



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  
CAREFIRST BLUECROSS BLUESHIELD  
AND THE FEDERAL EMPLOYEES PROGRAM  
OPERATIONS CENTER**

Report No. 1A-10-92-08-021

Date: November 28, 2008

--CAUTION--

This audit report has been distributed to Federal and Non-Federal officials who are responsible for the administration of the audited contract. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905); therefore, while this audit report is available under the Freedom of Information Act, caution needs to be exercised before releasing the report to the general public.



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

Office of the  
Inspector General

**Audit Report**

**FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM  
CONTRACT CS 1039  
CAREFIRST BLUECROSS BLUESHIELD AND THE  
FEDERAL EMPLOYEES PROGRAM OPERATIONS CENTER  
PLAN CODES 200/700  
WASHINGTON, D.C.**

Report No. 1A-10-92-08-021

Date: November 28, 2008

A handwritten signature in black ink, appearing to read "Michael R. Esser".

**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  
CONTRACT CS 1039  
CAREFIRST BLUECROSS BLUESHIELD AND THE  
FEDERAL EMPLOYEES PROGRAM OPERATIONS CENTER  
PLAN CODES 200/700  
WASHINGTON, D.C.**

**Report No. 1A-10-92-08-021**

**Date: November 28, 2008**

This final report discusses the results of our audit of general and application controls over the information systems at CareFirst BlueCross BlueShield (CareFirst) and the BlueCross BlueShield Association's (BCBSA) Federal Employees Program Operations Center (FEPOC).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for CareFirst/FEPOC, 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.

### Entity-wide Security Program

CareFirst and the FEPOC have established a comprehensive series of IT policies and procedures to create an awareness of IT security at the Plan. CareFirst and the FEPOC have also implemented an adequate risk assessment methodology, incident response capabilities, and IT security related human resources controls. However, the Office of the Inspector General (OIG) recommended that the CareFirst and FEPOC Business Impact Analysis be updated on an annual basis in accordance with policies and procedures.

### Access Controls

We found that CareFirst and the FEPOC have 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, the OIG noted that the firewall configuration policy and the password complexity requirements of the mainframe security software used at CareFirst could be improved.

### Application Development and Change Control

FEPOC has established policies and procedures to ensure that modifications to application software occur in a controlled environment. Such controls include: appropriate levels of approval required prior to the migration of program changes; various levels and types of system testing in accordance with industry standards; and segregation of duties along organizational lines. In addition, we did not review the change control methodology at CareFirst during this audit.

### System Software

CareFirst has implemented a thorough system software change control methodology. This includes: a change management tool to control and track changes; multiple levels of approvals; and the implementation of policies and procedures for conducting emergency changes and limiting access to system software.

### Business Continuity

We reviewed both CareFirst and FEPOC business continuity and disaster recovery plans and concluded that they contained many of the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed, updated, and tested on a periodic basis.

### Application Controls

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

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

Nothing came to our attention that caused us to believe that CareFirst and the FEPOC are not in compliance with the various requirements of the HIPAA regulations. Furthermore, we did not identify any weaknesses in CareFirst or the FEPOC's HIPAA cost allocation methodology.

# Contents

	<u>Page</u>
Executive Summary.....	i
I. Introduction .....	1
Background.....	1
Objectives .....	2
Scope .....	2
Methodology.....	3
Compliance with Laws and Regulations .....	3
II. Audit Findings and Recommendations.....	4
A. Entity-wide Security Program .....	4
B. Access Controls .....	6
C. Application Development and Change Control.....	8
D. System Software .....	8
E. Business Continuity .....	9
F. Application Controls .....	10
G. Health Insurance Portability and Accountability Act.....	19
III. Major Contributors To This Report.....	21
Appendix: BlueCross BlueShield Association's August 19, 2008 response to the draft audit report issued June 19, 2008.	

## **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 CareFirst BlueCross BlueShield (CareFirst) and the BlueCross BlueShield Association's (BCBSA) Federal Employees Program Operations Center (FEPOC).

The audit was conducted pursuant to 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.

### **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.

CareFirst headquarters is located in Owings Mills, Maryland. Employees responsible for processing FEHBP (also, Federal Employees Program or FEP) local Plan claims for CareFirst are primarily located in the Plan's facilities in Charleston, West Virginia and Owings Mills, Maryland. The West Virginia facility is operated by a subsidiary of CareFirst known as the Capital Area Services Company, Inc. (CASCI).

BCBSA contracts with Service Benefit Plan Administrative Services Center, a subsidiary of Group Hospitalization and Medical Services, Inc. (d/b/a CareFirst BCBS) to maintain the information technology infrastructure of the FEPOC. FEPOC employees are primarily located at CareFirst's Portals facility in Washington, D.C. The claims processing applications used by CareFirst and the FEPOC are run on a mainframe located at CareFirst's Columbia, Maryland data center.

This was the OIG's second audit of general and application controls at CareFirst and the FEPOC. All audit recommendations from the previous audit were closed as of June 26, 2006. CareFirst/FEPOC's compliance with the Health Insurance Portability and Accountability Act (HIPAA) was also reviewed.

All 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 FEP data processed and maintained in CareFirst/FEPOC's computer systems.

These objectives were accomplished by reviewing the following areas:

- Entity-wide security;
- Access controls;
- Application development & change control;
- Segregation of duties;
- System software;
- Business continuity;
- Application controls specific to CareFirst/FEPOC's claims processing systems; and
- HIPAA compliance.

## **Scope**

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The OIG evaluated the confidentiality, integrity, and availability of CareFirst/FEPOC's computer-based information systems used to process FEP claims, and found that there are opportunities for improvement in the information systems' internal controls. These areas are detailed in the "Audit Findings and Recommendations" section of this report.

The scope of this audit centered on the claims processing systems that process FEP claims for CareFirst and the FEPOC, as well as the business structure and control environment in which they operate. These systems include the Flexx system owned and operated by CareFirst, and the FEP Express system owned by the BCBSA and operated in conjunction with CareFirst. CareFirst is an independent licensee of the BCBSA.

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

The audit was performed at CareFirst/FEPOC offices in Washington, D.C., Columbia, Maryland, Owings Mills, Maryland, and Charleston, West Virginia. These on-site activities were performed in March and April 2008. The OIG completed additional audit work before and after the on-site visits at OPM's office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at CareFirst/FEPOC as of May 9, 2008.

## **Methodology**

In conducting this review the OIG:

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

Various laws, regulations, and industry standards were used as a guide to evaluating CareFirst/FEPOC'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 (ITGI) CobiT: Control Objectives for Information and Related Technology;
- OPM Carrier Letter 2007-6, Omnibus Budget Reconciliation Act of 1990 (OBRA 90) Inpatient Prospective Payment System Pricer Program Usage;
- GAO's Federal Information System Controls Audit Manual;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-61, Computer Security Incident Handling Guide; and
- Health Insurance Portability and Accountability Act of 1996.

