U.S. Office of Personnel Management
Office of the Inspector General
Office of Audits

Final Audit Report

Audit of the the Information Systems General and Application Controls at EmblemHealth

Report Number 1D-80-00-21-025
March 21, 2022

Executive Summary

Audit of the Information Systems General and Application Controls at EmblemHealth

Report No. 1D-80-00-21-025 **March 21, 2022**

Why Did We Conduct the Audit?

EmblemHealth 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 EmblemHealth's information technology (IT) environment.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- EmblemHealth has established adequate security management controls including IT security policies and procedures and risk management.
- EmblemHealth has adequate physical and logical access controls.
- EmblemHealth does not have adequate controls in place related to user-installed software. Additionally, our vulnerability and compliance scan exercise identified some technical weaknesses in EmblemHealth's network environment.
- EmblemHealth has adequate incident response procedures. However, EmblemHealth does not have database security event monitoring controls in place.
- EmblemHealth does not conduct routine security configuration audits. Additionally, we identified instances of unsupported software in EmblemHealth's network environment.
- EmblemHealth has adequate controls over contingency planning.
- EmblemHealth has adequate controls over its application change control process.

Abbreviations

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 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 EmblemHealth.

The audit was conducted pursuant to FEHBP contracts CS 1056 and CS 1040; 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.

EmblemHealth outsources FEHBP claims processing to Cognizant, a third-party contractor, that also maintains and hosts applications and systems that support the claims adjudication process. Cognizant is highly integrated with EmblemHealth and has IT security related responsibilities in many of the areas within our audit scope. As such, Cognizant participated in this audit along with EmblemHealth. EmblemHealth maintains the FEHBP contract with OPM and is ultimately responsible for addressing recommendations issued in this report. This was our second audit of general and application controls at EmblemHealth. The previous audit of the general and application controls at EmblemHealth was conducted in 2012. Final Audit Report No. 1D-80-00-12-045 was issued on December 10, 2012. All recommendations from the previous audit have been closed.

All 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 make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit were 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 EmblemHealth's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to EmblemHealth'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 EmblemHealth'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 EmblemHealth'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 EmblemHealth to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in New York, New York.

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 and application controls in place over EmblemHealth's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at EmblemHealth as of September 2021.

In conducting our audit, we relied to varying degrees on computer-generated data provided by EmblemHealth. 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.

We used judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of EmblemHealth'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 EmblemHealth's business structure and environment; and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended.

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

- GAO's FISCAM; and
- National Institute of Standards and Technology's 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 EmblemHealth's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, EmblemHealth 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 serve as the foundation of EmblemHealth's overall IT security program. We evaluated EmblemHealth's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

EmblemHealth has adequate security management controls.

EmblemHealth has developed adequate IT security policies and procedures. EmblemHealth has developed an adequate risk management methodology that includes internal risk assessments conducted by EmblemHealth and external risk assessments conducted by third parties. Furthermore, EmblemHealth creates remediation plans to address weaknesses identified in its risk assessments.

Nothing came to our attention to indicate that EmblemHealth has not implemented an adequate security management program.

B. Access Controls

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

We examined the physical access controls at EmblemHealth's facilities and data centers. We also examined the logical access controls protecting sensitive data on EmblemHealth's network environment and applications.

The access controls observed during this audit included, but were not limited to:

- Standards for appropriately granting and removing physical access to facilities and data centers;
- Standards for appropriately granting and removing logical access to applications and software resources; and
- Routine access reviews.

Nothing came to our attention to indicate that EmblemHealth has not implemented adequate access controls.

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

We observed the following controls in place:

- Endpoint security controls;
- Policies and procedures to protect sensitive data at rest; and
- Network access controls to prevent unauthorized devices on the internal network.

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

1. User-Installed Software

EmblemHealth's formal standards state that "users may not install any software without prior documented approval from IT." However, EmblemHealth did not demonstrate the implementation of adequate controls restricting user-installed software. EmblemHealth stated that this is accomplished using Palo Alto firewalls which are configured to block downloads of executable files. However, according to EmblemHealth's *Palo Alto Operations Guide*, firewalls are not configured to block downloads of executable files.

