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 GLOBALHEALTH, INC.

Report Number 1C-IM-00-19-037
April 16, 2020

EXECUTIVE SUMMARY

Audit of the Information Systems General Controls at GlobalHealth, Inc.

Report No. 1C-IM-00-19-037 **April 16, 2020**

Why Did We Conduct The Audit?

GlobalHealth, Inc. (GlobalHealth) 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 GlobalHealth's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by GlobalHealth 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 GlobalHealth's IT security controls determined that its IT security program is immature and could be improved. However, GlobalHealth is aware of many of its shortcomings and is actively working to correct its weaknesses. There are several areas where GlobalHealth has already successfully implemented controls. Specifically, our Audit of GlobalHealth's IT security controls found that:

- GlobalHealth is lacking numerous policies that make up the foundation of an information security program.
- GlobalHealth [redacted].
- The GlobalHealth vulnerability management program is immature and could be improved.
- GlobalHealth has not established security configuration standards for its operating systems and therefore cannot perform routine reviews of security configurations.
- GlobalHealth recently began collecting system event and audit logs. However, GlobalHealth is still in the process of developing the ability to utilize these logs to detect and respond to security events.
- GlobalHealth has implemented a demilitarized zone and moved all externally accessible systems into this zone.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
CSF	**Common Security Framework**
DMZ	**Demilitarized Zone**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
GlobalHealth	**GlobalHealth, Inc.**
HITRUST	**Health Information Trust Alliance**
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**
SIEM	**Security Information and Event Management**

TABLE OF CONTENTS

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 GlobalHealth, Inc. (GlobalHealth).

The audit was conducted pursuant to FEHBP contract CS 2893; 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.

This was our first audit of the information technology (IT) general security controls at GlobalHealth. All GlobalHealth 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 GlobalHealth'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 GlobalHealth'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 GlobalHealth'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 GlobalHealth to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Oklahoma City, Oklahoma.

The onsite portion of this audit was performed in September of 2019. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at GlobalHealth as of September 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by GlobalHealth. 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 GlobalHealth'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 GlobalHealth'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 to evaluating GlobalHealth'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 GlobalHealth's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, GlobalHealth 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 GlobalHealth's overall IT security program. We evaluated GlobalHealth's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

GlobalHealth has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. GlobalHealth has also documented policies for some information security areas, such as risk management, remote access, and encryption.

The following sections document several opportunities for improvement related to GlobalHealth's enterprise security controls.

1. Entity-Wide IT Policies and Procedures

GlobalHealth lacks numerous policies that make up the foundation of an information security program.

IT policies and procedures are the foundation of a strong information security program, as these documents provide guidance on how IT security should be managed at a specific organization. As mentioned above, GlobalHealth has created and approved some IT security policies. However, it is still lacking numerous policies that make up the foundation of an information security program. GlobalHealth is aware of its lack of documented IT security policies and procedures and has begun the process of implementing Health Information Trust Alliance's Common Security Framework (HITRUST CSF), a cybersecurity framework designed for the protection of sensitive health information. Founded in 2007, HITRUST's purpose is to create an integrated approach to information risk management and compliance to ensure that all organizational policies and procedures are aligned, maintained, and comprehensive.

HITRUST's advisory councils include subject matter experts from the healthcare sector as well as relevant technology vendors and information security and privacy assurance experts. Developed in collaboration with data protection and healthcare professionals, the HITRUST CSF combines multiple relevant regulations and standards into a single overarching security and privacy framework. Utilizing the CSF will assist GlobalHealth in developing the policies and procedures required as part of a comprehensive information security program.

FISCAM states that entities should have "A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources."

FISCAM further states that "to be effective, the [policies and plan] should be maintained to reflect current conditions. [They] should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in entity mission or the types and configuration of computer resources in use."

Failure to document well-defined IT security policies and procedures may result in wide-spread organizational problems. Security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied.

Recommendation 1

We recommend that GlobalHealth develop comprehensive IT security policies and procedures. At a minimum, it should ensure that the following topics are addressed in documented policies and procedures:

- Auditing/Monitoring User and Administrator Activity
- Configuration Management
- Cryptographic Key Management
- Data Exfiltration
- Firewall Management
- Inventory Management
- Log Management
- Patch Management
- Security Incident Response
- Segregation of Duties
- Software Lifecycle Management
- Vulnerability Management
- Web Content Filtering

GlobalHealth's Response:

"GlobalHealth is beginning a HITRUST engagement that will identify the required policies based on regulatory and industry standards. We will be incorporating the identified policies from this recommendation."

