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

# Final Audit Report

## AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT CAREFIRST BLUECROSS BLUESHIELD

**Report Number 1A-10-85-20-021**
**December 28, 2020**

# EXECUTIVE SUMMARY

*Audit of the Information Systems General and Application Controls at CareFirst BlueCross BlueShield*

**Report No. 1A-10-85-20-021** **December 28, 2020**

**Why Did We Conduct The Audit?**

CareFirst BlueCross BlueShield (CareFirst) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in CareFirst's information technology (IT) environment.

**What Did We Audit?**

The scope of the audit centered on the information systems used by CareFirst to process and store data related to medical encounters and insurance claims for FEHBP members as of April 2020.

**Michael R. Esser**
**Assistant Inspector General for Audits**

**What Did We Find?**

Our audit of CareFirst's IT security controls determined that:

- CareFirst has implemented controls to manage risk and the security of its IT environment. However, CareFirst does not require individuals with IT responsibilities to have specialized role-based training.
- CareFirst has implemented controls to manage both logical access to information systems and physical access to CareFirst facilities.
- CareFirst has implemented perimeter controls to protect external access to its internal network. [redacted]
- CareFirst has documented security configuration standards for its systems. However, CareFirst does not routinely scan some systems for compliance with its approved configuration standards.
- CareFirst has documented contingency plans to limit effects of adverse events.
- CareFirst has implemented application controls to protect the information and adjudication of claims through its claims processing system.
- The draft audit report contained three recommendations related to the weaknesses mentioned above. All three recommendations were implemented subsequent to the issuance of the draft audit report.

# ABBREVIATIONS

| | |
|---|---|
| **CareFirst** | **CareFirst BlueCross BlueShield** |
| **CFR** | **Code of Federal Regulations** |
| **FEHBP** | **Federal Employees Health Benefits Program** |
| **FEP** | **Federal Employee Program** |
| **FISCAM** | **Federal Information Systems Controls Audit Manual** |
| **GAO** | **U.S. Government Accountability Office** |
| **IT** | **Information Technology** |
| **NIST SP** | **National Institute of Standards and Technology Special Publication** |
| **OIG** | **Office of the Inspector General** |
| **OPM** | **U.S. Office of Personnel Management** |

# TABLE OF CONTENTS

# I. BACKGROUND

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

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

The FEHBP was established by the Federal Employees Health Benefits Act 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, or comprehensive medical services.

This was our third audit of general and application controls at CareFirst. The previous audits of CareFirst were conducted in 2008 and 2011. The Final Audit Report No. 1A-10-85-08-021 was issued on November 28, 2008, and the Final Audit Report No. 1A-10-85-11-029 was issued on June 23, 2011. All recommendations from the previous audits have been closed.

All CareFirst personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

# II. OBJECTIVES, SCOPE, AND METHODOLOGY

## OBJECTIVES

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

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

## SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of CareFirst's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of CareFirst's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by CareFirst to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Owings Mills, Maryland.

The onsite portion of this audit was performed in February of 2020. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at CareFirst as of April 2020.

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

In conducting this audit we:

- Performed a risk assessment of CareFirst's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM);

- Gathered documentation and conducted interviews;

- Reviewed CareFirst's business structure and environment; and

- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

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

- GAO's FISCAM; and

- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

## COMPLIANCE WITH LAWS AND REGULATIONS

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

# III. AUDIT FINDINGS AND RECOMMENDATIONS

## A. SECURITY MANAGEMENT

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

CareFirst has implemented a series of formal policies and procedures that govern its security management program. CareFirst has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. CareFirst also has implemented human resources policies and procedures related to hiring, transferring, and terminating employees.

However, we noted the following opportunity for improvement related to CareFirst's security management program.

### 1. Specialized Training

CareFirst requires annual IT security and privacy awareness training for all employees. However, CareFirst does not ensure individuals with specialized IT responsibilities receive technical training specific to their job function.

