UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

June 23, 2011

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Follow-up Review of Information Systems General and Application Controls at CareFirst BlueCross BlueShield and the Federal Employee Program Operations Center (REPORT NO. 1A-10-85-11-029)

The purpose of this memorandum is to communicate to you the findings and conclusions resulting from our follow-up review of information systems general and application controls conducted at CareFirst BlueCross BlueShield (CareFirst) and the Federal Employee Program Operations Center (FEPOC). We initiated the review because of concerns regarding several instances of premature closure of recommendations stemming from information technology (IT) audits of Federal Employees Health Benefits Program insurance carrier systems.

The original audit of CareFirst and the FEPOC was scheduled in 2008 because of the high risk associated with this health plan. CareFirst is the largest plan in the BlueCross BlueShield (BCBS) service benefit plan. In addition, CareFirst hosts the FEPOC, which is the entity that manages the national claims processing system (FEP Express) for the BCBS Federal Employee Program – all claims for BCBS federal members are processed by this system.

As a result of our audit we made 13 recommendations for improvement in a wide range of business process and technical areas, including the overall IT security environment, business continuity, access controls, and application processing controls for the FEP Express system. Several of the recommendations were made to correct systemic problems that impacted not just the CareFirst plan, but all BCBS plans using FEP Express to process federal employee claims.

In May 2010, we discovered that all recommendations were closed by the Healthcare and Insurance Office (HIO) without proper documentation that corrective action had been completed. In accordance with OMB Circular A-50 and by longstanding custom, my office shares responsibility for audit resolution by reviewing corrective actions and rendering an opinion regarding their relevance and effectiveness at mitigating the weaknesses identified during our audits. In this case, we were not involved in this process. Closing audit recommendations without following the established processes not only allows health plans to avoid correcting significant weaknesses, but it also wastes limited audit resources expended to identify the weaknesses in the first place.

Executive Summary

The original audit report detailed 13 weaknesses in the information systems general and application controls at CareFirst/FEPOC. The objective of this follow-up review was to evaluate the current status of each recommendation and determine which, if any, of the recommendations should be re-opened. We concluded that 9 of the 13 recommendations were adequately addressed, but that 4 recommendations had not been fully implemented. This report also contains two new recommendations that address the following outstanding weaknesses:

- CareFirst Business Impact Assessment (BIA): As part of the overall risk management process, CareFirst conducted a BIA to evaluate the degree to which disruptions to various business processes would have on the organization as a whole. However, we found that the CareFirst BIA had not been updated since March 2005 – three years prior to the original audit. As of April 2011, the CareFirst BIA still has not been updated.

- Comprehensive Medical Edits: The original test of FEPOC's FEP Express claims processing application revealed that this system did not have adequate [redacted] in insurance claims. It is common practice for health claims processing systems to include such controls to prevent payments for abusive or fraudulent billing. As of April 2011, FEP Express has still not been modified to address these weaknesses, which affect claims processed by all BlueCross BlueShield plans ($25.6 billion in 2010).

Background

Audit report 1A-10-92-08-021 was issued on November 28, 2008 with 13 audit recommendations. On May 17, 2010, HIO sent a closure letter to the BlueCross BlueShield Association (BCBSA) indicating that all 13 recommendations were being closed. However, at this time it was clear that several recommendations should have remained open, as the BCBSA had not provided evidence to HIO indicating that all corrective action had been implemented.

The issuance of the HIO closure letter created the possibility that CareFirst/FEPOC would halt its ongoing efforts to remediate the weaknesses identified during the audit. As a result of this concern, we initiated this follow-up review to determine the current status of the original audit recommendations and reopen any that had still not been completed.

Scope and Methodology

The scope of this review was limited to the business processes where weaknesses were identified during the original audit, including:

- BIAs;
- Firewall management;
- [redacted] management; and
- Claims adjudication controls.

In conducting this review we gathered documentation and conducted interviews related to remediation activity CareFirst/FEPOC has completed to address our original audit recommendations. Various laws, regulations, and industry standards were used as a guide to evaluate the CareFirst/FEPOC control structure. These criteria include, but are not limited to:

- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- Health Insurance Portability and Accountability Act of 1996;
- Omnibus Budget Reconciliation Act of 1990 (OBRA 90);
- Omnibus Budget Reconciliation Act of 1993 (OBRA 93); and
- Federal Information System Controls Audit Manual.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a review, the documentation, reporting, and quality control standards are not as rigorous.

