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 Health Alliance Medical Plans, Inc.

Report Number 2022-ISAG-036
July 13, 2023

Executive Summary

Audit of the Information Systems General and Application Controls at Health Alliance Medical Plans, Inc.

Report No. 2022-ISAG-036 **July 13, 2023**

Why Did We Conduct the Audit?

Health Alliance Medical Plans, Inc. (HAM), plan code K8, 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 HAM's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by HAM to process and store data related to medical encounters and insurance claims for FEHBP members as of March 2023.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- HAM is a subsidiary of The Carle Foundation (Carle), which offers a wide range of health care products and services in addition to its FEHBP line of business. Additionally, HAM inherits some IT controls from its parent company Carle.
- HAM and Carle have not updated [redacted].
- HAM and Carle have adequate physical and logical access controls in place.
- Carle does [redacted].
- HAM and Carle have [redacted].
- HAM has [redacted].
- HAM has some systems that are [redacted].
- HAM does [redacted].

Abbreviations

Carle	**The Carle Foundation**
CFR	**Code of Federal Regulations**
HAM	**Health Alliance Medical Plans, Inc.**
FEHBP	**Federal Employees Health Benefits Program**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
SDLC	**Software Development Life Cycle**

Table of Contents

Report Fraud, Waste, and Mismanagement

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 the Health Alliance Medical Plans, Inc. (HAM), plan code K8.

The audit was conducted pursuant to FEHBP contract CS 1980; 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 (5 U.S.C. §§ 401-424).

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.

HAM is a subsidiary of The Carle Foundation (Carle), which offers a wide range of health care products and services in addition to its FEHBP line of business. HAM inherits some IT controls from its parent company Carle.

This was our initial audit of the information systems general and application controls at HAM. All HAM and Carle 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 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 HAM'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 HAM'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 HAM'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 HAM'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 HAM to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Champaign, Illinois.

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 HAM'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 HAM as of March 2023.

In conducting our audit, we relied to varying degrees on computer-generated data provided by HAM. 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 HAM's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's Federal Information System Controls Audit Manual;
- Gathered documentation and conducted interviews;
- Reviewed HAM'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 HAM's control structure. These criteria included, but were not limited to, the following publications:

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether HAM's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, HAM 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 HAM and Carle's overall IT security program. We evaluated HAM and Carle's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

We observed the following controls in place:

- An adequate IT security awareness training program;
- Routine risk assessments; and
- Routine security awareness training is administered.

However, we noted the following opportunities for improvement related to HAM and Carle's security management controls.

1. Information Security Program Plan

HAM and Carle's *Information Security Program Plan* .

The *Information Security Program Plan* was designed to define the control objectives required to effectively manage the confidentiality, integrity, and availability of protected information. The *Information Security Program Plan* states that, "The Security Officer will review this program as needed, and at least annually, in order to maintain an ongoing and measurable state of compliance."

NIST SP 800-53, Revision 5, control PM-1 states that the organization "Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] … ."

Failure to increases the risk that HAM and Carle's security program will be in a state that is more susceptible to threats and vulnerabilities.

Recommendation 1:

We recommend that HAM and Carle review and update their documented *Information Security Program Plan* in accordance with its policy and NIST requirements.

HAM's Response:

"Health Alliance is currently in the process of performing a full review and update of the Information Security Program Plan, to reflect changes in infrastructure and enterprise acquisitions (this will include incorporation of new business units into the business continuity plan). The slated completion date for this refresh … is ."

OIG Comments:

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

B. Access Controls

HAM and Carle have adequate logical and physical access controls in place.

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 HAM's headquarter facility and data centers. We also examined the logical access controls protecting sensitive data on HAM's network environment and applications. HAM inherits some access controls from Carle.

We observed the following controls in place:

- Accounts are adequately disabled for terminated personnel;
- Physical access authorizations are enforced; and
- Environmental controls are adequate.

Nothing came to our attention to indicate that HAM and Carle have not implemented adequate access controls.

C. Network Security

Carle could improve its network security controls.

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. HAM inherits some network security controls from Carle.

We evaluated the 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:

- Perimeter controls to secure connections to external networks;
- Malicious code protection on end user devices; and
- Adequately disabled USB connection ports.

