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

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT WELLMARK INC. BLUE CROSS AND BLUE SHIELD

Report Number 1A-10-31-15-058
June 17, 2016

-- CAUTION --

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Wellmark Inc. Blue Cross and Blue Shield

Report No. 1A-10-31-15-058 **June 17, 2016**

Why Did We Conduct the Audit?

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of Federal Employees Health Benefits Plan (FEHBP) data processed and maintained in the Wellmark Inc. Blue Cross and Blue Shield (Wellmark) information technology (IT) environment.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit identified several minor control weaknesses where Wellmark could implement additional IT security controls or improve upon existing controls. However, we do not believe that these issues are indicative of systemic control problems, and we conclude that Wellmark generally has a comprehensive and mature IT security program in place. Specifically, we determined that:

- Wellmark has established an adequate security management program.
- Wellmark has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information.
- Wellmark has implemented an incident response and network security program. However, Wellmark does not have an adequate methodology in place to ensure that unsupported or out-of-date software is not utilized.
- Wellmark has implemented a configuration management program with documented program and change management policies including baseline standards for operating platforms.
- Wellmark has established a risk based contingency planning program including multiple plans and regular testing of its plans.
- The systems used to process FEHBP claims for Wellmark had edits in place to catch many of our test claims, but could potentially benefit from additional controls related to medical edits and patient history.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
the Association	**Blue Cross Blue Shield Association**
BCBS	**Blue Cross Blue Shield**
BCBSA	**Blue Cross Blue Shield Association**
CFR	**Code of Federal Regulations**
DO	**Director's Office**
FEHBP	**Federal Employees Health Benefits Plan**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Systems Control Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
The Plan	**Wellmark Inc. Blue Cross and Blue Shield**
Wellmark	**Wellmark Inc. Blue Cross and Blue Shield**

TABLE OF CONTENTS

I. BACKGROUND

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

The audit was conducted pursuant to FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act (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 Blue Cross Blue Shield Association (the Association), on behalf of participating Blue Cross and Blue Shield (BCBS) plans, has entered into a Government-wide Service Benefit Plan contract (CS 1039) with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS plans throughout the United States, such as Wellmark, to process the health benefit claims of its federal subscribers.

The Association has established a Federal Employee Program (FEP[1]) Director's Office (DO) in Washington, D.C. to provide centralized management for the Service Benefit Plan. The FEP DO coordinates the administration of the contract with the Association, member BCBS plans, and OPM.

All Wellmark 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.

[1] Throughout this report, when we refer to "FEP", we are referring to the Service Benefit Plan lines of business at Wellmark. When we refer to the "FEHBP", we are referring to the program that provides health benefits to federal employees.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

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

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to Wellmark's claims processing systems.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of Wellmark's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of Wellmark'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 Wellmark to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. Wellmark processes FEP claims through both a local claims system maintained by Wellmark and through FEP Direct, the Association's nation-wide claims adjudication system. The business processes reviewed are primarily located in Wellmark's Des Moines, Iowa facility.

The on-site portion of this audit was performed in July and August of 2015. 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 Wellmark as of November 2015.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Wellmark. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps but we determined that it was adequate to achieve our audit objectives.

However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review we:

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

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

- Title 48 of the Code of Federal Regulations;
- U.S. 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;
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether Wellmark's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Wellmark was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

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

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

Wellmark has implemented a series of formal policies and procedures that comprise its security management program. Wellmark has also developed an adequate risk management methodology that allows it to document, track, and mitigate or accept identified risks in a timely manner. We also reviewed Wellmark's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding security management.

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 Wellmark's facilities and data centers located in Des Moines and [redacted], as well as a contractor data center located in [redacted]. We also examined the logical controls protecting sensitive data in Wellmark's network environment and applications.

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

- Procedures for appropriately granting physical access to facilities and data centers;
- Strong environmental controls over the data centers; and
- Controls to monitor and filter email and Internet activity.

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

1) Facility Access Controls

Wellmark facilities contain turnstile access controls with electronic access card readers to control physical access. However, there is one auxiliary entrance at the main facility that only requires badge access without any piggybacking detection or prevention controls. The doorway leads to the claims scanning area that is used for the temporary storage of unsecured claims.

We expect all FEHBP contractors to have some form of technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, etc.) at all access points.

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data. NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 1

We recommend that Wellmark implement some form of piggybacking controls at all facility entry points.

Wellmark Response:

"[Wellmark Inc. Blue Cross and Blue Shield (The Plan)] agrees with the recommendation. Implementation of piggybacking controls at the door in question will be completed by March 18, 2016."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that Wellmark has implemented the recommended piggybacking controls; no further action is required.