Review Follow Up

In accordance with Office of Management and Budget (OMB) Circular A-50 and/or Public Law 103-355, all findings must be resolved within six months of the date of this report. In order to ensure findings are resolved within the required six-month period, we ask that the Healthcare and Insurance Office (HIO) respond directly to the Office of the Inspector General (OIG) within 90 days of the date of the report advising us whether they agree or disagree with the findings and recommendations. As stated in OMB Circular A-50, where agreement is indicated, the HIO should describe planned corrective action. If the HIO disagrees with any of the findings and recommendations, we need them to explain the reason for the disagreement and provide any additional documentation that would support their opinion.

Since this office exercises oversight regarding the progress of corrective actions, we also request that the HIO provide the OIG a report within six months describing corrective action taken. If the corrective action has not been completed, we also ask that the HIO continue to provide us with a report on the status of corrective action every March and September thereafter until action has been completed.

Results

The following sections outline the results of our follow up review of information systems general and application controls at CareFirst/FEPOC.

1. Business Impact Assessments (BIA)

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

a) 2008 Recommendation 1 – FEPOC BIA

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

2008 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."

2011 Status:

We confirmed that the FEPOC BIA was updated in September 2009. FEPOC plans to incorporate the results of the BIA into an update of its disaster recovery plan during 2011; this recommendation is closed.

b) 2008 Recommendation 2 – CareFirst BIA

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.

2008 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."

2011 Status:

As of April 2011 the CareFirst BIA has not been updated. CareFirst is in the planning stages for completing a BIA by December 31, 2011. CareFirst stated that the delay was the result of significant organizational and platform changes during the last 3 years, and that it would not have been a good use of resources to perform a BIA during this transformation.

2011 Recommendation 1

We recommend that CareFirst update its BIA and incorporate the results into the CareFirst disaster recovery plan. The BIA and disaster recovery plan should be reviewed on an annual basis and updated when necessary.

2. Firewall Management

CareFirst has established an IT security team at its data center that is responsible for configuring and maintaining the organization's firewalls. However, CareFirst has not established a corporate policy detailing firewall configuration requirements.

a) 2008 Recommendation 3 – Firewall Configuration Policy

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.

2008 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."

2011 Status:

We confirmed that CareFirst has implemented a firewall configuration policy; this recommendation is closed.

3. [redacted] Management

CareFirst uses [redacted] security software to govern access to mainframe applications. The [redacted] requirements for [redacted] are defined by the "[redacted]" outlined in the [redacted]. The OIG reviewed CareFirst's [redacted] and concluded that the [redacted] requirements are configured in a manner that is not consistent with CareFirst policy or industry acceptable best-practice.

a) 2008 Recommendation 4 – [redacted]

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

2008 BCBSA Response:

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

2011 Status:

CareFirst has not implemented the recommended system change and has formally accepted all associated risk. CareFirst stated that the system change was not feasible because of the impact the change would have on legacy claims processing applications. This recommendation is closed based on CareFirst's risk acceptance, but we advise CareFirst to continue to evaluate the feasibility of implementing the recommendation as legacy systems are decommissioned.

4. Claims adjudication controls

To validate the claims adjudication controls, a testing exercise was conducted on CareFirst/FEPOC's 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. The following system weaknesses were identified during this testing:

- incorrect pricing of claims involving special rules for certain categories of federal members (OBRA 90 and OBRA 93);
- incorrect application of [redacted] benefits, including a scenario where [redacted] was provided for an [redacted];
- lack of medical edits to prevent payment for common scenarios such as:
  - [redacted] provided to a patient by [redacted]
  - [redacted];
  - [redacted]
- no control to prevent [redacted].

a) 2008 Recommendation 5 – OBRA 93 Pricing

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

2008 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."

2011 Status:

The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

b) 2008 Recommendation 6 – [redacted]

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that [redacted] are applied correctly.

2008 BCBSA Response:

"First, we would like to clarify that the [redacted] *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* [redacted] *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."*

2011 Status:

The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

c) 2008 Recommendation 7- Chiropractic Office Visits and X-rays

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.

2008 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."

2011 Status:

We confirmed that the recommended system modifications have been implemented; this recommendation is closed.

d) 2008 Recommendation 8 – [redacted]

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a [redacted] is evaluated for appropriateness before [redacted] are paid.