NIST SP 800-53, Revision 4, states that the organization "Establishes [organization-defined policies] governing the installation of software by users" and "Enforces software installation policies through [organization-defined methods] … ."

Failure to control user-installed software creates risk that unapproved and potentially vulnerable software will be introduced into EmblemHealth's network environment.

Recommendation 1:

We recommend that EmblemHealth implement controls to enforce its policy that users may not install any software without prior documented approval.

EmblemHealth's Response:

"EmblemHealth has CyberArk Endpoint Privilege Manager (EPM) in place which enforces application whitelisting on all EmblemHealth devices. This is a strong

mitigating control preventing unauthorized applications from executing. EmblemHealth did submit evidence of the controls that prevent End Users from installing software on an EmblemHealth supplied devices. This evidence was shared on Sept. 24 in an email from Jim Altinay to Christopher Bouchey with the subject 'VPN'. This email outlined the following mitigating controls:

1. ***Less than 1% of the users have local admin rights to their machines and we are still working on further reducing this number. CyberArk EPM solution is used to elevate access for a specific process.***

2. ***Palo Alto firewalls block users from downloading software from the internet.***

3. ***Weekly Rapid7 and Quarterly Verizon scans identify any unsupported applications on workstations.***

The Palo Alto Operations Guide incorrectly stated that firewalls are not configured to block downloads of executable files. The firewalls are configured to block downloads of executables. Here is a screen shot of the control in place to block the download of software from the internet: [See Appendix for screen shot].

EmblemHealth will take the following steps:

1. ***EmblemHealth will look at additional controls via GPO and strengthening Application Whitelisting in our environment. We will have a formal recommendation by June 30, 2022.***

2. ***EmblemHealth has corrected the Palo Alto Operations Guide to reflect the fact that downloads of executables are in fact blocked as shown in the screen shot above. This was completed on Jan 10, 2022."***

OIG Comments:

In response to the draft audit report, EmblemHealth provided a screen shot demonstrating that controls are now in place to block the downloading of executable files. No further action is required.

2. Vulnerabilities Identified by OIG Scans

EmblemHealth should remediate the vulnerabilities identified during this audit.

EmblemHealth conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of 150 servers from a universe of 2,635. The sample selection included a variety of system functionalities and operating systems across production, test, and development. The judgmental sample was drawn from systems that store and/or process Federal member data, as well as other systems in the same general control environment that contain Federal member data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The specific vulnerabilities that we identified were provided to EmblemHealth in the form of an audit inquiry but will not be detailed in this report. EmblemHealth was aware of many of the vulnerabilities identified during our scanning exercise. However, EmblemHealth is unable to quickly remediate these vulnerabilities on legacy systems with application dependencies. EmblemHealth has ongoing projects to decommission these legacy systems.

NIST SP 800-53, Revision 4, states that organizations should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

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

Recommendation 2:

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

EmblemHealth's Response:

"EmblemHealth agrees with this recommendation and has been making measurable progress in this area. We have shown continuous improvement in vulnerability management as we have emerged from our transformation process. We expect to have all unsupported operating systems, required for records retention compliance, isolated from the rest of the network by Q3 2022. The steady progress we have made in this area is illustrated by the following snippet from an independent Verizon Business Cyber Risk Assessment program we have in place [See Appendix]. We have moved from a score of 5.43 to a score of 3.94 in the past year (lower is better). We expect to be

below the 3.0 mark by the end of Q3 2022, which is a moderate risk rating and meets the criteria for Verizon's Cybertrust certification.

EmblemHealth will take the following actions:

1. ***We will continue to eliminate or isolate unsupported operating systems as they are replaced by modern solutions – Q3 2022 estimated completion date.***

2. ***EmblemHealth will continue to patch our environment adhering to our vulnerability management standards to further reduce the risks (ongoing)."***

OIG Comments:

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

D. 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.

We observed the following controls in place:

- Security event monitoring throughout the network;
- Incident reporting and notification procedures; and
- Incident response procedures.

However, we noted the following opportunity for improvement related to EmblemHealth's security event monitoring and incident response controls.