## **Compliance with Laws and Regulations**

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

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

### **A. Entity-wide Security Program**

The entity-wide security component of this audit examined the policies and procedures that are the foundation of CareFirst/FEPOC's overall IT security controls. The OIG evaluated the adequacy of CareFirst/FEPOC's ability to manage risk, develop security policies, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

The OIG also reviewed various CareFirst human resources policies and procedures to evaluate the controls in place regarding various human resources functions such as hiring, terminations, transfers, conflicts of interest, training, and standards of conduct which are also followed by FEPOC.

The policies and procedures that comprise CareFirst/FEPOC's entity-wide security program appear to provide an adequate foundation to protect the organization's information resources. However, the section below details one instance where CareFirst and FEPOC policies related to risk management did not appear to be enforced.

#### **1. Business Impact Analysis**

As part of their overall risk management process, CareFirst and the FEPOC have conducted business impact analyses (BIA) to evaluate the degree that disruptions to various business processes would have on the organizations as a whole. However, both the FEPOC and the CareFirst BIAs are outdated.

##### FEPOC

The FEPOC BIA describes the potential financial and operational impacts that may result from a disruption of operations to FEPOC or CareFirst facilities. The BIA prioritizes the resumption of business processes, defines acceptable restoration times, and lists the resources required to support these processes.

The FEPOC BIA was last updated in December 2006. The executive summary section of the BIA states that "The BIA should be updated at least annually. Changes in priorities, applications, systems, personnel and regulations can modify or invalidate findings addressed in the BIA."

##### CareFirst

The CareFirst BIA process begins with the distribution of BIA surveys to the managers of various applications and business functions. The surveys are used to gather information related to acceptable downtimes and resources required to support the function. This information is then analyzed and incorporated into one overall BIA for CareFirst.

The CareFirst BIA was last updated in March 2005, based on survey results from September 2004. Although updated surveys were collected in May 2007, this information has not been incorporated into an updated BIA.

Both BIAs state that they are used as a basis for updating business continuity and disaster recovery plans. Failure to properly maintain BIAs increases the risk that system vulnerabilities and recovery priorities do not reflect the current environment, potentially leading to gaps in disaster recovery and business continuity procedures.

### **Recommendation 1**

We recommend that the FEPOC BIA be updated on an annual basis.

#### **BCBSA Response:**

*“The FEPOC reviews the BIA on an annual basis, and updates them every two to three years. Changes to the critical and non-critical systems do not occur in that interval where it would require updating the BIA annually. The FEPOC reviews and makes updates to the systems or processes related to our business at least twice a year in conjunction with the DR (Disaster Recover) exercises. If there are substantial changes to the systems, DR and business continuity documentation changes are accommodated at other times to ensure recoverability of all systems in the event of a disaster and during the next scheduled Disaster Recovery (DR) exercise.”*

#### **OIG Reply:**

The FEPOC BIA itself states that it should be updated on an annual basis. If this requirement does not accurately describe the current procedures, we recommend that the FEPOC address this inconsistency.

### **Recommendation 2**

We recommend that the CareFirst BIA be updated to include the results of the most recent BIA surveys, and be updated on a periodic basis thereafter.

#### **BCBSA Response:**

*“The data compiled in 2007 and shared with the OIG auditors was an official BIA. At that time, a new survey was completed and data was compiled. The business continuity and disaster recovery requirements were updated to reflect the information collected in this survey. All business continuity scenarios included in our plans were modified to reflect this data and these requirements. In addition, business continuity plans are reviewed/updated by the business owners on a semi-annual basis and audited on a test basis by corporate business continuity. CareFirst is currently undergoing a corporate reorganization that is anticipated to be completed in 2009. At that time, new BIA surveys will be completed and the data compiled will be incorporated in the business continuity and disaster recovery plans.”*

### **OIG Reply:**

The CareFirst BIA states that the survey data is “intended to identify the time-sensitive business operations and the resources required to support recovery of those operations.” The information compiled from the surveys is then used to develop and improve the overall business continuity program, including the BIA itself. OIG auditors were not provided with evidence that the business continuity and disaster recovery requirements were updated to reflect the information collected in the 2007 survey. The CareFirst BIA that was provided for review indicates that it was last updated in March 2005. If the CareFirst BIA was updated to include the compiled survey data in 2007, we recommend that, as part of the audit resolution process, CareFirst provide OPM’s Center for Retirement and Insurance Services (CRIS) with appropriate supporting documentation.

## **B. Access Controls**

Access controls are the policies, procedures, and techniques management has put in place to prevent or detect unauthorized physical or logical access to sensitive resources.

The OIG examined the logical controls protecting CareFirst/FEPOC’s network environment and claims processing-related applications. During this review, the following controls were documented:

- Procedures for authorizing, reviewing, and removing logical access to the information systems used to process FEP claims;
- Adequate authentication controls for the CareFirst and FEPOC network domains; and
- Procedures for monitoring and filtering network activity.

The OIG also examined the physical controls of CareFirst/FEPOC’s facilities in Owings Mills and Columbia, Maryland, Washington, D.C., and Charleston, West Virginia. Access to all of these facilities is controlled by an electronic access card system. Card readers are located on interior and exterior doors throughout the buildings, and the activity of each entrance is continuously monitored by various electronic and physical methods. The OIG also documented additional physical controls at the raised-floor area of the data center in Columbia, Maryland.

The following sections detail the opportunities for improvement that were noted for logical and physical access controls.

### **1. Firewall Configuration Policy**

The IT Security team at CareFirst's Columbia, Maryland data center is responsible for configuring and maintaining the organization's firewalls. However, CareFirst has not established a corporate policy detailing firewall configuration requirements.

NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, states that a firewall policy should dictate “how the firewall should handle applications traffic such as web, email, or telnet. The policy should describe how the firewall is to be managed and updated.” Furthermore, the NIST guidance states that periodic reviews of the firewalls should be conducted by comparing the actual firewall configuration to the expected configuration

based on the defined policy. Without a formal policy, CareFirst is unable to perform such a review, increasing the risk that the firewall is configured in a manner that does not provide optimum security for the organization.

**Recommendation 3**

We recommend that CareFirst implement a firewall configuration policy, and begin using this policy as a baseline during periodic firewall reviews and audits. The policy should contain the elements suggested by NIST SP 800-41 or other appropriate guidance.

**BCBSA Response:**

*“CareFirst agrees with this recommendation and has completed the implementation of the recommended firewall configuration policy as of May 15, 2008. The firewall configuration review/testing was completed during the period of May 22 through June 9, 2008.”*

**OIG Reply:**

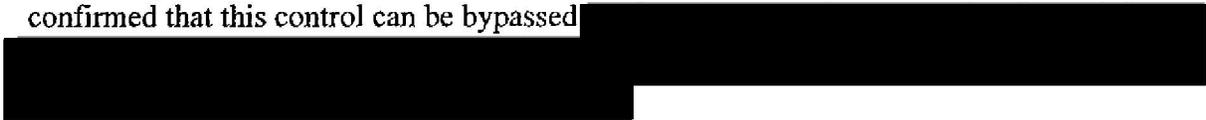
As part of the audit resolution process, we recommend that CareFirst/FEPOC provide OPM’s CRIS with appropriate supporting documentation detailing the steps taken to address this recommendation.