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

1. Network Segmentation

Carle does [redacted]. Carle uses a firewall to control connections with systems outside of its network as well as between public facing applications and the internal network. [redacted]

NIST SP 800-41, Revision 1, states that "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised external attackers. Important internal systems should be placed behind internal firewalls."

Failure to appropriately segment user-controlled systems from sensitive internal resources increases the risk that a compromise of a user's system could allow access to sensitive servers and data.

Recommendation 2:

We recommend that HAM ensure [redacted]

HAM's Response:

"This has been identified as a long-term project at the enterprise level for the Carle Health system. The project is underway and completion of phase 1 [redacted]

[redacted]. ***The initial stages of the SD-access implementation are currently underway and contracted project management is overseeing the deployment [See SD-Access Timeline], barring unforeseen delays, the initial implementation is slated for completion [redacted].”***

2. Network Access Control

Carle does [redacted] Carle is aware of the gap and has provided evidence of change control tickets demonstrating ongoing remediation progress.

NIST SP 800-53, Revision 5, control IA-3 states that an information system uniquely identify and authenticate devices before establishing a network connection.

Failure to [redacted] could allow [redacted]

Recommendation 3:

We recommend that HAM ensure [redacted]

HAM’s Response:

“As mentioned above in Response 2, [redacted] is currently being deployed enterprise wide. Health Alliance Medical Plans and affiliated entities will be covered by enforcement mode [redacted].”

3. Mobile Device Management

Carle uses a mobile device management tool to manage security patches, containerize data, apply configurations, and provide other functionality. [redacted]. HAM’s *Portable Device Policy* states that mobile device management software and policies are used to manage mobile devices. The policy further states that the Security Officer is responsible for conducting random audits and routine monitoring of mobile device compliance. [redacted]

NIST SP 800-53, Revision 5, control AC-19 states that the organization “Establish configuration requirements, connection requirements, and implementation guidance for

organization-controlled mobile devices, to include when such devices are outside of controlled areas … .”

NIST SP 800-53, Revision 5, control CM-6 states that the organization “Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.”

Failure to [redacted] increases the risk that mobile devices [redacted]

Recommendation 4:

We recommend that HAM ensure [redacted].

HAM’s Response:

“This response will cover Recommendations 4 and 5. Health Alliance IT shared service is in the process of migrating to the [redacted] This will result in the replacement of several different tools that were being utilized to manage mobile devices. IT is [redacted] to schedule and deploy the enterprise version of Intune to all corporate mobile devices [redacted] During that adoption, uniform configuration standards will be applied to corporate managed mobile devices.”

Recommendation 5

We recommend that HAM ensure [redacted] implemented until the controls from Recommendation 4 are in place.

HAM’s Response:

“Once the actions in Response 4 are completed, mobile assets will be centrally managed and monitored for compliance. Mobile devices will be audited for compliance and non-compliant assets will generate incident tickets for remediation.”

4. Cryptographic Protection

Carle performed credentialed vulnerability scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of 162 servers from a universe of approximately 178 servers. The sample selection included a variety of system functionality and operating systems across production, test, and development

environments. 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. [redacted]

NIST SP 800-53, Revision 5, control SC-8 (1) states that "Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPsec."

Failure to [redacted] increases the risk of [redacted]

Recommendation 6:

We recommend that HAM ensure [redacted].

HAM's Response:

"Enterprise IT has initiated a project to remediate this issue for the organization. Phase 1 of the project has been completed. Fixes have been applied to all the current [redacted] in use for server and workstation creation. Phase 2 for the project [redacted] is currently underway."

D. Security Event Monitoring and Incident Response

HAM and Carle have [redacted]

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. HAM inherits some security event monitoring and incident response controls from Carle.

We observed the following controls in place:

- Security event monitoring throughout the network;
- Policies and standards for analyzing security events; and

- An adequate incident response test.

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

1. Incident Response Training

HAM and Carle have a *Technical Incident Response Program*. [redacted] We were told that Carle's training consists of reviewing incident response playbooks. [redacted]

NIST SP 800-53, Revision 5, control IR-2 states that incident response training should be provided to system user's consistent with assigned roles and responsibilities within an organization defined time period. Additionally, training should be administered thereafter, and content should be reviewed and updated following at organization-defined frequencies.