1. Database Security Event Monitoring

EmblemHealth's *Logging and Monitoring Standard* states that "Logging, where technically feasible, will be aggregated to a log consolidation solution ... ." Furthermore, it requires periodic reporting of high-risk errors, traps and conditions and where technically feasible, real-time monitoring and alerting is enabled for critical or high-risk systems and incidents. However, EmblemHealth does not have controls in place to monitor malicious activity on databases. EmblemHealth had previously identified this

opportunity for improvement and is performing a feasibility study before starting a formal project to integrate databases with the existing monitoring tools.

NIST SP 800-53, Revision 4, states that the organization "Monitors the information system to detect … Attacks and indicators of potential attacks in accordance with [organization defined monitoring objectives] … ."

Failure to implement security event monitoring tools negatively affects EmblemHealth's ability to detect and respond to security incidents.

Recommendation 3:

We recommend that EmblemHealth integrate its databases with its central logging server and monitor for database alerts as appropriate.

EmblemHealth's Response:

"EmblemHealth has logging in place for all privileged activities on the critical Database servers, including Database Administration activities. All privileged activities are centrally logged presently. This represents the most significant threat to database confidentiality and integrity. We do acknowledge that there are opportunities to further integrate database logging into our SIEM and Security Operations Center (SOC).

EmblemHealth will take the following actions:

1. ***EmblemHealth will consult a third-party security expert to recommend database logging integration into our SIEM solution. This review will be complete by April 30th, 2022.***

2. ***EmblemHealth will implement the security expert's recommendation by June 30th, 2022."***

E. 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. EmblemHealth employs a team of technical personnel who manage system software configuration for the organization. We evaluated EmblemHealth's management of the configuration of its computer servers and databases.

We observed the following controls in place:

- Documented hardening standards and guidelines;
- Change management standards; and
- Adequate change documentation tracking.

However, we noted the following opportunities for improvement related to EmblemHealth's configuration management controls.

1. Security Configuration Auditing

EmblemHealth does not conduct routine security configuration audits.

As noted above, EmblemHealth maintains hardening standards and guidelines that document the approved configuration settings and the implementation process for new server builds. As part of the build process new server configurations are scanned for compliance against the hardening standards before being deployed into the production environment. However, no routine configuration scans are conducted after that initial scan.

NIST SP 800-53, Revision 4, states that an organization must "[monitor] and [control] changes to the configuration settings in accordance with organizational policies and procedures."

FISCAM requires, "Current configuration information [to] be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to perform routine security configuration auditing increases the risk that systems with unsecure configurations will go undetected, leaving the system vulnerable to a cyber attack.

Recommendation 4:

We recommend that EmblemHealth implement a process to routinely audit security configuration settings of its servers to ensure compliance with approved security configuration standards.

EmblemHealth's Response:

"EmblemHealth agrees with the recommendation and has implemented the following controls since the audit completed:

- ***EmblemHealth has implemented a weekly configuration variance meeting to review all changes made during the previous week. This review compares the variances discovered to the list approved by the Change Control Committee. If an unapproved change is detected there is an investigation opened.***

- ***A firewall management platform, Tufin, has been implemented to provide real time alerts of firewall changes. These alerts go to senior leadership in the firewall team. All alerts are reviewed to ensure the change was appropriate. These alerts are also reviewed in the weekly variance meeting mentioned above.***

- ***A network configuration management tool, NetMRI is implemented to maintain a real time repository of all network device configurations. A weekly change report is scheduled and will be reviewed in the variance meeting once the NetMRI software is upgraded to the latest version.***

EmblemHealth will take the following actions:

1. ***NetMRI will be upgraded to a current version by March 1, 2022.***

2. ***NetMRI reports will be added to the Weekly Variance Review process by April 1, 2022."***

2. System Lifecycle Management

Our vulnerability scanning exercise and review of EmblemHealth's server and network device inventory identified instances of unsupported software within the IT environment. The vendors of this software typically publicize information related to the product's "end-of-life" support dates (i.e., dates when the vendor will no longer release security updates and patches). EmblemHealth was aware of the unsupported software and tracks those instances. The challenge to removing the unsupported software is the need for legacy systems to be available during a period of transition to new systems. EmblemHealth indicated that several projects are in place to migrate away from legacy applications by 2022.

NIST SP 800-53, Revision 4, advises that the organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer … ." NIST SP 800-53, Revision 4, also states that "Unsupported components … provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components."