OIG Comment:

As a part of the audit resolution process, we recommend that GlobalHealth 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 GlobalHealth agrees to implement.

2. Segregation of Duties

As mentioned above, GlobalHealth does not have policies or procedures that address the requirement for segregation of duties controls. During our audit, we identified some segregation of duties conflicts. For example, the firewall change tickets provided to the auditors for review were created and approved by the same individual.

FISCAM suggests that "organizations adopt segregation of duties control matrices as a guideline of the job responsibilities that should not be combined."

Failure to properly identify conflicting roles increases the risk that employees are granted excess privileges that could be misused.

Recommendation 2

We recommend that GlobalHealth assess the current segregation of duties controls throughout the information security department, including but not limited to areas such as firewall management and change management.

GlobalHealth's Response:

"GlobalHealth has implemented a plan to accomplish the segregation of duties. We have identified a current need and have financial approval for a Security Administrator and Security Engineer that will allow us to perform segregation of duties. As we progress through HITRUST, we will evaluate and implement controls around segregation of duties."

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 GlobalHealth'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.

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

We observed the following controls in place:

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

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

1. Internal Network Segmentation

Firewalls are used at ingress and egress locations on GlobalHealth's network in order to control network traffic from external connections and vendors. A demilitarized zone (DMZ) has recently been established to segregate externally accessible systems from GlobalHealth's internal network. However, not all externally accessible systems have been moved into the DMZ. In addition, [redacted].

NIST SP 800-41, Revision 1, advises 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 by external attackers. Important internal systems should be placed behind internal firewalls."

Failure to segregate user and server network segments increases the risk that a system could be compromised and allow unauthorized access to sensitive servers and data.

Recommendation 3

We recommend that GlobalHealth complete its project to place externally accessible systems into the DMZ.

GlobalHealth's Response:

"A DMZ was created and external-facing services have been moved into it."

OIG Comment:

In response to the draft audit report, GlobalHealth provided evidence that all externally accessible systems have been moved into the DMZ. No further action is required.

Recommendation 4

We recommend that GlobalHealth [redacted]

GlobalHealth's Response:

"GlobalHealth will be [redacted] ***The results will be presented to the Executive Compliance Committee for review and acceptance no later than second quarter of 2020."***

2. Multi-Factor Authentication

GlobalHealth [redacted] Furthermore, GlobalHealth [redacted]

[redacted] Although FEHBP-contracted health insurance carriers are not government entities, they do process sensitive healthcare data of Federal employees. As such, [redacted]

Failure to [redacted]

Recommendation 5

We recommend that GlobalHealth [redacted]

GlobalHealth's Response:

[redacted]

3. Network Access Control

GlobalHealth [redacted]. This issue is compounded by the [redacted].

[redacted]

Failure to [redacted]

Recommendation 6

We recommend that GlobalHealth [redacted]

GlobalHealth's Response:

"GlobalHealth [redacted]

4. Firewall Policy

GlobalHealth personnel administer the firewalls for its two data centers, but outsource the firewall administration for GlobalHealth's office locations to a vendor. Neither GlobalHealth nor the vendor have documented firewall configuration policies that describe current rulesets, approved traffic, and other organization-defined policy.

NIST SP 800-41, Revision 1, states 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, advises that the organization should identify, document, and approve any deviations from established configuration settings.

Failure to document a standard firewall configuration policy increases the organization's risk of exposure to insecure traffic and vulnerabilities.

Recommendation 7

We recommend that GlobalHealth document approved security configuration standards for firewalls deployed in its technical environment.

GlobalHealth's Response:

"We have budgeted for and are currently reviewing baselining software with the intent of implementing this in 2020."

Recommendation 8

We recommend that GlobalHealth implement a process to document and track firewall configuration settings that deviate from the approved firewall configuration standard. Note – This recommendation cannot be implemented until the controls from Recommendation 7 are in place.