**2. Password Complexity Requirement**

CareFirst uses Resource Access Control Facility (RACF) security software to govern access to mainframe applications. The password complexity requirements for RACF user IDs are defined by the “password syntax rules” outlined in the RACF SETR List report. The OIG reviewed CareFirst’s SETR List and concluded that the RACF password complexity requirements are configured in a manner that is not consistent with CareFirst policy or industry acceptable best-practice.

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, provides guidelines that organizations should follow to ensure secure authentication to their information systems. The current settings at CareFirst are not adequate and present CareFirst/FEPOC with an increased risk of unauthorized system access.

CareFirst utilizes a third party program, “Control-SA” by BMC Software, Inc., to allow users to reset and update RACF passwords. We acknowledge that this program enforces password complexity in accordance with CareFirst and industry standards. However, the OIG auditors confirmed that this control can be bypassed



**Recommendation 4**

We recommend that CareFirst improve controls related to password requirements in a manner that prevents users from setting a RACF password that does not meet CareFirst policy and industry standards.

**BCBSA Response:**

*“The RACF system changes recommended would require significant effort in time and resources. As a mitigating control, CareFirst utilizes a third party program, ‘Control-SA’ by BMC Software, Inc. to allow users to reset and update RACF passwords. As acknowledged by the Office of the Inspector General (OIG) auditors, this program enforces password complexity in accordance with CareFirst and industry standards. Therefore, CareFirst security controls are in compliance with standard industry practice and HIPAA security guidelines.”*

**OIG Reply:**

The BCBSA response did not address the OIG’s concern that password controls enforced by “Control-SA” can be bypassed [REDACTED]

[REDACTED] We continue to recommend that CareFirst improve controls related to password requirements in a manner that prevents users from setting a RACF password that does not meet CareFirst policy and industry standards.

**C. Application Development and Change Control**

The OIG evaluated the policies and procedures governing software development and change control of the FEPOC’s FEP Express claims processing application. We did not review the change control methodology of CareFirst’s Flexx claims processing system during this audit.

The FEPOC has adopted a traditional system development life cycle (SDLC) methodology that incorporates the use of change requests managed by a project tracking tool. The FEPOC also uses a structured approval process for change requests. The following controls related to testing and approvals of software modifications were observed:

- Testing activities are controlled through formal test plans for major application modifications;
- Testing activities are conducted at different stages of the SDLC;
- Appropriate levels of approval must be completed before the change is migrated into the production environment; and
- Procedures and controls are in place for emergency changes.

The OIG also observed the following controls related to software libraries:

- The FEPOC has a software library management tool that provides sufficient control of application software;
- Application software is segregated among development, testing, and production regions; and
- There is a clear segregation of duties along organizational lines for all application software modifications.

**D. System Software**

The system software that houses the Flexx and FEP Express claims processing applications is located at CareFirst’s data center in Columbia, Maryland. The two applications are run on a

single mainframe (separate logical partitions) with the MVS operating systems and a shared RACF security database.

CareFirst has implemented a thorough system software change control methodology. This process utilizes a change management tool to control and track changes, and involves multiple levels of approvals. The approval process includes representatives from both CareFirst as owners of the system software and the Flexx application, and the FEPOC as owners of the FEP Express application.

It was also noted that CareFirst has implemented policies and procedures for conducting emergency changes and limiting access to system software to the appropriate individuals. The OIG reviewed several high level settings of CareFirst's RACF database, and did not identify any weaknesses other than the password complexity issue discussed in section B above.

## **E. Business Continuity**

The OIG reviewed CareFirst's and FEPOC's business continuity program to determine if (1) procedures were in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan existed to recover critical operations should interruptions occur.

The FEPOC relies on the CareFirst business continuity program for: mainframe, UNIX and network support; maintenance of mainframe system software; maintenance of midrange hardware and systems software; performing batch runs; and maintenance of network connectivity to the claims and enrollment systems located at the CareFirst data center. FEPOC's primary duty in a disaster recovery situation is to restore the application data needed for operations to continue.

In an effort to assess CareFirst's business continuity capabilities, we evaluated documentation related to the Plan's procedures that ensure continuity of the FEP business unit, including:

- CareFirst's Disaster Recovery Plans;
- CareFirst's Mainframe Disaster Recovery Procedure; and
- FEPOC offsite data recovery procedures.

The OIG found that each of these documents contain a majority of the key elements of a comprehensive service continuity program suggested by NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems." Each of the documents are reviewed, updated, and tested on a regular basis. The results of the testing exercises document test scenarios, test results, potential problems, and opportunities for improvement.

CareFirst's business continuity methodology relies on BIA processes of both CareFirst and the FEPOC. This involves identifying the systems that are critical to continuing business operations, prioritizing these systems, and outlining the specific resources needed to support each system. However, based on the issue identified in Section A above, the disaster recovery documentation could contain gaps until the BIA for both CareFirst and FEPOC is updated.

## **F. Application Controls**

The OIG evaluated the input, processing, and output controls associated with CareFirst/FEPOC's claims processing systems.

To validate the claims processing controls, a testing exercise was conducted on the Flexx and FEP Express claims processing applications. The exercise involved developing a test plan that included real life situations to present to CareFirst/FEPOC personnel in the form of institutional and professional claims. The test plan included expected results for each test case. Upon conclusion of the testing exercise, the expected results were compared with the actual results obtained during the exercise.

Two sets of test claims were used during the exercise. The first set of claims was entered into the Flexx system at CareFirst's CASCI facility in Charleston, West Virginia. Where appropriate, the Flexx system routed these claims to FEP Express. The second set of claims was entered directly into the FEP Express system at the FEPOC's Portals facility in Washington, D.C.

### **1. Input Controls**

The OIG identified all possible sources of claims coming into CareFirst's Flexx claims processing system, as well as the mechanisms established by CareFirst to accept and process the claims. For paper claims received by mail, we learned that CareFirst:

- Segregates claims by form type;
- Uses scanning equipment that assigns a document control number on scanned documents; and
- Visually verifies that claims are scanned correctly.

For claims transmitted electronically, CareFirst has adopted the following practices:

- The use of HIPAA compliant formats;
- The use of EC Map to verify that trading partners are using HIPAA formats; and
- The use of encryption when transmitting data.

The OIG did not identify any weaknesses related to CareFirst's process for receiving FEP claims.