Failure to provide [redacted] increases the risk that [redacted].

Recommendation 7:

We recommend that HAM ensure [redacted].

HAM's Response:

"Health Alliance is in the process of updating the Information Security Program [redacted]

Recommendation 8:

We recommend that HAM ensure [redacted]. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

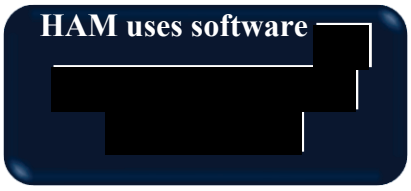
HAM's Response:

"Health Alliance leadership has identified this as an opportunity to improve and supplement our current process. There is executive level training for the incident

response program (HICS), the process is [redacted] ***Management is currently interviewing candidates for a new Information Security Education and Awareness specialist position*** [redacted]

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. HAM employs a team of technical personnel who manage system software configuration for the organization. HAM inherits some controls from Carle related to configuration change management. However, HAM is responsible for ensuring that its systems are securely configured.



We observed the following controls in place:

- Documented configuration management policy;
- System changes are analyzed in separate test environments; and
- Adequate software installation policies are enforced.

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

1. Baseline Configuration Review

HAM does [redacted]. HAM's baseline configurations for new system builds consist of multiple components including system images with current patch levels, system build specification documents, and configuration settings. [redacted]

NIST SP 800-53, Revision 5, control CM-2 states that the organization review and update the baseline configuration of the system at an organization-defined frequency, when required due to organization-defined circumstances, and when system components are installed or upgraded.

Failure to routinely [redacted] increases the risk that [redacted].

Recommendation 9:

We recommend that HAM develop and then implement [redacted]

HAM's Response:

"Health Alliance currently has a project underway [redacted]. System baselines have been developed and deployed for the server environment broadly. Shared Service IT has deployed [redacted] to the enterprise network environment and the workstation and VM image configurations are being evaluated. Enterprise has [redacted]. This will include wide deployment of agents to corporate assets that will facilitate increased environmental visibility and monitoring at the client level. This project will be dependent upon [redacted]

2. Least Functionality Review

HAM does [redacted]. HAM's *Server Security Policy* states that all unnecessary functionality and services must be removed. [redacted]. Configuration monitoring and enforcement tools have been recently deployed to support this effort.

NIST SP 800-53, Revision 5, control CM-7 (1) states that the organization "review the system [at an organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and … Disable or remove [them]."

Failure to routinely [redacted] increases the risk that a [redacted].

Recommendation 10:

We recommend that HAM [redacted]

HAM's Response:

"This process will be incorporated into the periodic system baseline review."

3. Impact Analyses

HAM was [redacted] we were provided with three examples of notes from a Technical Assessment Committee. [redacted].

NIST SP 800-53, Revision 5, control CM-4 states that the organization "Analyze changes to the system to determine potential security and privacy impacts prior to change implementation." According to NIST, this includes "reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks."

NIST SP 800-53, Revision 5, control CM-3 states that the organization "Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses … ."

NIST SP 800-53, Revision 5, control CM-1 states that the organization develop, document, and disseminate a policy that is consistent with all applicable standards and guidelines and procedures to facilitate the implementation of configuration management controls, which includes CM-3 and CM-4 control requirements.

Failure to [redacted] increases the risk that the [redacted].

Recommendation 11 :

We recommend that HAM update its *IT Change Control Policy* to define requirements for approving or disapproving configuration-controlled changes with explicit consideration for the results of impact analyses.

HAM's Response:

"IT Change Control Policy to be updated to include language requiring impact review of submitted changes."

Recommendation 12:

We recommend that HAM [redacted]

HAM's Response:

"Change Control submission form updated to include mandatory field for security and privacy impact analysis [redacted]."

4. Unsupported Software

As a result of our vulnerability scanning exercise, we identified various instances of unsupported software installed on HAM servers and workstations. In response to this finding, HAM attested that it had previously identified the unsupported software and has ongoing projects to upgrade or decommission them.