GlobalHealth's Response:

GlobalHealth partially agreed with the findings. "We have matured our Change Control process and are documenting firewall configuration. We are recording any request for change and recording the change activity using [redacted]. We are currently setting the baseline for the firewall."

OIG Comment:

The intent of this recommendation is for GlobalHealth to track any deviations from the firewall configuration policy/standard that we recommended GlobalHealth create in Recommendation 7, above. It is not possible to track deviations from a policy/standard without first establishing the standard itself. We recommend that GlobalHealth provide OPM's Healthcare and Insurances Office, Audit Resolution Group with evidence that it has documented a firewall configuration standard, then provide a sample of [redacted] tickets documenting any deviations from the configuration standard.

5. Firewall Auditing

As mentioned above, GlobalHealth does not have a documented firewall configuration policy/standard. As a result, GlobalHealth cannot effectively audit its firewall configurations.

NIST SP 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with organization's policies.

Failure to routinely audit firewall settings increases the risk that unauthorized changes to the firewall's configuration remain undetected.

Recommendation 9

We recommend that GlobalHealth perform routine audits of its current firewall configurations against an approved policy. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

GlobalHealth's Response:

"An Information Security Auditor position has been approved to resolve this issue. We anticipate the auditor will be hired by end of second quarter or third quarter 2020."

6. Data Exfiltration

GlobalHealth currently has detective controls in place for identifying sensitive data (e.g., social security numbers) [redacted]. Furthermore, GlobalHealth has a "bring your own device" program that utilizes [redacted]

Additionally, NIST SP 800-53, Revision 4, prescribes that "The organization designs information systems to support privacy by automating privacy controls."

Failure to [redacted]

Recommendation 10

We recommend that GlobalHealth implement technical controls to [redacted]

GlobalHealth's Response:

"We are currently evaluating and testing several solutions based on our [redacted] environment to determine if this can be done with our current technology. If we are unable to use our current technology, we plan [to] implement another solution."

Recommendation 11

We recommend that GlobalHealth implement technical controls to prevent [redacted].

GlobalHealth's Response:

"Due to recent changes to the [redacted] platform, we are evaluating if this can be done with our existing environment. If not, we will implement a new DLP solution."

7. Vulnerability Management

The GlobalHealth vulnerability management program is immature and could be improved. GlobalHealth has a small infrastructure team that is responsible for vulnerability management. Ad hoc and un-credentialed vulnerability scans are performed on some servers in its environment, while some systems are not scanned at all. As mentioned above in Section A.1, GlobalHealth does not have policies and procedures for remediating identified weaknesses in a timely manner. The effect of GlobalHealth's ad-hoc process for vulnerability detection and remediation was evidenced in the OIG's scan results, as discussed below in section B.8.

NIST SP 800-53, Revision 4, advises that the organization, "Scans for vulnerabilities in the information system and hosted applications …" and "Remediates legitimate vulnerabilities … in accordance with an organizational assessment of risk … ."

NIST SP 800-53, Revision 4, also explains that the organization should "[Implement] privileged access authorization … for … vulnerability scanning activities … ." It expounds on this requirement by stating, "Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning."

Failure to perform routine credentialed vulnerability scanning on all network devices increases the risk that system flaws go undetected, leaving GlobalHealth exposed to unknown threats.

Recommendation 12

We recommend that GlobalHealth develop and implement a process to routinely conduct credentialed vulnerability scans on all systems, track weaknesses, and remediate weaknesses in a timely manner.

GlobalHealth's Response:

"Currently, the staff is engaged in mitigating discovered vulnerabilities. As part of our ongoing effort, the new Security Administrator and Engineer will be tasked with scanning and mitigating any weakness discovered."

8. Vulnerabilities Identified by OIG Scans

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

NIST SP 800-53, Revision 4, states that organizations should 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 13

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

GlobalHealth's Response:

"The high-risk items are currently being addressed. This effort will be facilitated with additional headcount being hired."

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 of GlobalHealth's security event monitoring and incident response programs identified the following controls in place:

- Controls to geo-block traffic; and
- Alerts configured for account elevation, expiration, and lockout.

The following sections document several opportunities for improvement related to GlobalHealth's security event monitoring and incident response controls.