### **2. Processing Controls**

The results of the OIG's claims testing exercise indicated that several modifications should be made to CareFirst/FEPOC's claims processing methodology in order to produce results consistent with its contract with OPM and other regulations. The sections below document the unexpected results from the claims testing exercise. Although each section states whether the test claim was entered through the Flexx system or through FEP Express, this does not necessarily indicate which system should be modified to correct the problem.

**a. Omnibus Budget Reconciliation Act of 1993 (OBRA 93) Pricing**

Two OBRA 93 test claims were priced incorrectly.

The OIG processed two OBRA 93 test claims (one entered into Flexx and one entered into FEP Express) with an assistant surgeon provider using an “AS” modifier. For the claim entered into Flexx, the system paid the assistant surgeon 100 percent of the Plan allowance of the primary surgeon. For the claim entered into FEP Express, the system paid the assistant surgeon 100 percent of the amount allowed by the Medicare fee schedule for the primary surgeon.

Both test claims resulted in an overpayment to the provider, as the Center for Medicare Services Medicare Claims Processing Manual states that assistant surgeon claims should only be paid at 13.6 percent of the Medicare fee schedule.

**Recommendation 5**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that OBRA 93 claims are priced appropriately.

**BCBSA Response:**

*“OBRA ’93 claims pricing is an FEP responsibility that is handled by Palmetto, an outside vendor. Due to the complex nature of the pricing of claims with procedure code modifier ‘AS,’ these claims were excluded from the pricing requirements in the Vendor’s contract. The necessary changes to the Vendor’s contract have been made to allow for the pricing of these claims. Effective May 26, 2008, FEP claims with the procedure code modifier of ‘AS’ began to be priced in accordance to the Medicare Fee Schedule by Palmetto. Because the FEP Director’s office was aware of the processing deficiency, periodic listings identifying these overpayments were sent to Plans to initiate refunds. Once this change was made, the final listings of overpayments caused by the lack of the ‘AS’ modifier reduction were sent to Plans to initiate recoveries.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that CareFirst/FEPOC provide OPM’s CRIS with appropriate supporting documentation indicating that the appropriate modifications have been made. We will test the functionality of the new controls during a follow-up review or as part of the next audit. We also recommend that all recoveries of overpayments identified by the FEP Director’s Office be reported to OPM’s Insurance Services Program and coordinated through the audit resolution process.

**b. Chiropractic Spinal Manipulations Accumulator**

In two test scenarios, chiropractic benefits related to spinal manipulations were incorrectly applied.

The BlueCross BlueShield (BCBS) FEP benefit brochure states that subscribers with the “standard” option are allowed 12 spinal manipulations per calendar year.

In the first test scenario, the OIG submitted two claims into the Flexx system with a total of 16 spinal manipulations. One manipulation on the second claim was denied because it was a duplicate of a manipulation on the first claim. Although the denied manipulation was not paid, the system’s accumulator counted this manipulation against the allowed amount, and the subscriber only received benefits for 11 manipulations.

In the second test scenario, the OIG submitted two claims into the FEP Express system with a total of 16 manipulations. One manipulation on the second claim had the same date and provider, but a different procedure code, as a manipulation on the first claim. The system’s accumulator only counted these two manipulations as one, and the subscriber received benefits for 13 manipulations.

#### **Recommendation 6**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that chiropractic spinal manipulation benefits are applied correctly.

#### **BCBSA Response:**

*“First, we would like to clarify that the accumulation of the number of manipulations is a FEPEXpress function. We conducted the same type of testing performed by the OIG auditors in an effort to determine whether there are any issues with the manner in which FEPEXpress accumulates the number of manipulations per year. We did not receive the same results as the ones obtained by the OIG auditors. Attachment A contains copies of our test results using the FEP reporting requirements for this service.”*

#### **OIG Reply:**

After reviewing the test results provided by BCBSA, it appears that BCBSA did not execute the testing scenario with the same methodology that the OIG used during the audit. As stated above, the OIG submitted two claims into the FEP Express system with a total of 16 manipulations. One manipulation on the second claim had the same date and provider, but a different procedure code, as a manipulation on the first claim.

The OIG provided BCBSA with printouts from the original testing exercise in which this problem was encountered. We suggest that BCBSA use this same methodology to duplicate the problem, and continue to recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that chiropractic spinal manipulation benefits are applied correctly.

### c. Chiropractic Office Visits and X-rays

The BCBS FEP benefit structure allows for one chiropractic office visit and one set of x-rays each calendar year. However, in two test scenarios, benefits were paid for multiple office visits for one subscriber.

In the first test scenario, the OIG submitted two claims for one subscriber into the Flexx system. The first claim contained procedure codes for a “new patient” office visit and a set of x-rays. The second claim used the same provider, and contained procedure codes for an “established patient” office visit and a set of x-rays. Both claims processed through the system and were paid without encountering any edits.

In the second test scenario, the OIG submitted two claims for one subscriber into the FEP Express system. Both claims were for the same subscriber and provider, and both contained procedure codes for a “new patient” office visit and a set of x-rays. The system processed and paid both claims without triggering any system edits.

The BCBS benefit brochure states that subscribers are entitled to “an initial office visit” and an “initial set of x-rays.” The OIG acknowledges that the term “initial” could be interpreted to mean an initial office visit and set of x-rays from *multiple* providers. However, the actual benefit negotiated between OPM and the BCBSA covers *one* office visit and *one* set of x-rays per calendar year. The 2009 benefit brochure will be updated to more clearly define this benefit.

#### **Recommendation 7**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that subscribers receive benefits for only one chiropractic office visit and one set of x-rays each calendar year.

#### **BCBSA Response:**

***“The 2008 Blue Cross Blue Shield Service Benefit Brochure states on page 46, ‘initial office visit’ for a Chiropractor. During late 2007, we became aware of the difficulty in the administration of this benefit due to the language used. Initially, an edit was put in the FEP system to limit the benefit to one visit. However, because the brochure reads initial visit, we had to remove the edit as there was no definition provided to the members to define whether initial office visit meant per Chiropractor or per episode or per benefit period. As a result, we have made a request for a Contract modification to change the word ‘initial’ to ‘one’ visit. This request was submitted with the 2009 Benefit Changes/Clarifications. The results of the 2009 Benefit negotiations have not yet been published. Once this information is made available, we will provide an update to our response.”***

**OIG Reply:**

After the contract is modified to specify that “one” chiropractic office visit is allowed per year, we recommend that CareFirst/FEPOC reinstate the edit to ensure that the system appropriately enforces this element of the contract.

**d. Chiropractic Diagnosis**

A test claim was processed where benefits were paid for chiropractic spinal manipulations associated with an inappropriate diagnosis.

The OIG submitted a test claim into the Flexx system with a procedure code for a spinal manipulation where the subscriber had a diagnosis of chicken pox. The claim was processed through the system and was paid without encountering any system edits.

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

**Recommendation 8**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a subscriber’s diagnosis is evaluated for appropriateness before chiropractic benefits are paid.