NIST SP 800-53, Revision 5, control SA-22 states that the organization "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer;" or acquire an alternative source for continued support.

Failure to [redacted] increases the risk that [redacted].

Recommendation 13:

We recommend that HAM replace or identify extended support for software identified during this audit which is no longer supported by the developer, vendor, or manufacturer.

HAM's Response:

"Health Alliance management has identified this as a long term [redacted] for the organization. Unsupported or obsolete software will be remediated where technically feasible (this includes extended support services if applicable) or exemptions will be issued, tracked, and periodically reassessed. There is currently a project underway to update or migrate applications that are at or near 'end-of-life,' this is being organized at the enterprise level to reduce gaps in the organization's security posture."

OIG Comments:

The response overview states that HAM contests this finding. [redacted] " Additionally, the NIST SP 800-53, Revision 5 guidance clearly states that unsupported software should be replaced, removed, or an alternative source should be in place for continued support. Therefore, we continue to recommend that HAM [redacted]

5. Known Exploitable Vulnerability

[redacted]

NIST SP 800-53, Revision 5, control SI-2 (6) states that the organization "Remove previous versions of [organization-defined software and firmware components] after updated versions have been installed."

Failure to [redacted] increases the risk that it [redacted]

Recommendation 14:

[redacted].

HAM's Response:

"This project is underway. The majority of the identified systems have been remediated [redacted] ***IT is coordinating with business owners for the remaining assets."***

6. Missing Security Patches

[redacted] HAM's *Patch Management Policy* states that patches are installed on a quarterly basis. [redacted]

[redacted]. A service ticket was opened with the application's vendor to resolve the issue.

NIST SP 800-53, Revision 5, control SI-2 states that the organization "Install security-relevant software and firmware updates within [an organization-defined time period] of the release of the updates … ."

Failure to [redacted] increases the risk that [redacted]

Recommendation 15:

We recommend that HAM install all security-relevant software updates identified during this audit.

HAM's Response:

"Health Alliance's Cybersecurity team identified an issue with the previous patching tool used for the enterprise [redacted]) and is deploying the replacement solutions [redacted] Once completed, [redacted]"

F. Contingency Planning

HAM and Carle's contingency planning controls are adequate.

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed HAM and Carle's contingency planning documentation and processes to prevent or minimize interruptions to business operations if disruptive events were to occur. HAM inherits some controls from Carle related to contingency planning.

We observed the following controls in place:

- Documented contingency plan tests;
- An adequately documented business impact assessment; and
- Backup tapes are encrypted.

Nothing came to our attention to indicate that HAM and Carle have not implemented adequate contingency planning controls.

G. Application Change Control

HAM could improve its SDLC controls.

We evaluated HAM's application development and change control process. HAM has implemented policies and procedures related to application configuration management and has also adopted a system development life cycle (SDLC) methodology that IT personnel follow during routine software modifications. HAM does not inherit controls from Carle related to the SDLC of its [redacted] claims adjudication system. We observed the following controls in place:

- Documented change management policy;
- Application change review and approval process; and
- Application change documentation tracking.

However, we noted the following opportunities for improvement related to HAM's application change controls.

1. Developer Training

[redacted]

NIST SP 800-53, Revision 5, control AT-3 states that the organization "Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities] … ." NIST SP 800-53, AT-3 also states, "Roles that may require role-based training include … software developers … ."

Failure to [redacted] increases the risk that [redacted]

Recommendation 16:

We recommend that HAM [redacted]

HAM's Response:

"This project is currently in development, with the first phase being implemented in [redacted] a standalone cybersecurity education module to staff, which will be administered on an annual basis. Information Security is also in the process of hiring an Education and Training specialist to craft and curate specialized training modules for general users as well as privileged access holders [candidate has accepted the position and has a start date of June 26th, 2023]. [redacted]

2. Security Testing and Evaluation

[redacted]

HAM tests code only for general security features, such as ensuring appropriate personnel have access to tables. The *IT SDLC: Testing Policy* states that typical testing activities include unit testing, user acceptance testing, integration testing, and stress testing. [redacted].

NIST SP 800-53, Revision 5, control SA-11 states that "Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as … static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches."