1. Network Monitoring

GlobalHealth monitors traffic at the edge of its network. It also has a tool in place to report when administrative accounts are created or deleted. In response to the draft audit report, GlobalHealth has also provided evidence of the installation of a Security Information and Event Management (SIEM) tool, which is now ingesting system event and audit logs. However, GlobalHealth is still in the process of building out the ability to receive and respond to alerts from the SIEM tool.

NIST SP 800-53, Revision 4, states that organizations should "[monitor] and [control] communications at the external boundary of the system and at key internal boundaries within the system … ."

NIST SP 800-53, Revision 4, also advises organizations to routinely "[review] and [analyze] information system audit records … for indications of … organization-defined inappropriate or unusual activity … ."

Failure to routinely monitor key network points increases the risk that inappropriate or malicious activity will go undetected, increasing the impact of a potential breach.

Recommendation 14

We recommend that GlobalHealth implement a comprehensive process to monitor internal network activity.

GlobalHealth's Response:

"GlobalHealth has budgeted for and is currently evaluating internal monitoring software."

2. Incident Response Procedures

GlobalHealth does not have a documented incident response process. Furthermore, it has conducted only one tabletop incident response test, in November of 2019. GlobalHealth is aware of these gaps and reported that its incident response policy is scheduled to be documented and approved by the first quarter of 2020.

GlobalHealth does not have an approved incident response process and therefore cannot effectively test its incident response process.

FISCAM states, "It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed."

NIST SP 800-53, Revision 4, advises that the organization "Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery … ."

NIST SP 800-53, Revision 4, also advises that "The organization tests the incident response capability for the information system … to determine the incident response effectiveness and document the results."

Failure to document and test the incident response plan increases the risk that responses to security events could be delayed or ineffective.

Recommendation 15

We recommend that GlobalHealth develop and implement incident response procedures in accordance with NIST SP 800-53, Revision 4.

GlobalHealth's Response:

"GlobalHealth has begun the process of re-evaluating on incident response. As we progress in becoming HITRUST certified, we will be incorporating NIST standards."

Recommendation 16

We recommend that GlobalHealth routinely test its incident response plan and that any lessons learned are incorporated into the plan and relevant policies. Note – This recommendation cannot be cannot be implemented until the controls from Recommendation 15 are in place.

GlobalHealth's Response:

GlobalHealth partially agreed with the findings. "GlobalHealth has a basic Incident Response plan. GlobalHealth conducted a baseline tabletop exercise in November of 2019. It focused on a response to a [redacted] attack. We are documenting the outcome and our AVPs have requested that managers from different departments go through the same exercise by the end of the first quarter of 2020. The outcome of the exercise is assuring alignment with NIST standards, having corporate-wide incidence plans for business-facing departments and updating the IT disaster recovery plan"

OIG Comment:

During the fieldwork phase of this audit, we received a draft version of GlobalHealth's incident response plan. While the plan does cover the basic elements of NIST SP 800-53, Revision 4, IR-1 a.1., we were not provided a final, approved copy of the plan. In addition, we did not receive incident response procedures as described in NIST SP 800-53, Revision 4, IR-1 a.2. In response to Recommendation 15, GlobalHealth has indicated that these procedures are currently being developed.

Additionally, while performing a scenario-specific tabletop exercise is certainly beneficial, the primary purpose of an incident response test is to evaluate the effectiveness of the established incident response policies and procedures. As such, GlobalHealth should first develop and approve incident response policies and procedures as prescribed in Recommendation 15. At that time, GlobalHealth should submit evidence that tests were completed based on the established incident response procedures, that lessons learned were documented, and that the incident response policies and procedures were updated based on the test results.

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 GlobalHealth'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.

GlobalHealth has a documented change control process.

Our review found the following controls in place:

- A standardized system change control process is followed; and
- System configuration changes are documented.

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

1. Security Configuration Standards

GlobalHealth configures its servers using a standard image for most operating systems. The images are developed internally and maintained by GlobalHealth personnel. However, GlobalHealth has not established security configuration standards for its operating systems. Security configuration standards are formally approved documents that detail an organization's approved security settings for each operating system in its network.

GlobalHealth does not have approved security configuration standards for all of its operating platforms.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements … ."

In addition, NIST SP 800-53, Revision 4, also states that an organization should "[Develop], [document], and [maintain] … a current baseline configuration of the information system."

