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

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT SCOTT AND WHITE HEALTH PLAN

Report Number 1C-A8-00-20-019
December 14, 2020

EXECUTIVE SUMMARY

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT SCOTT AND WHITE HEALTH PLAN

Report No. 1C-A8-00-20-019 **December 14, 2020**

Why Did We Conduct The Audit?

The Scott and White Health Plan (SWHP) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP). Baylor Scott & White Health (BSWH) provides information technology and security services to SWHP.

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

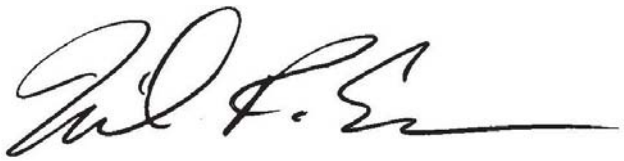
What Did We Audit?

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

What Did We Find?

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

- BSWH has developed an adequate risk management methodology and created remediation plans to address weaknesses identified during risk assessments.
- BSWH has not performed IT security control risk assessments of its third party vendors.
- BSWH has firewalls at the edge of its network to control traffic from external connections and vendors.
- [redacted]
- [redacted]
- BSWH has an established incident response program, [redacted]
- BSWH has documented and implemented a system change control process.
- BSWH has not established [redacted]



Michael R. Esser
Assistant Inspector General for Audits

ABBREVIATIONS

BSWH	**Baylor Scott and White Health**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
SWHP	**Scott and White Health Plan**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 4

A. SECURITY MANAGEMENT 4

1. Vendor Risk Assessments 4

B. NETWORK SECURITY 5

1. Internal Network Segmentation 6
2. Network Access Control 6
3. Firewall Configuration Standard 7
4. Firewall Auditing 9
5. Credentialed Vulnerability Scanning 10
6. Vulnerabilities Identified by OIG Scans 10

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE 11

1. Incident Response Testing 11

D. CONFIGURATION MANAGEMENT 12

1. Security Configuration Standards 13
2. Security Configuration Auditing 14

APPENDIX: BSWH's September 21, 2020, response to the draft audit report, issued July 21, 2020.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

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

The audit was conducted pursuant to FEHBP contract CS 2942; 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, indemnity benefits, or comprehensive medical services.

Baylor Scott and White Health (BSWH) is the parent company of SWHP and provides all of the information technology (IT) infrastructure and security services to SWHP. This was our first audit of the IT general security controls at BSWH. All BSWH 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 BSWH's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Network security;
- Incident response; and
- Configuration management.

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 BSWH's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of BSWH'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 BSWH to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Dallas, Texas.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general controls in place over BSWH's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at BSWH as of June 2020.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BSWH. 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 BSWH'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 BSWH'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 BSWH's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy; and

- 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 BSWH's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, BSWH 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 the examination of the policies and procedures that are the foundation of BSWH's overall IT security program. We evaluated BSWH's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BSWH has implemented a series of formal policies and procedures that govern their security management program. The Plan has also developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

The following section documents an opportunity for improvement related to BSWH's security management program.

1. Vendor Risk Assessments

BSWH contracts with several vendors that perform business processes related to health claims processing. However, BSWH has not performed risk assessments of the IT security controls implemented by these vendors to protect the sensitive data they handle.

BSWH has not performed risk assessments of the IT security controls of its third party vendors.

NIST SP 800-53, Revision 4, states that "Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities)."

Failure to conduct risk assessments on all vendors to identify relevant threats, vulnerabilities, impacts, and likelihoods could leave BSWH unknowingly susceptible to adverse events.

Recommendation 1

We recommend that BSWH implement a formal process to assess vendor risk prior to service acquisition and then periodically over the course of the relationship. This process should also be applied to all existing vendors.

BSWH's Response:

"BSWH performs a vendor security program review prior to service acquisition or at renewal of contract as part of the BSWH Information Security Agreement (ISA). Vendors are required to maintain security at the level described in the ISA, or higher, throughout the duration of the agreement. BSWH acknowledges that a more robust vendor risk assessment pre-contracting, and periodic vendor risk assessments during the life of the contract, would strengthen the overall security posture of BSWH. Implementation of a more robust formal vendor risk assessment process is in progress [redacted]."

OIG Comment:

As a part of the audit resolution process, we recommend that BSWH provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement also applies to subsequent recommendations in this audit report that BSWH agrees to implement.