Failure to [redacted], increases the risk [redacted]

Recommendation 17:

We recommend that HAM [redacted]

HAM's Response:

"Health Alliance is in the process of contracting with LRS to conduct periodic security scans of the [redacted] remainder of the applications useable business lifespan. However due to the migration to [redacted] will be used in a static state. Health Alliance does not anticipate performing any configuration changes or developing new code. Maintenance will be limited to addressing 'break/fix' incidents. If requested, we can provide details for code reviews related to [redacted]."

OIG Comments:

The response overview states that HAM contests this finding. [redacted]

[redacted]

Appendix

2022 OIG Audit Response
Health Alliance Medical Plans, Inc.

June 8, 2023

EXECUTIVE SUMMARY

Draft Report Response

Health Alliance Management does not contest the majority of the findings identified by the OPM audit team. Identified items were either known prior to or discovered during the interview process. For known issues Enterprise has or was in the process of developing projects or strategic plans to address gaps. Newly identified findings have been added to work plans or submitted as incidents for remediation. The two items that leadership has flagged as contested are the findings related to: code review for [redacted] (**Recommendation 17**) and unsupported/obsolete applications in network environment (**Recommendation 13**) [see entries for context].

Aside from the items mentioned above, Health Alliance has included supplemental information related to project/work plans to mitigate the remaining findings. These are included in the accompanying zip file. A sizable portion of the corrective action plans referenced below will be dependent upon the enterprise's deployment of the Microsoft Enterprise Security Suite and its comprehensive set of tools and applications. A copy of the organization's 5-year project plan is included in the supplemental information package to illustrate IT's roadmap.

Health Alliance can provide additional information related to specific projects or mitigation plans upon request.

Management requests that any information related to or identified specifically with the Enterprise's security posture be redacted (i.e., identified security applications, project plans, procedures, network diagrams, etc.).

-Glenn Westfield, Information Security Officer Health Alliance Medical Plans,

X _____

Glenn Westfield
Information Security Officer - Health Alliance

ORGANIZATION RESPONSES

Security Management

i. Information Security Program Plan

Recommendation 1

We recommend that HAM and Carle review and update its documented Information Security Program Plan in accordance with its policy and NIST requirements.

Plan Response

Health Alliance is currently in the process of performing a full review and update of the Information Security Program Plan, to reflect changes in infrastructure and enterprise acquisitions (this will include incorporation of new business units into the business continuity plan). The slated completion date for this refresh is [redacted]

Access Controls

No recommendation noted.

Network Security

ii. Network Segmentation

Recommendation 2

We recommend that HAM ensure [redacted].

Plan Response

This has been identified as a long-term project at the enterprise level for the Carle Health system. The project is underway and completion of phase 1 [redacted]. The initial stages of the SD-access implementation are currently underway and contracted project management is overseeing the deployment [See SD-Access Timeline], barring unforeseen delays, the initial implementation is slated for completion [redacted].

iii. Network Access Control

Recommendation 3

We recommend that HAM ensure [redacted].

Plan Response

As mentioned above in Response 2, [redacted] is currently being deployed enterprise wide. Health Alliance Medical Plans and affiliated entities will be covered by enforcement mode [redacted]

iv. Mobile Device Management

Recommendation 4

We recommend that HAM ensure [redacted].

Plan Response

This response will cover Recommendations 4 and 5. Health Alliance IT shared service is in the process of migrating to the [redacted]. This will result in the replacement of several different tools that were being utilized to manage mobile devices. IT is [redacted] to schedule and deploy the enterprise version of Intune to all corporate mobile devices [redacted]. During that adoption, uniform configuration standards will be applied to corporate managed mobile devices. [Enterprise Microsoft Roadmap]

Recommendation 5

We recommend that HAM ensure [redacted]. Note – this recommendation cannot be implemented until the controls from Recommendation 4 are in place.

Plan Response

Once the actions in Response 4 are completed, mobile assets will be centrally managed and monitored for compliance. Mobile devices will be audited for compliance and non-compliant assets will generate incident tickets for remediation.

v. Cryptographic Protection

Recommendation 6

We recommend that HAM ensure [redacted].