Failure to upgrade or decommission unsupported software leaves information systems vulnerable to cyber attack without any remediation available.

Recommendation 5:

We recommend that EmblemHealth develop and implement action plans to upgrade or decommission the unsupported software identified during this audit.

EmblemHealth's Response:

"EmblemHealth agrees with this recommendation and has taken the following actions already:

1. ***We have a requirement in our outsourcing contract to have all software and hardware at a level of N-1 or better version (where N is the most current mainline supported version).***

2. ***Where we are not at N-1 due to business requirements we have the following provisions:***

    - ***The software or hardware must be supported by the vendor.***

    or

    - ***Extended support from the vendor must be purchased (e.g., Windows 2008).***

    or

    - ***A risk assessment / acceptance process must be followed with an approved risk acceptance reviewed by the Chief Information Security Officer (CISO) of EmblemHealth.***

EmblemHealth will take the actions identified in recommendation #2, additionally EmblemHealth will take the following additional action:

1. ***All risk acceptances in place will be reviewed and re-certified by the EmblemHealth CISO by June 30, 2022."***

F. Contingency Planning

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business process. We reviewed elements of EmblemHealth's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when

EmblemHealth has adequate controls over contingency planning.

disruptive events occur.

The controls observed during this audit included, but were not limited to:

- Documented business impact assessments;
- Documented contingency plans; and
- Documented contingency plan tests.

Nothing came to our attention to indicate that EmblemHealth has not implemented adequate contingency planning controls.

G. Application Change Control

We evaluated the policies and procedures governing EmblemHealth's application development and change control process. EmblemHealth has implemented policies and procedures related to application configuration management and has adopted a system development life cycle methodology that IT personnel follow during routine software modifications.

We observed the following controls in place:

- Documented system development lifecycle policy and process workflows;
- Documented change management process; and
- Adequate documentation tracking throughout the application change management process.

Nothing came to our attention to indicate that EmblemHealth has not implemented adequate controls over its application change control process.

Appendix

EmblemHealth®

Draft Audit Report No. 1D-80-00-21-025 Information Systems General and Application Controls at EmblemHealth

Audit Response: Comments and Action Plans

McDermott, Thomas
1-14-2022

Attached is EmblemHealth's response to the draft audit report detailing the results of the information technology audit of EmblemHealth by the Office of the Inspector General at the U.S. Office of Personnel Management (OPM). We are providing our comments and action plans for each of the five recommendations included in the draft audit report.

Prior to the issuance of the final audit report EmblemHealth will provide any redaction requests, with supporting justification if any are requested.

OPM Audit Recommendation #1:

1. User-Installed Software

EmblemHealth's formal standards state that, "users may not install any software without prior documented approval from IT." However, EmblemHealth did not demonstrate the implementation of adequate controls restricting user-installed software. EmblemHealth stated that this is accomplished using Palo Alto firewalls which are configured to block downloads of executable files. However, according to EmblemHealth's Palo Alto Operations Guide, firewalls are not configured to block downloads of executable files.

NIST SP 800-53, Revision 4, states that the organization "Establishes [organization-defined policies] governing the installation of software by users" and "Enforces software installation policies through [organization-defined methods]."

Failure to control user-installed software creates risk that unapproved and potentially vulnerable software will be introduced into EmblemHealth's network environment.

Recommendation 1:
We recommend that EmblemHealth implement controls to enforce its policy that users may not install any software without prior documented approval.