2) Physical Access Recertification

Wellmark's process for removing physical access to its facilities for terminated employees requires managers to notify the physical security department with the individual's expected termination date. On a monthly basis, lists of all employees with active access to secure areas are sent to the manager responsible for those areas for validation. The managers are required to respond regardless of whether there is a discrepancy in the list or not.

However, our test work determined that Wellmark's existing procedures to remove terminated individuals from access lists could be improved. We compared a list of employees listed as having access to facilities to a list of employees that were terminated in the last year, and discovered that multiple employees remained on the access lists well after their termination dates. Our test work did not identify the cause of this problem, but did reveal that Wellmark's procedures for initial access removal and also the subsequent validation process are not fully successful. Wellmark should analyze this process further in an effort to determine the root cause of the issues we identified.

NIST SP 800-53, Revision 4, states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

Recommendation 2

We recommend Wellmark analyze its process for routinely auditing all active access lists to determine why individuals are remaining on access lists well after their termination dates. Subsequent action should be taken to address any problems identified in this analysis.

Wellmark Response:

"The Plan agrees with the recommendation. The Standard Operating Procedures related to terminations have been enhanced."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that Wellmark has enhanced their procedures for auditing physical access lists; no further action is required.

Wellmark has enhanced its physical access controls to adequately secure its facilities and resources.

3) Data Center Access Controls

The main entrance to the raised floor area of Wellmark's primary data center is protected by a door that requires three-factor authentication to open. However, an auxiliary door to the raised floor area requires only single-factor authentication via electronic access card. The space accessible by this auxiliary door is segregated from the rest of the data center by a chain link fence, but the area does contain servers that process sensitive data, and it also has logical and physical network connections to the main data center area.

We expect all FEHBP contractors to require multifactor authentication (e.g., cipher lock or biometric device in addition to an access card) at all data center entrances, and some form of technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, two door "man traps", etc.).

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data.

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

Recommendation 3

We recommend Wellmark reassess the physical access controls at its primary data center and implement multi-factor authentication and piggybacking prevention controls at all entrances.

Wellmark Response:

"The Plan agrees with the recommendation. Multi-factor authentication has been implemented at the primary data center and piggybacking prevention will be implemented by March 18, 2016."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that Wellmark has implemented the recommended physical access controls; no further action is required.

C. Network Security

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

We evaluated Wellmark's incident response and network security program and reviewed the results of historical automated vulnerability scans performed by Wellmark. Additionally, we worked with Wellmark employees to independently perform automated vulnerability scans on a sample of servers, databases, and user workstations.

1) Vulnerabilities Identified in Automated Scans

The specific vulnerabilities that we identified in our scans will not be detailed in this report, but the issues we identified are summarized at a high level below.

System Patching

Wellmark has documented patch management policies and procedures. However, our scans detected several instances where computer servers were missing at least one critical patch or service pack older than the grace period allowed by Wellmark's policy. Wellmark did provide evidence indicating that it was previously aware of these missing patches. However, Wellmark does not have a process to formally document its acceptance of risk for non-compliant systems. Such a process would allow Wellmark to better track and periodically reassess systems with missing patches, decreasing the risk of unpatched vulnerabilities being exploited.

NIST SP 800-53, Revision 4, states that the organization must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly.

Recommendation 4

We recommend Wellmark update its patch management policy to require the formal acceptance of risk for any systems that are not compliant with the policy. This documentation should be regularly reviewed to determine whether there is an ongoing need to keep these patches uninstalled.

Wellmark Response:

"The Plan agrees with the recommendation. The patch management policy has been enhanced to include a formal patch management exception analysis, documentation, approval, tracking, and periodic review."

Wellmark has enhanced its patch management policy to include exception tracking and approval.

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that Wellmark has sufficiently updated its patch management policy; no further action is required.

Noncurrent Software

The results of the vulnerability scans indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities. Wellmark did provide evidence indicating that it was previously aware of the unsupported software. However, no evidence has been provided that Wellmark has documented a formal risk acceptance or that it had immediate plans to phase out this software.

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

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

Recommendation 5

We recommend that Wellmark implement a formal software lifecycle management methodology to ensure that only current and supported versions of system software are installed on the production servers.

Wellmark Response:

"The Plan agrees with the recommendation. By May 15, 2016, the existing formal technology standard will be enhanced to define that only supported versions of system software are installed on production servers and a formal variance process will be developed that includes the exception documentation, approval, and periodic review. The identified noncurrent software applications will be removed, upgraded, or have a documented variance by April 1, 2016."

OIG Comment:

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

D. Configuration Management

Configuration management consists of the policies and procedures used to ensure systems are configured according to approved risk-based configuration controls.

