to be validated. Rather, we recommend that Medco's validation of the

[1] HHS OIG Audit Report "Invalid Prescriber Identifiers on Medicare Part D Drug Claims." http://oig.hhs.gov/oei/reports/oei-03-09-00140.pdf (page 4/25)

prescriber can be done by any of the four valid prescriber identifiers allowed by HHS (DEA, NPI, UPIN, or state license numbers). We also recommend that claims should not be rejected at the point of sale for missing a valid prescriber identifier, but Medco should attempt to retroactively obtain a valid identifier for these claims. When unable to obtain a valid prescriber identifier, Medco should pursue reimbursement from the pharmacy or member that submitted the claim.

b) Expired Prescriptions

Medco's claims processing applications do not have the controls in place to accurately process claims based on state laws for expired prescriptions.

We submitted several test claims for prescriptions where the fill date was between 5 months and 2 years after the prescription was written. Medco's system denied all claims that were filled more than one year after the issue date, and paid all claims that were less than one year old. However, several U.S. states and territories have prescription laws that do not conform to the one year expiration timeline, and Medco is not accurately processing claims from these areas.

For example, prescriptions from Puerto Rico expire after 6 months, but Medco's system would inappropriately process and pay claims from there that were between 6 and 12 months old.

In addition, prescriptions from the states listed below expire at a point in time greater than one year. Medco's system inappropriately denies claims for prescriptions older than one year but within the legal limit for that area. This practice could prevent FEHB members from receiving medication that they are legally entitled to.

States where prescriptions expire later than one year:

- Alabama (no expiration)
- California (no expiration)
- Connecticut (no expiration)
- District of Columbia (no expiration)
- Georgia (no expiration)
- Idaho (15 months)
- Iowa (18 months)
- Maine (15 months)
- Massachusetts (no expiration)
- New Mexico (no expiration)
- New York (no expiration)
- Oregon (24 months)
- South Carolina (24 months)
- South Dakota (no expiration)
- Wyoming (24 months)

Recommendation 5

We recommend that Medco make the appropriate system modifications to alert pharmacies in Puerto Rico when they attempt to submit claims for expired prescriptions (those more than six months old).

Medco Response:

"Medco notes that effective November 2011, the edit that previously allowed claims at Puerto Rico pharmacies to be filled up to 12 months after the prescription was written was changed in our system. Going forward, any claims submitted from a Puerto Rico pharmacy will now reject if the fill date would be more than 6 months from the date on which the prescription was written. With regard to mail service, as per the case law from 2000, the US Court of Appeals for the First Circuit affirmed a district court decision that the Pharmacy Act of PR is not applicable to mail-order services based outside of Puerto Rico that supply pharmaceuticals to customers within Puerto Rico."

OIG Reply:

As part of the audit resolution process, we recommend that Medco provide OPM's HIO with evidence that its systems have been modified to alert pharmacies in Puerto Rico when they attempt to submit claims for expired prescriptions.

Recommendation 6

We recommend that Medco make the appropriate system modifications to approve and pay claims greater than one year old if allowed by the prescription laws in that state.

Note: this recommendation does not apply to Medco's BCBS contract, as Medco does not process retail pharmacy claims for BCBS.

Medco Response:

"First, pharmacy regulations in the states in which the back end pharmacies are located do not allow a prescription that is over one year from when it is written to be transferred into the pharmacy. Thus, Medco is adhering to pharmacy law. For retail pharmacies, plans have the ability to determine coverage for a prescription, even if the coverage limits are more stringent than provided by pharmacy law. So, for example, pharmacy law might allow a member to obtain a refill of a prescription a few days after obtaining the original fill; however, the plan, as a matter of plan design, might use a refill too soon edit to prevent that refill from being paid for by the plan. Similarly, pharmacy law would allow any valid prescription to be filled, but the plan design might not cover a particular drug if it were off the formulary; or required prior authorization. The same logic applies for payment of claims for prescriptions that are over a year old. This might be allowed by pharmacy law in certain states; however, it is generally not contemplated by our plans.

If the plans decide to implement this recommendation and allow prescriptions over a year old to be filled at retail pharmacies, Medco will implement the request of the plans."

Additional comments from Medco's FEHBP clients:

GEHA: "Since the majority of the Plan's prescription spend is through mail order, we would need to maintain a standardized one year renewal period for all prescriptions."