B. 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 BSWH's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

BSWH has firewalls at the edge of its network to control network traffic from external connections.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Adequate remote access controls; and
- Internal controls to filter web content.

The following sections document several opportunities for improvement related to BSWH's network security controls.

1. Internal Network Segmentation

Firewalls are used at ingress and egress locations on BSWH's network in order to control network traffic from external connections and vendors. A demilitarized zone is used to segregate externally accessible systems in BSWH's network. [redacted]

NIST SP 800-41, Revision 1, advises that [redacted]

[redacted]

Recommendation 2

We recommend that BSWH [redacted]

BSWH's Response:

"BSWH prior to the audit was actively engaged in a broad multi-year network segmentation program. The SWHP related segmentation, [redacted] ***."***

2. Network Access Control

[redacted]

This issue is compounded

NIST SP 800-53, Revision 4, states that an information system should [redacted]

[redacted]

Recommendation 3

We recommend that BSWH complete [redacted]

BSWH's Response:

"BSWH accepts this recommendation, only as it relates to [redacted]. Prior to the audit, BSWH was actively engaged in a broad multi-year network segmentation program [redacted], BSWH disagrees with this finding. BSWH does have applicable controls in place and evidence of same was provided on June 10, 2020 (IR-10)."

OIG Comment:

We agree that this recommendation only [redacted] and that BSWH has adequate network access controls in place [redacted]. We have updated the language in the final report to more accurately reflect the controls in place at BSWH.

3. Firewall Configuration Standard

BSWH maintains a [redacted]

NIST SP 800-41, Revision 1, explains that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies."

NIST SP 800-53, Revision 4, [redacted]

[redacted]

Recommendation 4

We recommend that BSWH [redacted]

BSWH's Response:

"BSWH does not accept these recommendations, BSWH has an effective firewall configuration process in place and documented that includes the elements stated in NIST SP 800-41. Appropriate evidence of this effective firewall configuration process with appropriate controls has been provided."

OIG Comment:

BSWH provided two documents to demonstrate that it had documented its firewall configuration near the end of our audit fieldwork, BSWH's Network Operations and Security Standard and Firewall Configuration Standard. Combined, these two documents include the majority of elements stated in NIST SP 800-41, Revision 1. However, the Firewall Configuration Standard appeared to be in draft form due to the watermark on the document and the fact that it was created during our audit fieldwork. In response to the draft audit report, BSWH provided the same two documents including the draft of the Firewall Configuration Standard. We recommend that BSWH provide OPM's Healthcare and Insurance Office, Audit Resolution Group with the fully implemented version of the Firewall Configuration Standard.

Recommendation 5

We recommend that BSWH implement a process to [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 4 are in place.

BSWH's Response:

"BSWH does not accept these recommendations, BSWH has an effective firewall configuration process in place and documented that includes the elements stated in NIST SP 800-41. Appropriate evidence of this effective firewall configuration process with appropriate controls has been provided."

OIG Comment:

As mentioned in our comment above, one of the two documents provided as evidence that firewall configuration standards are in place appears to be a draft. We recommend that BSWH provide OPM's Healthcare and Insurance Office, Audit Resolution Group with the fully implemented version of the Firewall Configuration Standard.

4. Firewall Auditing

As mentioned above, BSWH does [redacted]

NIST SP 800-41, Revision 1, states that [redacted]

[redacted]

Recommendation 6

We recommend that BSWH perform routine audits of [redacted] against an approved policy. Note – this recommendation cannot be implemented until the controls from Recommendation 4 are in place.

BSWH's Response:

"BSWH accepts this recommendation, BSWH has started implementation of a continuous firewall auditing process [redacted] ***As noted above in B-3, recommendation 5, BSWH disagrees with B-3, recommendation 5."***

5. Credentialed Vulnerability Scanning

During a review of BSWH's historical vulnerability scans on its own network [redacted]

NIST SP 800-53, Revision 4, [redacted]

Recommendation 7

We recommend that BSWH [redacted]

BSWH's Response

"BSWH had a credential scanning process at the time of the audit, however, there was no [redacted]. The process is being enhanced to address this issue and is targeted to be completed [redacted]."