**BCBSA Response:**

*“Medical Edits are the responsibility of the local Plans. Please reference the Attachment B for a copy of FEP Administrative Manual Volume I, Chapter 15 – 107 for a description of this requirement. It would be a duplication of efforts and costly to the Program for FEPEXpress to contain the various medical policies for each specific Plan as well as requiring numerous Plan specific edits.*

*CareFirst will work with the FEP Director’s Office to re-evaluate its medical edits in an effort to determine what local system edits may require enhancements in order to ensure that these types of situations are pended for review of the medical appropriateness of the services prior to payment. We estimate that this evaluation will be completed by the end of first quarter 2009.”*

**OIG Reply:**

As part of the audit resolution process, we recommend that CareFirst/FEPOC provide OPM’s CRIS with appropriate supporting documentation indicating that the system’s medical edits have been enhanced to ensure that a subscriber’s diagnosis is evaluated for appropriateness before chiropractic benefits are paid.

**e. Multiple Procedure Instances**

Two test claims were processed and paid for a subscriber receiving the same surgical procedure twice in one day from different providers.

Both claims were entered into the FEP Express system (in separate batches), and were identical with the exception of the provider data. The system processed and paid both claims, even though they were for a vasectomy. It is highly unlikely in the real world that a patient would have two vasectomies performed on the same day by different providers.

This test scenario was also entered into the Flexx system, which appropriately suspended the claims as “suspected duplicates.” The OIG believes that similar edits should be incorporated into FEP Express to support the BCBS Plans that may not have suspected duplicate edits in their local systems, as well as for Plans that enter claims directly into FEP Express (as CareFirst does for overseas claims).

### **Recommendation 9**

We recommend that CareFirst/FEPOC incorporate the appropriate edits into FEP Express that will allow the system to identify and suspend claims that are identical to previously processed claims in all fields except for the provider.

We acknowledge the fact that, for certain procedures, it may be possible to have the same type of service rendered on the same day by different providers. The system could be programmed to selectively apply the new edit based on the procedure in question. In order to avoid hindering the efficiency of the edit process, the edit could be designed to bypass entire classes of procedures where multiple same-day instances of a procedure are likely to occur (e.g., office visits, lab tests, dental procedures).

### **BCBSA Response:**

*“There are surgical procedures that are normally performed one time; however, we have encountered a number of exceptions with these procedures. Sometimes, only a partial procedure is performed or the first procedure was unsuccessful and it must be performed again. An example of such a procedure would be a vasectomy. If the procedure was unsuccessful, it can be re-performed at the patient’s request.*

*The example used by the OIG auditors was a vasectomy performed on the same day by two different providers. Because the example included two different providers, the claim did not defer on FEPEXpress as a possible duplicate. Different providers are not part of the FEP System Duplicate Criteria. However, the question with the two vasectomies is the medical appropriateness of two doctors performing this procedure on the same day, on the same member. Since this is not accepted medical practice (Local Medical Policy) for the CareFirst service area, the second claim correctly deferred on the FLEXX System. This is the correct process as Medical Edits are housed at the local Plans. However, the claim paid on FEPEXpress as there are no Medical Edits on FEPEXpress.*

*If the OIG auditors can provide FEP with a listing of the procedures that should be included in a new edit that is designed to limit members to one surgical service per lifetime, we will evaluate the feasibility of limiting these services. At this time, we*

*cannot determine the types of surgical procedures that we should limit members to one per lifetime. Therefore, no changes will be made to the FEPEXpress at this time.”*

**OIG Reply:**

This test claim was deferred by the local Flexx system as a “suspected duplicate,” not as a medical policy edit. This indicates that the capability exists to create a system edit to identify and suspend claims that are identical to previously processed claims in all fields except for the provider. We continue to recommend that this edit be implemented in FEP Express in order support the BCBS Plans that may not have suspected duplicate edits in their local systems, as well as for Plans that enter claims directly into FEP Express (as CareFirst does for overseas claims).

**f. Procedure Bundling**

A test claim containing multiple laboratory procedures was not appropriately bundled.

The OIG submitted a test claim in the FEP Express system that contained nine laboratory procedures that were expected to be bundled into a single procedure (Basic Metabolic Panel). The test claim also contained the procedure code for a pre-bundled Basic Metabolic Panel. The system did not bundle the nine separate procedures, and did not deny the Basic Metabolic Panel as a duplicate.

A similar test claim was also entered into the Flexx system, which appropriately bundled the nine procedures and denied the Basic Metabolic Panel as a duplicate. The OIG believes that similar edits should be incorporated into FEP Express to support the BCBS Plans that may not have procedure bundling edits in their local systems, as well as for Plans that enter claims directly into FEP Express (as CareFirst does for overseas claims).

**Recommendation 10**

We recommend that CareFirst/FEPOC implement the appropriate modifications to FEP Express to ensure that the system can appropriately process claims where procedure bundling is required.

**BCBSA Response:**

*“The bundling of like medical services is based upon local medical policies and is considered a Medical Edit that is handled at the Plan level. The test claims processed through FLEXX were appropriately bundled by ClaimCheck which performs various medical edits/bundling for the Plan. The auditors also submitted the unbundled claims directly to FEPEXpress, which appropriately did not bundle these services as the bundling process is not maintained on FEPEXpress. As a result, no changes are required to the FEPEXpress.”*

**OIG Reply:**

The BCBSA response indicates that the bundling of similar medical services is based upon local medical policies. This statement is incorrect, as the methodology for bundling

of similar medical services is defined by the Current Procedural Terminology manual issued by the American Medical Association on an annual basis. In addition, the BCBSA response did not address the fact that not all BCBS Plans have procedure bundling medical edits implemented in their local systems, and some Plans enter claims directly into FEP Express (as CareFirst does for overseas claims). The OIG continues to believe that these vulnerabilities warrant modifications to FEP Express.

**g. Procedure to Diagnosis Inconsistency**

A test claim was processed where benefits were paid for a procedure associated with an inappropriate diagnosis.

The OIG entered a test claim into the FEP Express system with a procedure code for a transurethral incision of the prostate and a diagnosis of an ankle fracture. The system processed and paid the claim without triggering any edits.

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

**Recommendation 11**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a subscriber's diagnosis is evaluated for appropriateness before benefits are paid.

**BCBSA Response:**

*“The determining of whether the services are related to the diagnosis requires Medical Edits to defer the claim for review. Medical Edits are maintained at the Plan level. The test claim in question processed correctly in the local Plan system. However, the auditors also processed the test claim directly in FEPEXpress, which appropriately did not edit the claim for diagnosis/procedure compatibility since such edits reside in the local system. Therefore, no changes are required to FEPEXpress.”*

**OIG Reply:**

The BCBSA response indicates that medical edits are handled at the Plan level. However, the response did not address the fact that not all BCBS Plans have diagnosis/procedure compatibility edits in their local systems, and some Plans enter claims directly into FEP Express (as CareFirst does for overseas claims). The OIG continues to believe that these vulnerabilities warrant modifications to FEP Express.