Plan Response

Enterprise IT has initiated a project to remediate this issue for the organization. Phase 1 of the project has been completed. Fixes have been applied to all the current [redacted]

[redacted] in use for server and workstation creation. Phase 2 for the project [redacted] is currently underway.

SECURITY EVENT MONITORING AND INCIDENT RESPONSE

vi. Incident Response Training

Recommendation 7

We recommend that HAM ensure [redacted]

Plan Response

Health Alliance is in the process of updating the Information Security Program [redacted].

Recommendation 8

We recommend that HAM ensure [redacted]. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

Plan Response

Health Alliance leadership has identified this as an opportunity to improve and supplement our current process. There is executive level training for the incident response program (HICS), the process is [redacted] Management is currently interviewing candidates for a new Information Security Education and Awareness specialist position [redacted]

CONFIGURATION MANAGEMENT

vii. Baseline Configuration Review

Recommendation 9

We recommend that HAM develop and then implement [redacted].

Plan Response

Health Alliance currently has a project underway [redacted]. System baselines have been developed and deployed for the server environment broadly. Shared Service IT has deployed [redacted] to the enterprise network environment and the workstation and VM

image configurations are being evaluated. Enterprise has [redacted]. This will include wide deployment of agents to corporate assets that will facilitate increased environmental visibility and monitoring at the client level. This project will be dependent upon [redacted]

viii. Least Functionality Review

Recommendation 10

We recommend that HAM [redacted].

Plan Response

This process will be incorporated into the periodic system baseline review.

ix. Impact Analyses

Recommendation 11

We recommend that HAM update its *IT Change Control Policy* to define requirements for approving or disapproving configuration-controlled changes with explicit consideration for the results of impact analyses.

Plan Response

IT Change Control Policy to be updated to include language requiring impact review of submitted changes.

Recommendation 12

We recommend that HAM [redacted]

Plan Response

Change Control submission form updated to include mandatory field for security and privacy impact analysis [redacted].

x. Unsupported Software

Recommendation 13

We recommend that HAM replace or identify extended support for software identified during this audit which is no longer supported by the developer, vendor, or manufacturer.

Plan Response

Health Alliance management has identified this as a long term [redacted]sk for the organization. Unsupported or obsolete software will be remediated where technically feasible (this includes extended support services if applicable) or exemptions will be

issued, tracked, and periodically reassessed. There is currently a project underway to update or migrate applications that are at or near "end-of-life," this is being organized at the enterprise level to reduce gaps in the organization's security posture.

xi. Know Exploitable Vulnerability

Recommendation 14

[redacted].

Plan Response

This project is underway. The majority of the identified systems have been remediated [redacted]. IT is coordinating with business owners for the remaining assets.

xii. Missing Security Patches

Recommendation 15

We recommend that HAM install all security-relevant software updates identified during this audit.

Plan Response

Health Alliance's Cybersecurity team identified an issue with the previous patching tool used for the enterprise ([redacted]) and is deploying the replacement solutions ([redacted]). Once completed, [redacted].

CONTINGENCY PLANNING

No recommendation noted.

APPLICATION CHANGE CONTROL

xiii. Developer Training

Recommendation 16

We recommend that HAM require developers to complete role-based security and privacy training.

Plan Response

This project is currently in development, with the first phase being implemented in June of 2023. HR will roll out a standalone cybersecurity education module to staff, which will be administered on an annual basis. Information Security is also in the process of hiring an Education and Training specialist to craft and curate specialized training modules for general users as well as privileged access holders [candidate has accepted the position

and has a start date of June 26th, 2023]. For the latter, training will be required prior to activation of the elevated access account.

xiv. Security Testing and Evaluation

Recommendation 17

We recommend that HAM updates its policies and procedures to require security testing and evaluation when changes are made to [redacted] code.

Plan Response

Health Alliance is in the process of contracting with LRS to conduct periodic security scans of the [redacted] remainder of the applications useable business lifespan. However due to the migration to [redacted] will be used in a static state. Health Alliance does not anticipate performing any configuration changes or developing new code. Maintenance will be limited to addressing "break/fix" incidents. If requested, we can provide details for code reviews related to [redacted].

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: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

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