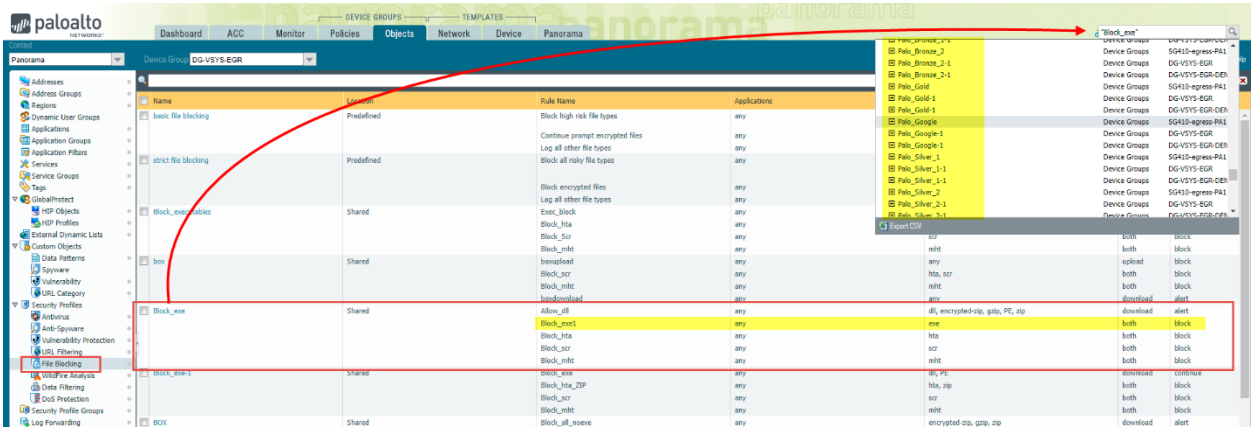
EmblemHealth's Response to Recommendation #1:

EmblemHealth has CyberArk Endpoint Privilege Manager (EPM) in place which enforces application whitelisting on all EmblemHealth devices. This is a strong mitigating control preventing unauthorized applications from executing. EmblemHealth did submit evidence of the controls that prevent End Users from installing software on an EmblemHealth supplied devices. This evidence was shared on Sept. 24 in an email from Jim Altinay to Christopher Bouchey with the subject "VPN". This email outlined the following mitigating controls:

1. Less than 1% of users have local admin rights to their machines and we are still working on further reducing this number. CyberArk EPM solution is used to elevate access for a specific process.
2. Palo Alto firewalls block users from downloading software from the internet.

3. Weekly Rapid7 and Quarterly Verizon scans identify any unsupported applications on workstations.

The Palo Alto Operations Guide incorrectly stated that firewalls are not configured to block downloads of executable files. The firewalls are configured to block downloads of executables. Here is a screen shot of the control in place to block the download of software from the internet:



EmblemHealth will take the following steps:

1. EmblemHealth will look at additional controls via GPO and strengthening Application Whitelisting in our environment. We will have a formal recommendation by June 30 2022.
2. EmblemHealth has corrected the Palo Alto Operations Guide to reflect the fact that downloads of executables are in fact blocked as shown in the screen shot above. This was completed on Jan 10, 2022.

OPM Recommendation #2:

2. Vulnerabilities Identified by OIG Scans

EmblemHealth conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of 150 servers from a universe of 2,635. The sample selection included a variety of system functionality and operating systems across production, test, and development. The judgmental sample was drawn from systems that store and/or process Federal member data, as well as other systems in the same general control environment that contain Federal member data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The specific vulnerabilities that we identified were provided to EmblemHealth in the form of an audit inquiry but will not be detailed in this report. EmblemHealth was aware of many of the vulnerabilities identified during our scanning exercise. However, EmblemHealth is unable to quickly remediate these vulnerabilities on legacy

systems with application dependencies. EmblemHealth has ongoing projects to decommission these legacy systems.

NIST SP 800-53, Revision 4, states that organization must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

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

Recommendation 2:
We recommend that EmblemHealth remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