**CareFirst does not require specialized training for individuals with IT responsibilities.**

NIST SP 800-53, Revision 4, states, "The organization provides role-based security training to personnel with assigned security roles and responsibilities … ."

Failure to provide role-based technical training for IT staff increases the risk that these individuals are not adequately prepared to identify and address constantly evolving IT threats.

**Recommendation 1**

We recommend that CareFirst require specialized training for employees with significant security roles and responsibilities.

**CareFirst Response:**

***"CareFirst agrees with the recommendation and has implemented a program to provide specialized security training to personnel with significant roles and responsibilities (Attachment 1). This was implemented on July 1, 2020."***

**OIG Comment:**

In response to the draft audit report, CareFirst provided evidence that it has implemented specialized training requirements for employees with significant security roles and responsibilities; no further action is required.

## B. ACCESS CONTROLS

### 1. Logical Access

Logical access controls are procedures, policies, and techniques used to inhibit or identify unauthorized access to an organization's system, applications, processes, and information.

We examined logical access controls on CareFirst's network environment and claims processing applications during this audit.

We observed the following controls in place:

- Identification and authentication policies and procedures to gain access to CareFirst's systems;
- Procedures and policies for granting, removing, and adjusting system and application access; and
- Procedures and policies for the review and audit of user accounts.

Nothing came to our attention to indicate that CareFirst has not implemented adequate prevention and detection controls related to logical access.

### 2. Physical Access

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

We examined the physical access controls at CareFirst's facilities and data centers and observed the following controls in place:

- Identification and authentication policies and procedures to gain access to CareFirst's facilities;

- Procedures and policies for granting, removing, and adjusting facility and data center access; and

- Procedures and policies for the review and audit of physical access permissions.

Nothing came to our attention to indicate that CareFirst has not implemented adequate prevention and detection controls related to physical access.

## C. NETWORK SECURITY

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

We evaluated the CareFirst network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;

- Network segmentation controls separating users from sensitive internal resources; and

- Documented policies and procedures to identify and respond to information security incidents.

However, we noted the following opportunity for improvement related to CareFirst's network security controls.

### 1. Network Access Controls

[redacted] CareFirst is currently in the process of rolling out a tool [redacted]

NIST SP 800-53, Revision 4, suggests that "The information system uniquely identifies and authenticates [devices] before establishing a [network] connection."

Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

**Recommendation 2**

We recommend that CareFirst implement network access controls [redacted]

**CareFirst Response:**

***"CareFirst agrees with the recommendation and has implemented network access controls [redacted] (Attachment 2). This was implemented on July 13, 2020."***

**OIG Comment:**

In response to the draft audit report, CareFirst provided evidence that it has implemented network access controls that block unauthorized devices from connecting to the wired internal network; no further action is required.

## D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. CareFirst employs a team of technical personnel who manage system software configuration for the organization.

We evaluated CareFirst's management of the configuration of its computer servers and databases. Our review found the following controls in place:

- Documented system change control process; and

- Established patch management process.

The following section documents an opportunity for improvement related to CareFirst's configuration management program.

**1. Secure Configuration Auditing**

CareFirst has documented security configuration standards for all operating platforms in its environment. CareFirst performs routine configuration scans on its Windows systems and some of its other operating platforms using an automated tool to verify that systems are in compliance with approved standards. However, CareFirst does not perform routine configuration audits on all operating platforms in its environment.

NIST SP 800-53, Revision 4, requires that organizations routinely check the security configurations for all systems, and FISCAM requires that "Current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement configuration compliance auditing using approved security configuration standards increases the risk of inappropriately configured systems. Undetected misconfigurations can create a potential gateway for unauthorized access or malicious activity.

**Recommendation 3**

We recommend that CareFirst improve its configuration compliance auditing process to ensure that all operating platforms are routinely audited for compliance with the approved security configuration standards.