6. Vulnerabilities Identified by OIG Scans

BSWH worked with us to conduct credentialed vulnerability and configuration compliance scans on a sample of servers in BSWH's network environment. The specific vulnerabilities that we identified were provided to BSWH in the form of an audit inquiry, but will not be detailed in this report. The Plan has opened tickets for the vulnerabilities and begun taking appropriate actions.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 8

We recommend that BSWH remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

BSWH's Response

"BSWH implemented a new Vulnerability Response (VR) system in early 2020 and a high-priority Vulnerability Response Improvement Project is in progress and targeted to be completed by [redacted]."

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

Our review found the following controls in place:

- Controls to monitor security events throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

The following section documents one opportunity for improvement related to BSWH's security event monitoring and incident response controls.

1. Incident Response Testing

BSWH's Security Incident Standard says that the Security Incident Response Plan should be tested annually. [redacted] BSWH has scheduled a tabletop incident response exercise.

NIST SP 800-53, Revision 4, states [redacted]

[redacted]

Recommendation 9

We recommend that BSWH [redacted]

BSWH's Response:

"BSWH does not accept this recommendation because BSWH is conducting routine incident response testing pursuant to its policy."

OIG Comment:

BSWH had not conducted an incident response test since its Security Incident Standard was developed in 2016. BSWH had an incident response test scheduled for early 2020; however, COVID-19 delayed the test until after our audit fieldwork ended. In response to the draft audit report, BSWH provided evidence indicating that an adequate incident response test has since been conducted; 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. We evaluated BSWH's policies and procedures that govern its configuration management program. We also reviewed the results of configuration compliance scans to validate the effectiveness of its configuration management program.

Our review found the following controls in place:

- Documented system hardening process;
- Established patch management process; and
- System configuration changes are documented.

BSWH has a documented change control process.

The sections below document areas for improvement related to BSWH's configuration management controls.

1. Security Configuration Standards

BSWH maintains build guides for Windows and UNIX. The guides were developed internally and are maintained by BSWH personnel. [redacted]

NIST SP 800-53, Revision 4, states [redacted]

[redacted]

[redacted]

Recommendation 10

We recommend that BSWH document [redacted]

BSWH's Response:

"BSWH accepts this recommendation regarding the [redacted] security configuration standards. BSWH is actively improving formalization of its approval process within the applicable platforms. This is [redacted]"

Recommendation 11

We recommend that BSWH implement a process to [redacted]

BSWH's Response:

"BSWH accepts this recommendation. BSWH's deployment of platform-specific security configuration monitoring system for all operating system environments [redacted]

2. Security Configuration Auditing

[redacted]

Recommendation 12

We recommend that BSWH [redacted]

BSWH's Response:

"Platform specific monitoring is being deployed [redacted]

APPENDIX

Confidential and Sensitive Information

September 21, 2020

VIA SECURE E-MAIL PORTAL

To: US Office of Personnel Management
Office of Inspector General
Office of Audits
Attn: [redacted]

RE: Formal Response to
Audit of the Information Systems General Controls at Scott and White Health Plan

Dear Mr. [redacted]:

Baylor Scott & White Health (BSWH) provides information technology (IT) and security services to its managed affiliates, including Scott and White Health Plan (SWHP). SWHP and BSWH understands and takes seriously their obligation to protect the confidentiality, integrity, and availability of data processed and maintained in BSWH's IT environment for all of its patients and members, including data processed for the Federal Employees Health Benefits Program (FEHBP) through SWHP, and appreciates the opportunity to provide comments to the Office of Inspector General (OIG), Office of Audit Services Draft Audit report dated July 21, 2020.

Please note redactions will be required of this response, exhibits, attachments and audit report consistent with redactions addressed in SWHP and BSWH's Freedom of Information Act request as accepted by the Office of Inspector General. We are also requesting that all completion dates set forth in this response be redacted. We are providing Exhibit A and attachments thereto as additional evidence that we have met the standards for those recommendations which we disagree. However, Exhibit A and the attachments contain highly sensitive and confidential information. Therefore, SWHP and BSWH requests that Exhibit A and the attachments be redacted in their entirety from public disclosure which is consistent with the redactions previously accepted by the Office of Inspector General. Lastly, we have attached our comments to the Draft Audit report including the deletion of those recommendations that we believe there is no basis for including, because they do not accurately reflect the facts of our current security environment.

SWHP and BSWH respectfully provide the following responses to the Draft Audit Report (Report Number 1C-A8-00-20-019), issued July 21, 2020.

A-1 Vendor Risk Assessments

Recommendation 1: We recommend that BSWH implement a formal process to assess vendor risk prior to service acquisition and then periodically over the course of the relationship. This process should also be applied to all existing vendors.