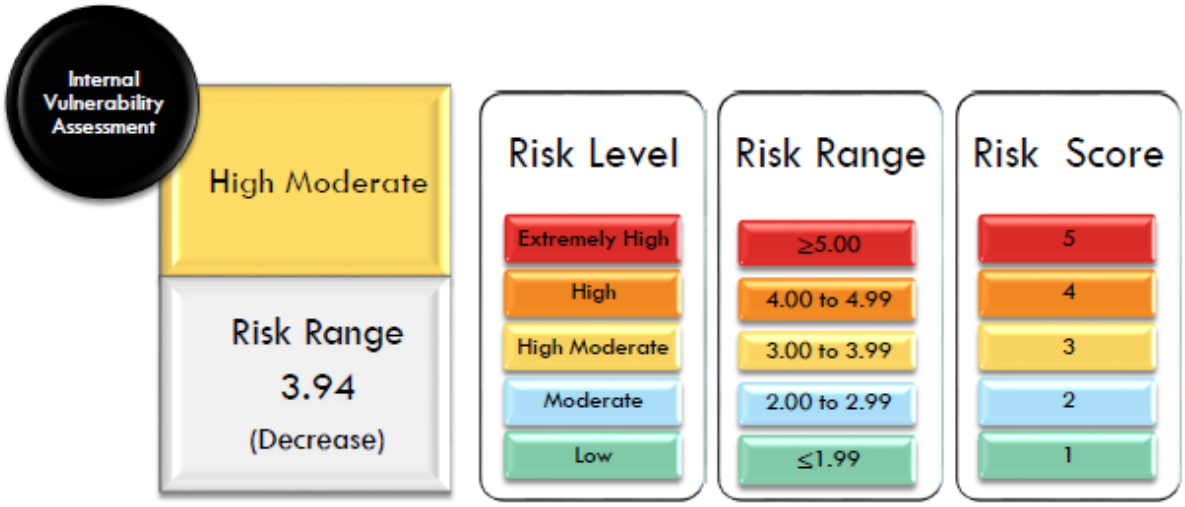
EmblemHealth's Response to Recommendation #2:

EmblemHealth agrees with this recommendation and has been making measurable progress in this area. We have shown continuous improvement in vulnerability management as we have emerged from our transformation process. We expect to have all unsupported operating systems, required for records retention compliance, isolated from the rest of the network by Q3 2022. The steady progress we have made in this area is illustrated by the following snippet from an independent Verizon Business Cyber Risk Assessment program we have in place. We have moved from a score of 5.43 to a score of 3.94 in the past year (lower is better). We expect to be below the 3.0 mark by the end of Q3 2022, which is a moderate risk rating and meets the criteria for Verizon's Cybertrust certification.

OVERALL INTERNAL VULNERABILITY (LAN) ASSESSMENT RISK SCORE

The score below is based on the information collected from the vulnerability assessment conducted on **2021-08-04.** Risk is determined by different threat types identified by the Verizon Data Breach Investigations Report (DBIR).

Risk Assessment Results



Current Assessment Year

Previous Assessment Year

Overall Internal Vulnerability (LAN) Assessment Risk Score: The score noted above is based on the information collected from the vulnerability assessment conducted on 2021-08-04. Risk is determined by different threat types identified by the Verizon Data Breach Investigations Report (DBIR). Risk assessment results show an internal vulnerability assessment score of 3.94 (High Moderate) for Q1. This is a decrease from 5.43 (Extremely High) in Q1 of the previous year.

EmblemHealth will take the following actions:

1. We will continue to eliminate or isolate unsupported operating systems as they are replaced by modern solutions – Q3 2022 estimated completion date.
2. EmblemHealth will continue to patch our environment adhering to our vulnerability management standards to further reduce the risks (ongoing).

OPM Recommendation #3:

1. Database Security Event Monitoring

EmblemHealth's Logging and Monitoring Standard states that "Logging, where technically feasible, will be aggregated to a log consolidation solution...." Furthermore, it requires periodic reporting of high-risk errors, traps and conditions and where technically feasible, real-time monitoring and alerting is enabled for critical or high-risk systems and incidents. However, EmblemHealth does not have controls in place to monitor malicious activity on databases. EmblemHealth had previously identified this opportunity for improvement and is performing a feasibility study before starting a formal project to integrate databases with the existing monitoring tools.

NIST SP 800-53, Revision 4, states that the organization "Monitors the information system to detect attacks and indicators of potential attacks in accordance with [organization defined monitoring objectives]."

Failure to implement security event monitoring tools negatively affects EmblemHealth's ability to detect and respond to security incidents.

Recommendation 3:
We recommend that EmblemHealth integrate its databases with its central logging server and alert for database alert as appropriate.

EmblemHealth Response to Recommendation #3:

EmblemHealth has logging in place for all privileged activities on the critical Database servers, including Database Administration activities. All privileged activities are centrally logged presently. This represents the most significant threat to database confidentiality and integrity. We do acknowledge that there are opportunities to further integrate database logging into our SIEM and Security Operations Center (SOC).