FSBP: ***We wish "to keep within our contract and allow only one (1) year for prescription refills."***

OIG Reply:

We acknowledge the fact that individual plans maintain the right to set coverage limits that are more stringent than state pharmacy laws, and that GEHA and FSBP have done so. We recommend that APWU and SAMBA inform Medco whether they wish to continue the one-year expiration limit or to allow claims to adjudicate based on prescription expiration dates outlined in state laws.

F. Health Insurance Portability and Accountability Act

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

Medco has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. Medco has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. Each line of business, subsidiary, and some departments have designated a Privacy Official who has the responsibility of ensuring their area is compliant with HIPAA Privacy and Medco's HIPAA Privacy policies. Medco 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 Medco 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], IT Auditor
- [redacted] Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

Appendix

medco

Medco Health Solutions, Inc.
100 Parsons Pond Drive
Franklin Lakes, NJ 07417

tel 201 269 3400
www.medco.com

December 1, 2011

[redacted]
Office of Personnel Management / Office of the Inspector General
1900 E Street NW
Room 6400 (OIG)
Washington, D.C. 20415

RE: Medco Response to OPM OIG Draft Audit Report

Dear [redacted],

Medco has received the Draft Report of the Audit of Information Systems General and Application Controls at Medco Health Solutions. Please find the enclosed responses to the recommendations outlined in the draft report. In addition, responses from each of the plans have been included as attachments.

Should you have any questions, please feel free to contact me at [redacted]

Sincerely,

[redacted]
Senior Client Auditor, Client Audit Services

CC: [redacted], Medco
[redacted], Medco
[redacted], Medco

Medco Health Solutions, Inc.
100 Parsons Pond Drive
Franklin Lakes, NJ 07417

tel 201 269 3400
www.medco.com

medco

Medco has received the Draft Report of the Audit of Information Systems General and Application Controls at Medco Health Solutions. There are six categories where OPM OIG has noted recommendations to Medco. The following Medco responses address those recommendations.

Access Controls

Data Center Access Controls: Recommendation 1
We recommend that Medco improve the physical access controls at its data center. [redacted]

Medco Response:
Medco appreciates the safety concerns raised regarding the access controls into the Data Center space. [redacted] Due to the small number of personnel who have access to the building and the computer room, as well as the security controls in place, the risk of "piggybacking" is controlled.

System Administrator Review: Recommendation 2
We recommend that Medco maintain documentation indicating that system administrator activity is reviewed on a routine basis.

Medco Response:
Medco notes that the SOP for management of the privileged accounts on the mainframe has been updated to include an explicit requirement for periodic review and signoff on the reports at the management level.

Claims Adjudication

Debarment: Recommendation 3
We recommend that Medco implement procedures to routinely update its pharmacy master database with OPM OIG's debarred provider listing.

Medco Health Solutions, Inc.
100 Parsons Pond Drive
Franklin Lakes, NJ 07417

tel 201 269 3400
www.medco.com

Medco Response:
Medco notes that in addition to screening against the HHS OIG list referenced in the audit finding, Medco also checks the Excluded Parties List System (EPLS) maintained by the General Services Administration. It is Medco's understanding that all executive agencies of the federal government provide information relating to exclusion, debarment or suspension for inclusion on the EPLS. Medco notes that OPM is included in the list of agencies in EPLS. Medco believes that by screening against the EPLS, Medco meets OPMs requirements. Please refer to the attached monthly review memo (Attachment 1) that was provided to OPM OIG. The memo notes that the General Services Administration list is checked monthly.

Invalid Prescriber: Recommendation 4
Medco's claims processing applications do not have the ability to detect prescriptions containing invalid (non-existent) prescribers. We submitted test claims for prescriptions written by non-existent prescribers. The National Provider Identifier (NPI) numbers for these providers had a valid structure (last number was a correctly calculated check digit), but they were not assigned to a valid prescribing doctor. We also submitted test claims that contained a NPI number without an accurate check digit. Medco's system appropriately suspended the claims containing NPI numbers with incorrect check digits. However, all claims with an accurate check digit were processed and paid without encountering any system edits or suspensions, even though the NPI numbers were not assigned to a valid prescriber.