**h. Non-participating Provider Pricing**

A non-participating (non-par) provider was paid an amount significantly greater than the amount allowed by the Medicare fee schedule.

The OIG submitted a test claim into the FEP Express system for an office visit with a diagnosis of chicken pox for a Medicare subscriber. Although the Medicare fee schedule allows \$38.50 for an office visit, the system paid the provider the full \$6,000 of submitted charges.

The non-participating provider allowance (NPA) is calculated as the greater of the Medicare fee schedule or the Plan's pricing allowance (PPA). In this test case the processor entered a PPA equal to the submitted charges of \$6,000. We would expect the system to suspend the claim after detecting the large variance between the NPA and the Medicare fee schedule.

This system weakness increases the risk that non-par providers are being significantly overpaid when they inadvertently or fraudulently submit charges well in excess of the Medicare fee schedule amount.

### **Recommendation 12**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that non-par provider claims are suspended for review when there is a large variance between the NPA and the Medicare fee schedule. CareFirst/FEPOC will need to determine an acceptable variance above which the claims should be suspended.

### **BCBSA Response:**

*“Non-Par professional claims are priced by FEPEXpress. We are currently conducting a study to determine the specifications required to implement an edit that would defer any non-par priced claim that exceeds 40% of the Medicare Fee Schedule. The results of the study are expected during the fourth quarter 2008 with implementation of the recommendation in 2009.”*

### **OIG Reply:**

As part of the audit resolution process, we recommend that CareFirst/FEPOC provide OPM's CRIS with appropriate supporting documentation indicating the steps taken to address this recommendation. We will test the functionality of the new controls during a follow-up review or as part of the next audit.

#### **i. OBRA 90 Transfer**

An OBRA 90 test claim was incorrectly processed as a transfer claim.

The OIG submitted an OBRA 90 test claim into FEP Express that included a discharge status of '43,' and the system processed and paid this claim as a transfer. However, OPM Carrier Letter 2007-6, "OBRA 90 IPPS PRICER Program Usage," states that only claims with a discharge status of '02' should be processed as transfers.

The OIG suspects that the BCBSA's FEP Express system has not been updated to incorporate the discharge status codes outlined in the Carrier Letter. As a result,

CareFirst/FEPOC has incorrectly priced all OBRA 90 claims with a status code of '43' that have been processed after February 28, 2007, the date the Carrier Letter was issued.

### **Recommendation 13**

We recommend that CareFirst/FEPOC implement the necessary system modifications to ensure compliance with the requirements of OPM Carrier letter 2007-6.

### **BCBSA Response:**

*"OBRA '90 Pricing is a function of FEPEXpress. When the system changes to comply with OPM Carrier letter 2007-6 was implemented, patient status '43' was incorrectly included in the transfer application in the OBRA '90 Pricer. As a result, these claims may have been underpaid. We were aware of this issue from previous audits of other Plans. The system correction to limit the OBRA'90 Transfer pricing to patient status '02' will be implemented on October 18, 2008."*

### **OIG Reply:**

As part of the audit resolution process, we recommend that CareFirst/FEPOC provide OPM's CRIS with appropriate supporting documentation indicating the steps taken to address this recommendation. We will evaluate the effectiveness of the planned October 18, 2008 update as part of a follow-up review or during the next audit.

## **3. Output Controls**

CareFirst has adopted adequate policies and practices to provide guidance for the generation and distribution of system output related to the claims processing applications within the scope of this audit. These include activities such as:

- The use of a "totals sheet" to keep track of all output as well as stuffed envelopes;
- The use of a Bh2 log to keep track of batches that were sent to their bulk mail distributor; and
- The use of a recreated documents sheet to keep track of any damaged output.

The OIG did not identify any weaknesses related to CareFirst's procedures for controlling system output for FEP claim transactions.

## **G. Health Insurance Portability and Accountability Act**

The OIG reviewed CareFirst/FEPOC's efforts to maintain compliance with various HIPAA regulations.

The FEPOC primarily relies on CareFirst for compliance efforts related to the HIPAA security and privacy rules. CareFirst has implemented a series of IT security policies and procedures that adequately address the requirements of the HIPAA security rule. In addition, CareFirst has developed a privacy policies and procedures manual that directly addresses all requirements of the HIPAA privacy rule.

The OIG reviewed CareFirst's and the FEPOC's compliance with the HIPAA standards for electronic transactions, and determined that both organizations adhere to the requirements of this rule.

The OIG also reviewed CareFirst's and the FEPOC's methodology for allocating HIPAA related costs (budgeted and actual) to its various lines of business for 2003 through 2007. The OIG did not identify any weaknesses in CareFirst's HIPAA cost allocation methodology.

Finally, the OIG documented that both the FEPOC and CareFirst have adopted the National Provider Identifier as the standard unique health identifier for health care providers, as required by HIPAA.

### **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] Auditor

## Appendix

August 19, 2008

██████████ Chief  
Chief, Information Systems Audits Group  
U. S. Office of Personnel Management  
Office of the Inspector General  
1900 E Street, N.W., Room 6400  
Washington, D.C. 20415

**Reference: OPM DRAFT AUDIT REPORT  
FEP Operations/CareFirst Maryland  
Audit Report Number 1A-10-92-08-021  
(Dated and Received 06/19/08)**

Dear ██████████

This is in response to the above-referenced U.S. Office of Personnel Management (OPM) Draft Audit Report covering the Federal Employees' Health Benefits Program (FEHBP) Audit of Information Systems General and Application Controls for the FEP Operations Center (FEPOC) and the CareFirst DC Plan's interface with the FEP claims processing system, access and security controls. The response to this report is divided into two sections. The first section is the response to the report and the second section is requested wording changes that Plan staff feels will better characterize their organizational environment (Attachment C). Our comments concerning the recommendations in the report are as follows:

**A. Entity-wide Security Program**

**1. Business Impact Analysis (BIA)**

Both BIAs state that they are used as a basis for updating business continuity and disaster recovery plans. Failure to properly maintain BIAs increases the risk that system vulnerabilities and recovery priorities do not reflect the current environment, potentially leading to gaps in disaster recovery and business continuity procedures.

**OIG Recommendation 1**

We recommend that FEPOC BIA be updated on an annual basis.

## **Response to Recommendation 1**

The FEPOC reviews the BIA on an annual basis, and updates them every two to three years. Changes to the critical and non-critical systems do not occur in that interval where it would require updating the BIA annually. The FEPOC reviews and makes updates to the systems or processes related to our business at least twice a year in conjunction with the DR (Disaster Recover) exercises. If there are substantial changes to the systems, DR and business continuity documentation changes are accommodated at other times to ensure recoverability of all systems in the event of a disaster and during the next scheduled Disaster Recovery (DR) exercise.