EmblemHealth will take the following actions:

1. EmblemHealth will consult a third-party security expert to recommend database logging integration into our SIEM solution. This review will be complete by April 30th, 2022.
2. EmblemHealth will implement the security expert's recommendation by June 30th, 2022.

OPM Recommendation #4

1. Security Configuration Auditing

As noted above, EmblemHealth maintains hardening standards and guidelines that document the approved configuration settings and the implementation process for new server builds. As part of the build process new server configurations are scanned for compliance against the hardening standards before being deployed into the production environment. However, no routine configuration scans are conducted after that initial scan.

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprises the information system.

Failure to perform routine security configuration auditing increases the risk that systems with unsecure configurations will go undetected, leaving the system vulnerable to a cyber-attack.

Recommendation 4:
We recommend that EmblemHealth implement a process to routinely audit security configuration settings of its servers to ensure compliance with approved security configuration standards.

EmblemHealth Response to Recommendation #4:

EmblemHealth agrees with the recommendation and has implemented the following controls since the audit completed:

- EmblemHealth has implemented a weekly configuration variance meeting to review all changes made during the previous week. This review compares the variances discovered to the list approved by the Change Control Committee. If an unapproved change is detected there is an investigation opened.
- A firewall management platform, Tufin, has been implemented to provide real time alerts of firewall changes. These alerts go to senior leadership in the firewall team. All alerts

are reviewed to ensure the change was appropriate. These alerts are also reviewed in the weekly variance meeting mentioned above.

- A network configuration management tool, NetMRI is implemented to maintain a real time repository of all network device configurations. A weekly change report is scheduled and will be reviewed in the variance meeting once the NetMRI software is upgraded to the latest version

EmblemHealth will take the following actions:

1. NetMRI will be upgraded to a current version by March 1, 2022
2. NetMRI reports will be added to the Weekly Variance Review process by April 1, 2022

OPM Recommendation #5

2. System Lifecycle Management

Our vulnerability scanning exercise and review of EmblemHealth's server and network device inventory identified instances of unsupported software within the IT environment. The vendors of this software typically publicize information related to the product's "end-of-life" support dates (i.e., dates when the vendor will no longer release security updates and patches). EmblemHealth was aware of the unsupported software and tracks those instances. The challenge for removing the unsupported software is the need for legacy systems to be available during a period of transition to new systems. EmblemHealth indicated that several projects are in place to migrate away from legacy applications by 2022.

NIST SP 800-53, Revision 4, advises that the organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer …." NIST SP 800-53, Revision 4, also states that "Unsupported components … provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components."

Failure to upgrade or decommission unsupported software leaves information systems vulnerable to cyber-attack without any remediation available.

Recommendation 5:
We recommend that EmblemHealth develop and implement action plans to upgrade or decommission the unsupported software identified during this audit.

EmblemHealth's Response to Recommendation #5:

EmblemHealth agrees with this recommendation and has taken the following actions already:

1. We have a requirement in our outsourcing contract to have all software and hardware at a level of N-1 or better version (where N is the most current mainline supported version).

2. Where we are not at N-1 due to business requirements we have the following provisions:
   - The software or hardware must be supported by the vendor.

   or

   - Extended support from the vendor must be purchased (e.g., Windows 2008).

   or

   - A risk assessment / acceptance process must be followed with an approved risk acceptance reviewed by the Chief Information Security Officer (CISO) of EmblemHealth.

EmblemHealth will take the actions identified in recommendation #2, additionally EmblemHealth will take the following additional action:

1. All risk acceptances in place will be reviewed and re-certified by the EmblemHealth CISO by June 30, 2022.

If you have any questions about the comments or action plans, feel free to contact me. EmblemHealth considers Information Security a priority. Draft Audit Report No. 1D-80-00-21-025 Information Systems General and Application Controls at EmblemHealth, was reviewed with senior leadership and we look forward to working with you to create the final report.

X Thomas McDermott

Signed by: 34c9dfec-897e-4f22-bad0-654d79501db8

Thomas McDermott (he/him)
Vice President Technology and CISO
EmblemHealth | ConnectiCare | AdvantageCare Physicians

P 646-447-4110 **M** [redacted]
emblemhealth.com/together

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