Although retail pharmacies should validate prescribers before submitting a prescription claim, we believe that it is the responsibility of Medco to verify that prescriptions are written by valid prescribers prior to authorizing a claim for payment. A centralized method of verifying NPI numbers would be more efficient than relying on the efforts of various pharmacies whose processes Medco cannot control, and would also provide Medco assurance all claims are verified with consistent quality. The weakness in the current control structure could be exploited by individuals submitting fraudulent prescriptions from an invalid prescriber. If the pharmacist filling the prescription does not detect the anomaly, Medco will pay benefits for the claim and the individual will gain unauthorized access to prescription drugs.

A current database of valid NPI numbers is actively maintained by the Centers for Medicare and Medicaid Services. Medco could leverage this resource to make improvements to its claims adjudication process.

We recommend that Medco make the appropriate system modifications in order to detect claims being processed with invalid NPIs.

Medco Response:
Medco notes that each plan determines the edits that are in place for that plan. Currently, no plan has requested the type of edit described above. Moreover, the recommendation, if implemented by the plans, will result in patients not obtaining drugs from prescribers who are licensed prescribers. This is because not all prescribers have NPI numbers at this time. Furthermore,

Medco Health Solutions, Inc.
100 Parsons Pond Drive
Franklin Lakes, NJ 07417

tel 201 269 3400
www.medco.com

medco

while the above recommendation directs Medco to the CMS file, it does not take into account that the CMS file (1) is furnished only every 4-6 weeks, and thus does not provide current information; (2) does not require that the prescriber register using the exact name that might be on the patient's prescription; (3) does not provide all the addresses at which a prescriber practices (it only has one location); (4) does not provide termination dates for NPI numbers; and (5) does not provide clear practice area information. Thus, relying on this database would result in legitimate claims being rejected at point of sale. The recommendation also does not take into account instances where, for example, a vaccine is administered at a pharmacy so the NPI number for the prescriber could be the same as the NPI of the pharmacy.

For 2012, CMS continues to instruct plans not to reject a claim at point of sale for invalid NPI numbers, so OPM's recommendation runs counter to CMS's requirement and will result in patients not receiving drugs to which they are entitled that are prescribed by licensed prescribers. However, if the plans choose to implement this recommendation, Medco will implement it.

Expired Prescriptions: Recommendation 5
We recommend that Medco make the appropriate system modifications to alert pharmacies in Puerto Rico when they attempt to submit claims for expired prescriptions (those more than six months old).

Medco Response:
Medco notes that effective November 2011, the edit that previously allowed claims at Puerto Rico pharmacies to be filled up to 12 months after the prescription was written was changed in our system. Going forward, any claims submitted from a Puerto Rico pharmacy will now reject if the fill date would be more than 6 months from the date on which the prescription was written. With regard to mail service, as per the case law from 2000, the US Court of Appeals for the First Circuit affirmed a district court decision that the Pharmacy Act of PR is not applicable to mail-order services based outside of Puerto Rico that supply pharmaceuticals to customers within Puerto Rico.

Expired Prescriptions: Recommendation 6
We recommend that Medco make the appropriate system modifications to approve and pay claims greater than one year old if allowed by the prescription laws in that state.

Medco Response:
First, pharmacy regulations in the states in which the back end pharmacies are located do not allow a prescription that is over one year from when it is written to be transferred into the pharmacy. Thus, Medco is adhering to pharmacy law. For retail pharmacies, plans have the ability to determine coverage for a prescription, even if the coverage limits are more stringent than provided by pharmacy law. So, for example, pharmacy law might allow a member to obtain a refill of a prescription a few days after obtaining the original fill; however, the plan, as a matter of plan design, might use a refill too soon edit to prevent that refill from being paid for by the

Medco Health Solutions, Inc.
100 Parsons Pond Drive
Franklin Lakes, NJ 07417

tel 201 269 3400
www.medco.com

plan. Similarly, pharmacy law would allow any valid prescription to be filled, but the plan design might not cover a particular drug if it were off the formulary; or required prior authorization. The same logic applies for payment of claims for prescriptions that are over a year old. This might be allowed by pharmacy law in certain states; however, it is generally not contemplated by our plans.

If the plans decide to implement this recommendation and allow prescriptions over a year old to be filled at retail pharmacies, Medco will implement the request of the plans.