## **OIG Recommendation 2**

We recommend that the CareFirst BIA be updated to include the results of the most recent BIA surveys, and be updated on a periodic basis thereafter.

## **Response to Recommendation 2**

The data compiled in 2007 and shared with the OIG auditors was an official BIA. At that time, a new survey was completed and data was compiled. The business continuity and disaster recovery requirements were updated to reflect the information collected in this survey. All business continuity scenarios included in our plans were modified to reflect this data and these requirements. In addition, business continuity plans are reviewed/updated by the business owners on a semi-annual basis and audited on a test basis by corporate business continuity. CareFirst is currently undergoing a corporate reorganization that is anticipated to be completed in 2009. At that time, new BIA surveys will be completed and the data compiled will be incorporated in the business continuity and disaster recovery plans.

### **B. Access Controls**

#### **1. Firewall Configuration Policy**

The IT Security team at CareFirst's Columbia, Maryland data center is responsible for configuring and maintaining the organization's firewalls. However, CareFirst has not established a corporate policy detailing firewall configuration requirements.

NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, states that a firewall policy should dictate "... how the firewall should handle applications traffic such as web, email, or telnet. The policy should describe how the firewall is to be managed and updated."

### **OIG Recommendation 3**

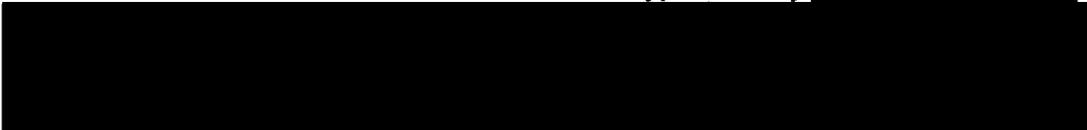
We recommend that CareFirst implement a firewall configuration policy, and begin using this policy as a baseline during periodic firewall reviews and audits. The policy should contain the elements suggested by NIST SP 800-41 or other appropriate guidance.

### **Response to Recommendation 3**

CareFirst agrees with this recommendation and has completed the implementation of the recommended firewall configuration policy as of May 15, 2008. The firewall configuration review/testing was completed during the period of May 22 through June 9, 2008.

## **2. Password Complexity**

CareFirst utilizes a third party program, "Control-SA" by BMC Software, Inc., to allow users to reset and update RACF passwords. We acknowledge that this program enforces password complexity in accordance with CareFirst and industry standards. However, the OIG auditors confirmed that this control can be bypassed by 



### **OIG Recommendation 4**

We recommend that CareFirst improve controls related to password requirements in a manner that prevents users from setting a RACF password that does not meet CareFirst policy and industry standards.

### **Response to Recommendation 4**

The RACF system changes recommended would require significant effort in time and resources. As a mitigating control, CareFirst utilizes a third party program, "Control-SA" by BMC Software, Inc. to allow users to reset and update RACF passwords. As acknowledged by the Office of the Inspector General (OIG) auditors, this program enforces password complexity in accordance with CareFirst and industry standards. Therefore, CareFirst security controls are in compliance with standard industry practice and HIPAA security guidelines.

**C. Application Controls**

**3. Processing Controls**

**a. OBRA '93 Pricing**

The OIG processed two OBRA '93 test claims (one entered into Flexx and one entered into FEP Express) with an assistant surgeon provider using an "AS" modifier. For the claim entered into Flexx, the system paid the assistant surgeon 100% of the Plan allowance or the primary surgeon. For the claim entered into FEPEXpress, the system paid the assistant surgeon 100% of the amount allowed by the Medicare fee schedule for the primary surgeon.

**OIG Recommendation 5**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that OBRA '93 claims are priced appropriately.

**Response to Recommendation 5**

OBRA '93 claims pricing is an FEP responsibility that is handled by Palmetto, an outside vendor. Due to the complex nature of the pricing of claims with procedure code modifier "AS," these claims were excluded from the pricing requirements in the Vendor's contract. The necessary changes to the Vendor's contract have been made to allow for the pricing of these claims. Effective May 26, 2008, FEP claims with the procedure code modifier of "AS" began to be priced in accordance to the Medicare Fee Schedule by Palmetto. Because the FEP Director's office was aware of the processing deficiency, periodic listings identifying these overpayments were sent to Plans to initiate refunds. Once this change was made, the final listings of overpayments caused by the lack of the "AS" modifier reduction were sent to Plans to initiate recoveries.

## **b. Chiropractic Spinal Manipulations Accumulator**

In two test scenarios, chiropractic benefits related to spinal manipulations were incorrectly applied. In the first test scenario, the OIG submitted two claims into the Flexx system with a total of 16 spinal manipulations. One manipulation on the second claim denied because it was a duplicate of a manipulation on the first claim. Although the denied manipulation was not paid, the system's accumulator counted this manipulation against the allowed amount, and the subscriber only received benefits for 11 manipulations.

In the second test scenario, the OIG submitted two claims into the FEP Express system with a total of 16 manipulations. One manipulation on the second claim had the same date and provider, but a different procedure code, as a manipulation on the first claim. The system's accumulator only counted these two manipulations as one, and the subscriber received benefits for 13 manipulations.

### **OIG Recommendation 6**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that chiropractic spinal manipulation benefits are applied correctly.

### **Response to Recommendation 6**

First, we would like to clarify that the accumulation of the number of manipulations is a FEPEXpress function. We conducted the same type of testing performed by the OIG auditors in an effort to determine whether there are any issues with the manner in which FEPEXpress accumulates the number of manipulations per year. We did not receive the same results as the ones obtained by the OIG auditors. Attachment A contains copies of our test results using the FEP reporting requirements for this service.

We could not get the system to pay more than 12 manipulations using the normal processing method. The system deferred the claim with the 13<sup>th</sup> manipulation (Note that this deferral is not over-rideable). However, we do have a process in our system in which more than the 12 manipulations can be paid if the services are submitted as Plan Approved which is used for our Case Management services. For Case Management services, members are allowed to exceed the established maximums, if it is deemed as a cost effective treatment method to improve or maintain the member's health. Our review indicates that the FEP system is correctly accumulating these services and no changes are required at this time.

**c. Chiropractic Office Visits and X-rays**

The BCBS FEP benefit structure allows for one chiropractic office visit and one set of x-rays each calendar year. However, in two test scenarios, benefits were paid for multiple office visits for one subscriber.

**OIG Recommendation 7**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that subscribers receive benefits for only one chiropractic office visit and one set of x-rays each calendar year.

**Response to Recommendation 7**

The 2008 Blue Cross Blue Shield Service Benefit Brochure states on page 46, "initial office visit" for a Chiropractor. During late 2007, we became aware of the difficulty in the administration of this benefit due to the language used. Initially, an edit was put in the FEP system to limit the benefit to one visit. However, because the brochure reads initial visit, we had to remove the edit as there was no definition provided to the members to define whether initial office visit meant per Chiropractor or per episode or per benefit period. As a result, we have made a request for a Contract modification to change the word "initial" to "one" visit. This request was submitted with the 2009 Benefit Changes/Clarifications. The results of the 2009 Benefit negotiations have not yet been published. Once this information is made available, we will provide an update to our response.