2008 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."

2011 Status:

This recommendation resulted from a test claim that was processed where benefits were paid for [redacted] associated with an [redacted]. This scenario illustrates a medical inconsistency that would typically be detected by comprehensive medical edit software.

We have audited multiple BCBS Plans and have documented an extreme inconsistency in the effectiveness of the medical edits implemented on each Plan's local claims processing system. Some Plans have very thorough medical edits from in-house developed systems or the use of third-party medical edit software. [redacted]

[redacted]

We believe that the most effective way to ensure that all BCBS FEP claims are subject to the same level of quality control is to install comprehensive medical edit software on FEP Express.

2011 Recommendation 2

We recommend that CareFirst/FEPOC implement comprehensive medical edit capabilities on FEP Express.

e) 2008 Recommendation 9 – [redacted]

We recommend that CareFirst/FEPOC incorporate the appropriate edits into FEP Express that will allow the system to identify and suspend claims that are [redacted].

We acknowledge the fact that, for certain procedures, it may be possible to have the [redacted] 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 [redacted]

2008 BCBSA Response:

"There are [redacted] *; however, we have encountered a number of exceptions with these procedures. Sometimes,* [redacted]

The example used by the OIG auditors was a [redacted] *Because the example included* [redacted] *the claim did not defer on FEPExpress as a* [redacted]*. are not part of the FEP System* [redacted]*. However, the question with the* [redacted] *Since this is not accepted medical practice (Local Medical Policy) for the CareFirst service area,* [redacted] *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 [redacted] *we will evaluate the feasibility* [redacted]*. At this time, we cannot determine the types of* [redacted] *Therefore, no changes will be made to the FEPExpress at this time."*

2011 Status:

This recommendation resulted from two test claims that were processed and paid for a subscriber [redacted] This scenario illustrates a medical inconsistency that would typically be detected by comprehensive medical edit software.

As mentioned in section 4(e), we believe that the most effective way to ensure that all BCBS FEP claims are subject to the same level of quality control is to install comprehensive medical edit software on FEP Express; see recommendation 2, above.

f) 2008 Recommendation 10 – [redacted]

We recommend that CareFirst/FEPOC implement the appropriate modifications to FEP Express to ensure that the system can appropriately process claims where [redacted].

2008 BCBSA Response:

"[redacted] *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* [redacted] *by ClaimCheck which performs various medical edits/bundling for the Plan. The auditors also submitted the* [redacted] *directly to FEPExpress, which appropriately* [redacted] *these services as the* [redacted] *is not maintained on FEPExpress. As a result, no changes are required to the FEPExpress."*

2011 Status:

We believe that the most effective way to ensure that all BCBS FEP claims are subject to the same level of quality control is to install comprehensive medical edit software on FEP Express. However, we acknowledge that implementing [redacted] on FEP Express would require each BCBS Plan to modify their system to [redacted] after they have processed through FEP Express. We agree that implementing this control would not be cost effective; this recommendation is closed.

g) 2008 Recommendation 11 – [redacted]

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that a [redacted] before benefits are paid.

2008 BCBSA Response:

"The determining of whether the [redacted] *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 [redacted]y since such edits reside in the local system. Therefore, no changes are required to FEPExpress."

2011 Status:

This recommendation resulted from a test claim where benefits were paid for [redacted]. This scenario illustrates a [redacted] that would typically be detected by comprehensive medical edit software.

As mentioned in section 4(e), we believe that the most effective way to ensure that all BCBS FEP claims are subject to the same level of quality control is to install comprehensive medical edit software on FEP Express; see recommendation 2, above.

h) 2008 Recommendation 12 – Non-participating Provider Pricing

We recommend that CareFirst/FEPOC implement the appropriate system modifications to ensure that non-par provider claims are suspended for review when [redacted] CareFirst/FEPOC will need to determine an acceptable variance above which the claims should be suspended.

2008 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 d[redacted] The results of the study are expected during the fourth quarter 2008 with implementation of the recommendation in 2009."

2011 Status:

The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

i) 2008 Recommendation 13 – OBRA 90 Transfer

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

2008 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."

2011 Status:

The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

cc: John O'Brien
Director, Healthcare and Insurance

Shirley Patterson
Assistant Director for Federal Employee Insurance Operations