- BSWH performs a vendor security program review prior to service acquisition or at renewal of contract as part of the BSWH Information Security Agreement (ISA). Vendors are required to maintain security at the level described in the ISA, or higher, throughout the duration of the agreement. BSWH acknowledges that a more robust vendor risk assessment pre-contracting, and periodic vendor risk assessments during the life of the contract, would strengthen the overall security posture of BSWH. Implementation of a more robust formal vendor risk assessment process is in progress [redacted]

B-1 Internal Network Segmentation

Recommendation 2: We recommend that BSWH [redacted]

- BSWH prior to the audit was actively engaged in a broad multi-year network segmentation program. The SWHP related segmentation [redacted]

B-2 Network Access Control

Recommendation 3: We recommend that BSWH complete [redacted]

- BSWH accepts this recommendation, only as it relates t[redacted]. Prior to the audit, BSWH was actively engaged in a broad multi-year network segmentation program [redacted] wireless networks, BSWH disagrees with this finding. BSWH does have applicable controls in place and evidence of same was provided on June 10, 2020 (IR-10).

B-3 Firewall Configuration Standard

Recommendation 4: We recommend that BSWH [redacted]

Recommendation 5: We recommend that BSWH implement a process to [redacted] Note – This recommendation cannot be implemented until the controls from Recommendation 4 are in place.

- BSWH does not accept these recommendations, BSWH has an effective firewall configuration process in place and documented that includes the elements stated in NIST SP 800-41. Appropriate evidence of this effective firewall configuration process with appropriate controls has been provided.

B-4 Firewall Auditing

Recommendation 6: We recommend that BSWH perform routine audits [redacted] against an approved policy. Note – this recommendation cannot be implemented until BSWH improves its security configuration standards for firewalls deployed in its technical environment (reference B-3)

- BSWH accepts this recommendation, BSWH has started implementation of a continuous firewall auditing process [redacted] As noted above in B-3, recommendation 5, BSWH disagrees with B-3, recommendation 5.

B-5 Credentialed Vulnerability Scanning

Recommendation 7: We recommend that BSWH [redacted]

- BSWH had a credential scanning process at the time of the audit, however, there was [redacted]. The process is being enhanced to address this issue [redacted]

B-6 Vulnerabilities Identified by OIG Scans

Recommendation 8: We recommend that BSWH remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

- BSWH implemented a new Vulnerability Response (VR) system in early 2020 and a high-priority Vulnerability Response Improvement Project is in progress and [redacted]

C-1 Incident Response Testing

Recommendation 9: We recommend that BSWH [redacted]

- BSWH does not accept this recommendation because BSWH is conducting routine incident response testing pursuant to its policy.

D-1 Security Configuration Standards

Recommendation 10: We recommend that BSWH document [redacted]

- BSWH accepts this recommendation regarding the [redacted] security configuration standards. BSWH is actively improving formalization of its approval process within the applicable platforms. This is [redacted]

Recommendation 11: We recommend that BSWH implement a process to [redacted]. Note – This recommendation cannot be implemented until the controls from Recommendation 1 are in place.

- BSWH accepts this recommendation. BSWH's deployment of platform-specific security configuration monitoring system for all operating system environments [redacted]

D-2 Security Configuration Auditing

Recommendation 12: We recommend that BSWH [redacted] Note – this recommendation cannot be implemented until BSWH documents approved security configuration standards for all operating system platforms and databases deployed in its technical environment. (reference D-1)

- Platform specific monitoring is being deployed [redacted]

SWHP and BSWH take their responsibility of IT and security compliance seriously and has processes and controls in place to protect the confidentiality and integrity over data entrusted to them. We will continue to improve processes and controls, as appropriate, to enable us to continue to maintain the confidentiality and integrity over data, including the FEHBP data.

Thank you for the opportunity to provide this response.

Sincerely,

Victor K. Richey
Chief Operating Officer

Scott&White HEALTH PLAN
PART OF BAYLOR SCOTT & WHITE HEALTH

1206 West Campus Drive | MS-A4-126 | Temple, TX 76502
Tel: 254.298.6090 | Fax: 254.298.3005

FirstCare HEALTH PLANS
PART OF BAYLOR SCOTT & WHITE HEALTH

12940 North Highway 183 | Austin, TX 78750

Date: 09/21/2020

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