**d. Chiropractic Diagnosis**

A test claim was processed where benefits were paid for chiropractic spinal manipulations associated with an inappropriate diagnosis.

**OIG Recommendation 8**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a subscriber's diagnosis is evaluated for appropriateness before chiropractic benefits are paid.

**Response to Recommendation 8**

Medical Edits are the responsibility of the local Plans. Please reference the Attachment B for a copy of FEP Administrative Manual Volume I, Chapter 15 – 107 for a description of this requirement. It would be a duplication of efforts and costly to the Program for FEPEXpress to contain the various medical policies for each specific Plan as well as requiring numerous Plan specific edits.

CareFirst will work with the FEP Director's Office to re-evaluate its medical edits in an effort to determine what local system edits may require enhancements in order to ensure that these types of situations are pended for review of the medical appropriateness of the services prior to payment. We estimate that this evaluation will be completed by the end of first quarter 2009.

**e. Multiple Procedure Instances**

Two test claims were processed and paid for a subscriber receiving the same surgical procedure twice in one day from different providers.

**OIG Recommendation 9**

We recommend that CareFirst/FEPOC incorporate the appropriate edits into FEP Express that will allow the system to identify and suspend claims that are identical to previously processed claims in all fields except for the provider.

We acknowledge the fact that, for certain procedures, it may be possible to have the same type of service rendered on the same day by different providers. The system could be programmed to selectively apply the new edit based on the procedure in question. In order to avoid hindering the efficiency of the edit process, the edit could be designed to bypass entire classes of procedures where multiple same-day instances of a procedure are likely to occur (e.g., office visits, lab tests, dental procedures).

### **Response to Recommendation 9**

There are surgical procedures that are normally performed one time; however, we have encountered a number of exceptions with these procedures. Sometimes, only a partial procedure is performed or the first procedure was unsuccessful and it must be performed again. An example of such a procedure would be a vasectomy. If the procedure was unsuccessful, it can be re-performed at the patient's request.

The example used by the OIG auditors was a vasectomy performed on the same day by two different providers. Because the example included two different providers, the claim did not defer on FEPEXpress as a possible duplicate. Different providers are not part of the FEP System Duplicate Criteria. However, the question with the two vasectomies is the medical appropriateness of two doctors performing this procedure on the same day, on the same member. Since this is not accepted medical practice (Local Medical Policy) for the CareFirst service area, the second claim correctly deferred on the FLEXX System. This is the correct process as Medical Edits are housed at the local Plans. However, the claim paid on FEPEXpress as there are no Medical Edits on FEPEXpress.

If the OIG auditors can provide FEP with a listing of the procedures that should be included in a new edit that is designed to limit members to one surgical service per lifetime, we will evaluate the feasibility of limiting these services. At this time, we cannot determine the types of surgical procedures that we should limit members to one per lifetime. Therefore, no changes will be made to the FEPEXpress at this time.

### **f. Procedure Bundling**

A test claim containing multiple laboratory procedures was not appropriately bundled.

### **OIG Recommendation 10**

We recommend that CareFirst/FEPOC implement the appropriate modifications to FEP Express to ensure that the system can appropriately process claims where procedure bundling is required.

### **Response to Recommendation 10**

The bundling of like medical services is based upon local medical policies and is considered a Medical Edit that is handled at the Plan level. The test claims processed through FLEXX were appropriately bundled by ClaimCheck which performs various medical edits/bundling for the Plan. The auditors also submitted the unbundled claims directly to FEPEXpress, which appropriately did not bundle these services as the bundling process is not maintained on FEPEXpress. As a result, no changes are required to the FEPEXpress.

### **g. Procedure to Diagnosis Inconsistency**

A test claim was processed where benefits were paid for a procedure associated with an inappropriate diagnosis. The OIG entered a test claim into the FEPEXpress system with a procedure code for a transurethral incision of the prostate and a diagnosis of an ankle fracture. The system processed and paid the claim without triggering any edits.

### **OIG Recommendation 11**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a subscriber's diagnosis is evaluated for appropriateness before benefits are paid.

### **Response to Recommendation 11**

The determining of whether the services are related to the diagnosis requires Medical Edits to defer the claim for review. Medical Edits are maintained at the Plan level. The test claim in question processed correctly in the local Plan system. However, the auditors also processed the test claim directly in FEPEXpress, which appropriately did not edit the claim for diagnosis/procedure compatibility since such edits reside in the local system. Therefore, no changes are required to FEPEXpress.

#### **h. Non-Participating Provider Pricing**

A non-participating (non-par) provider was paid an amount significantly greater than the amount allowed by the Medicare fee schedule.

##### **OIG Recommendation 12**

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that non-par provider claims are suspended for review when there is a large variance between the NPA and the Medicare fee schedule. CareFirst/FEPOC will need to determine an acceptable variance above which the claims should be suspended.

##### **Response to Recommendation 12**

Non-Par professional claims are priced by FEPEXpress. We are currently conducting a study to determine the specifications required to implement an edit that would defer any non-par priced claim that exceeds 40% of the Medicare Fee Schedule. The results of the study are expected during the fourth quarter 2008 with implementation of the recommendation in 2009.

#### **i. OBRA '90 Transfer**

An OBRA '90 test claim was incorrectly processed as a transfer claim. The OIG submitted an OBRA '90 test claim into FEP Express that included a discharge status of '43', and the system processed and paid this claim as a transfer. However, OPM Carrier Letter 2007-6, "OBRA '90 IPPS PRICER Program Usage," states that only claims with a discharge status of '02' should be processed as transfers.

##### **OIG Recommendation 13**

We recommend that CareFirst/FEPOC implement the necessary system modifications to ensure compliance with the requirements of OPM Carrier letter 2007-6.

**Response to Recommendation 13**

OBRA '90 Pricing is a function of FEPEXpress. When the system changes to comply with OPM Carrier letter 2007-6 was implemented, patient status "43" was incorrectly included in the transfer application in the OBRA '90 Pricer. As a result, these claims may have been underpaid. We were aware of this issue from previous audits of other Plans. The system correction to limit the OBRA'90 Transfer pricing to patient status "02" will be implemented on October 18, 2008.

We appreciate the opportunity to provide our response to this Draft Audit Report and would request that our comments be included in their entirety as part of the Final Audit Report.

Sincerely,

Robert C. McMillan,  
Executive Director  
Program Integrity  
Financial Services, Audit and Compliance

RM/jb

Attachments

cc: Shirley Patterson, OPM  
Gentry Israel, Director, CareFirst BCBS  
Danita Andrews, FEP