We evaluated Wellmark's configuration management program as it relates to the operating systems that support the processing of FEP claims, and determined that the following controls were in place:

- Documented corporate configuration policy;
- Documented baseline configurations for all operating systems; and
- Thorough change management procedures for system software and hardware.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding operating system configuration management.

E. Contingency Planning

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

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

Wellmark has documented contingency plans that are tested regularly.

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34, Revision 1. Wellmark 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.

Wellmark routinely tests both the disaster recovery and business continuity plans. The testing includes various functional and table top tests that result in recommendations for improving the plans.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding the contingency planning process.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting Wellmark's claims adjudication process. Wellmark processes all FEP claims through its local claims processing system and then through the Association's FEP Direct nationwide claims adjudication system.

1) Application Configuration Management

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

Wellmark has documented system development life cycle procedures that IT personnel follow during routine software modifications. All changes require approval and undergo testing prior to migration to the production environment.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding the application configuration management process.

2) Claims Processing System

We evaluated the policies and procedures governing input, processing, and output controls associated with Wellmark's claims processing system.

Wellmark has documented procedures for its claims adjudication process to control the proper input, processing, and output of FEHBP claims. Additionally, there is an extensive quality assurance process in place to ensure accuracy at each step of claims processing.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding the claims processing system.

3) Debarment

Wellmark has adequate procedures for updating its claims system with debarred provider information. Wellmark receives the OPM OIG debarment list every month, makes the appropriate updates to the FEP Direct claims processing system, and conducts quality assurance reviews. Any claim submitted for a debarred provider is flagged by Wellmark to

adjudicate through the OPM OIG debarment process to include initial notification, a 15 day grace period, and then denial.

Nothing came to our attention to indicate that Wellmark has not implemented adequate controls regarding the debarment process.

4) Application Controls Testing

We conducted a test of Wellmark's claims adjudication application to validate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which Wellmark's system adjudicated the claims. This included processing the claims through FEP Direct.

Our test results indicated that Wellmark's system has controls and system edits in place to identify many of our test scenarios.

Wellmark's claims processing system had edits to detect many of our flawed test claims, but not all.

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

Medical Editing

Our claims testing exercise identified several scenarios where Wellmark's claims processing system and FEP Direct failed to detect medical inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- *Invalid Place of Service (Professional)* – a test claim was submitted with a procedure code for a lung biopsy with a place of service code for a residential substance abuse facility;
- *Provider / Procedure Inconsistency (Professional)* – (1) a test claim was submitted with a procedure code for a pericardiectomy performed by a nurse practitioner; and (2) a test claim was submitted with a procedure code for a partial nephrectomy performed by a nurse practitioner;
- *Gender / Procedure Inconsistency (Institutional)* – (1) a test claim was submitted with a procedure code for a vasectomy performed on a female; (2) a test claim was submitted with a procedure code for a biopsy of the scrotum performed on a female; and (3) a test claim was submitted with a procedure code for a transuretheral prostatectomy performed on a female; and
- *Diagnosis / Procedure Inconsistency (Professional)* – (1) a test claim was submitted with a procedure code for a spinal manipulation with a diagnosis of a heart attack; (2) a test claim was submitted with a procedure code for a spinal manipulation with a diagnosis of

a malignant neoplasm; (3) a test claim was submitted with a procedure code for a toe amputation with a diagnosis of a headache; and (4) a test claim was submitted with a procedure code for a brain lesion removal with a diagnosis of abdominal pain.

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

The Association has an ongoing project in place related to improving the medical edits within FEP Direct. The specific scenarios identified in this audit should be analyzed as part of that project.

Recommendation 6

We recommend that the Association review the scenarios documented above and ensure that they are analyzed as part of the FEP Direct medical edits project.

Wellmark Response:

"[Blue Cross Blue Shield Association (BCBSA)] reviewed FEP claims history and the Plan reviewed Plan claims history and did not identify any of the scenarios identified during the audit. However, BCBSA submitted a request to the FEP Policy Work Group to review the recommended enhancements on February 25, 2016 for implementation. BCBSA will update the Contracting Office once a decision is made on implementing the edits."

Patient History

Our claims testing exercise identified several scenarios where Wellmark's claims processing system and FEP Direct failed to consider a patient's medical history. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- *Once Per Lifetime Procedures (Institutional)* – a test claim was submitted with a procedure code for a hysterectomy performed on a female member and the claim processed and paid appropriately. A subsequent test claim with a procedure code for a hysterectomy was submitted for the same member and that claim also processed and paid; and
- *Medical Review Claims (Institutional)* – a test claim was submitted with a procedure code for a manually assisted delivery for a female member and the claim processed and paid appropriately. A subsequent test claim with a procedure code for a manually assisted

delivery was submitted for the same member with a date of service one month after the initial claim and the claim processed and paid.