**CareFirst Response:**

***"CareFirst agrees with the recommendation and has enabled compliance scanning (Attachment 3) for the two operating platforms in question (Attachment 4-5). This was implemented on July 26, 2020."***

**OIG Comment:**

In response to the draft audit report, CareFirst provided evidence it has improved its compliance auditing process by including all operating platforms in the scope of its compliance scanning; no further action is required.

## E. CONTINGENCY PLANNING

Contingency planning consists of procedures and policies that ensure sufficient availability of critical data and operations, information systems, and business processes.

We reviewed CareFirst's contingency planning documentation and processes to prevent or minimize interruptions to CareFirst's business operations if disruptive events were to occur. We identified the following controls in CareFirst's contingency planning process:

**CareFirst has implemented plans to minimize business disruptions from adverse events.**

- Contingency plans including disaster recovery and business continuity plans;
- Contingency plan testing and follow-up; and
- Data center emergency response procedures.

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

## F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting CareFirst's claims adjudication process for preferred provider organization members. CareFirst receives claims using a system called Federal Employee Program (FEP) Bridge and adjudicates claims using the Blue Cross Blue Shield Association's nationwide FEP Direct system. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, and provider debarment.

### 1. Application Change Control

We evaluated the policies and procedures governing application development and change control over CareFirst's claims processing system.

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

- Unit and system integration testing are conducted in accordance with industry standards; and

- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

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

## 2. Claims Processing System

We evaluated the business process controls associated with CareFirst's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that CareFirst has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;

- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and

- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that CareFirst has not implemented adequate controls over its claims processing system.

## 3. Debarment and Suspension

CareFirst has documented procedures that require monitoring for debarred or suspended providers. CareFirst's credentialing department maintains its provider database and is responsible for monitoring for sanctions. When CareFirst receives a list of debarred providers, the provider names are checked against the existing database. If a match is found, CareFirst updates the explanation of benefit information in the claims processing system and the provider information in the database.

Nothing came to our attention to indicate that CareFirst has not implemented adequate controls over the debarment and suspension process.

# APPENDIX

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans
Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

October 21, 2020

[redacted] Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management (OPM)
1900 E Street, NW
Room 6400
Washington, D.C. 20415-1100

**Reference: OPM DRAFT IT AUDIT REPORT**
**CareFirst Blue Cross Blue Shield (CareFirst)**
**Audit Report Number 1A-10-85-20-021**
**(Dated August 27, 2020)**

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

## A. SECURITY MANAGEMENT

### Specialized Training

***Recommendation 1***

We recommend that CareFirst require specialized training for employees with significant security roles and responsibilities.

***Plan Response***

CareFirst agrees with the recommendation and has implemented a program to provide specialized security training to personnel with significant roles and responsibilities (**Attachment 1**). This was implemented on July 1, 2020.

## B. ACCESS CONTROLS

**No recommendation noted.**

## C. NETWORK SECURITY

### Network Access Controls

***Recommendation 2***

We recommend that CareFirst implement network access controls [redacted]

***Plan Response***

CareFirst agrees with the recommendation and has implemented network access controls [redacted]

(**Attachment 2**). This was implemented on July 13, 2020.

## D. CONFIGURATION MANAGEMENT

### Secure Configuration Auditing

***Recommendation 3***

We recommend that CareFirst improve its configuration compliance auditing process to ensure that all operating platforms are routinely audited for compliance with the approved security configuration standards.

***Plan Response***

CareFirst agrees with the recommendation and has enabled compliance scanning (**Attachment 3**) for the two operating platforms in questioned (**Attachment 4-5**). This was implemented on July 26, 2020.

## E. CONTINGENCY PLANNING

**No recommendation noted.**

## F. Claims Adjudication

**No recommendation noted.**

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

Sincerely,

[redacted]

[redacted]

Managing Director, FEP Program Assurance

cc: [redacted], OPM
[redacted], FEP
[redacted], FEP

# Report Fraud, Waste, and Mismanagement

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

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

**By Phone:**

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

**By Mail:**

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