Failure to detect these patient history issues increases the risk that benefits are being paid for procedures that were not actually performed.

We previously identified issues with the way in which FEP Direct analyzes a patient's history as part of an audit of another BCBS plan (Report No. 1A-10-49-14-021). The specific scenarios identified in this audit should be analyzed as part of the efforts to address that existing recommendation.

Recommendation 7

We recommend that the Association review scenarios documented above related to patient history and ensure that they are analyzed as part of the ongoing efforts to address patient history edits in FEP Direct.

Wellmark Response:

"BCBSA reviewed FEP claims history and the Plan reviewed Plan claims history and did not identify any of the scenarios identified during the audit. However, BCBSA submitted a request to the FEP Policy Work Group to review the recommended enhancements on February 25, 2016 for implementation in the FEPExpress claims system. BCBSA will update the Contracting Office once a decision is made on implementing the edits."

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audits Group

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Senior Team Leader

[redacted], Group Chief

APPENDIX

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

March 2, 2016

[redacted], Group Chief
Information Systems Audits Group
U.S. Office of Personnel Management
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT AUDIT REPORT
Wellmark, Inc. IT Audit
Plan Codes 140/640
Audit Report Number 1A-10-31-15-058
(Dated January 8, 2016)

The following represents the Plan's response to the recommendations included in the draft report.

B. Access Controls

1. Facility Access Controls

Recommendation 1

We recommend that Wellmark implement some form of piggybacking controls at all facility entry points.

Plan Response

The Plan agrees with the recommendation. Implementation of piggybacking controls at the door in question will be completed by March 18, 2016.

2. Physical Recertification

Recommendation 2

We recommend Wellmark analyze its process for routinely auditing all active access lists to determine why individuals are remaining on access lists well after their termination dates. Subsequent action should be taken to address any problems identified in this analysis.

Plan Response

The Plan agrees with the recommendation. The Standard Operating Procedures related to terminations have been enhanced.

3. Data Center Access Controls

Recommendation 3

We recommend Wellmark reassess the physical access controls at its primary data center and implement multi-factor authentication and piggybacking prevention controls at all entrances.

Plan Response

The Plan agrees with the recommendation. Multi-factor authentication has been implemented at the primary data center and piggybacking prevention will be implemented by March 18, 2016.

C. Network Security

1. Vulnerabilities Identified in Automated Scans

Recommendation 4

We recommend Wellmark update its patch management policy to require the formal acceptance of risk for any systems that are not compliant with the policy. This documentation should be regularly reviewed to determine whether there is an ongoing need to keep these patches uninstalled.

Plan Response

The Plan agrees with the recommendation. The patch management policy has been enhanced to include a formal patch management exception analysis, documentation, approval, tracking, and periodic review.

Recommendation 5

We recommend that Wellmark implement a formal software lifecycle management methodology to ensure that only current and supported versions of system software are installed on the production servers.

Plan Response

The Plan agrees with the recommendation. By May 15, 2016, the existing formal technology standard will be enhanced to define that only supported versions of system software are installed on production servers and a formal variance process will be developed that includes the exception documentation, approval, and periodic review.

The identified noncurrent software applications will be removed, upgraded, or have a documented variance by April 1, 2016.

F. Claims Adjudication

4. Application Control Testing

Recommendation 6

We recommend that the Association review scenarios documented above and ensure they are analyzed as part of the FEP Direct medical edits project.

BCBSA Response

BCBSA reviewed FEP claims history and the Plan reviewed Plan claims history and did not identify any of the scenarios identified during the audit. However, BCBSA submitted a request to the FEP Policy Work Group to review the recommended enhancements on February 25, 2016 for implementation. BCBSA will update the Contracting Office once a decision is made on implementing the edits.

Recommendation 7

We recommend that the Association review scenarios documented above related to patient history and ensure that they are analyzed as part of the ongoing efforts to address patient history edits in FEP Direct.

BCBSA Response

BCBSA reviewed FEP claims history and the Plan reviewed Plan claims history and did not identify any of the scenarios identified during the audit. However, BCBSA submitted a request to the FEP Policy Work Group to review the recommended enhancements on February 25, 2016 for implementation in the FEPExpress claims system. BCBSA will update the Contracting Office once a decision is made on implementing the edits.

We appreciate the opportunity to provide our response to each of the findings in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [redacted] or [redacted] at [redacted].

Sincerely,

[redacted]

Managing Director, Program Assurance

cc: [redacted], Wellmark, Inc.
[redacted], OPM
[redacted], FEP
[redacted], FEP

Report Fraud, Waste, and Mismanagement

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

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

By Phone:

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

By Mail:

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