Failure to establish approved system configuration settings increases the risk that the system may not be configured in a secure manner.

Recommendation 17

We recommend that GlobalHealth document and implement approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

GlobalHealth's Response:

"Configuration baseline software has been budgeted and is being evaluated."

Recommendation 18

We recommend that GlobalHealth implement a process to document and track any configuration settings that deviate from the approved security configuration standards. Note – This recommendation cannot be implemented until the controls from Recommendation 17 are in place.

GlobalHealth's Response:

"A solution will be implemented after controls from recommendation 17 are in place."

2. Security Configuration Auditing

GlobalHealth does not perform routine reviews of security configurations after the initial build of a new server. As noted above, GlobalHealth does not have documented security configuration standards for its operating platforms and databases deployed in its technical environment. Without approved security configuration standards, GlobalHealth cannot effectively audit its systems' security settings (i.e., there are no approved settings to which to compare the actual settings).

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

FISCAM states that "A process and related procedures needs to be established to document the results from monitoring configuration items and ensure that discrepancies are properly corrected."

Failure to implement a configuration compliance auditing program increases the risk that servers are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 19

We recommend that GlobalHealth implement a process to routinely audit server security configuration settings against an approved security configuration standard. Note – this recommendation cannot be implemented until the controls from Recommendation 18 are in place.

GlobalHealth's Response:

"A solution will be implemented after controls from recommendation 18 are in place."

APPENDIX

210 Park Ave. | Suite 2800 | Oklahoma City, OK 73102-5621

January 24, 2020 **SENT VIA EMAIL**

[redacted]
Office of the Inspector General
U.S. Office of Personnel Management
Washington, D.C.

RE: GlobalHealth Response & Action Plans

OPM/OIG Information Technology Audit

GlobalHealth appreciates the time taken to review and prepare these audit findings. We regard the findings as an opportunity to improve our commitment to our members. Below you will find our response, action plans, and time frames.

GlobalHealth will be undertaking two major projects this year and increasing our security operations and Information Security program. We are currently contracting with Meditology Associates to implement and ready us for HITRUST certification. Assessment, implementation, and certification will take 18 months. The initial focus is to become certified with a 3+ score in all domains, meeting HITRUST minimum certification requirements for the following areas:

REGULATORY FACTORS INCLUDED

Federal

- CMS Minimum Requirements
- HIPAA
- CRR V2016

State

- Nevada Security of Personal Information
- Texas Health and Safety Code
- 23 NYCRR 500
- Massachusetts Data Protection Act

Once we complete initial certification, we will continue to progress to a measured and managed state.

The second project is to implement a SIEM by June 2020. The contract will be finalized the last week in January with a start date the second week in February 2020. It is anticipated that we will meet our June 2020 deadline to be fully implemented, monitoring, and mitigating any identified issues.

In support of these initiatives and other recommendations by OPM/OIG, we are reviewing our operation security staff. Initial plans are to hire a security administrator and security engineer by the second quarter of 2020. To support the HITRUST and several identified baselining issues, an internal Information Security auditor will be hired by the third quarter of 2020.

RECOMMENDATION RESPONSES

SECURITY MANAGEMENT

Entity-Wide IT Policies and Procedures - Recommendation 1

We recommend that GlobalHealth develop comprehensive IT security policies and procedures. At a minimum, it should ensure that the following topics are addressed in documented policies and procedures:

- Auditing/Monitoring User and Administrator Activity
- Configuration Management
- Cryptographic Key Management
- Data Exfiltration
- Firewall Management
- Inventory Management
- Log Management
- Patch Management
- Security Incident Response
- Segregation of Duties
- Software Lifecycle Management
- Vulnerability Management
- Web Content Filtering

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth is beginning a HITRUST engagement that will identify the required policies based on regulatory and industry standards. We will be incorporating the identified policies from this recommendation.

Segregation of Duties - Recommendation 2

We recommend that GlobalHealth assess the current segregation of duties controls throughout the information security department, including but not limited to areas such as firewall management and change management.

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth has implemented a plan to accomplish the segregation of duties. We have identified a current need and have financial approval for a Security Administrator and Security Engineer that will allow us to perform segregation of duties. As we progress through HITRUST, we will evaluate and implement controls around segregation of duties.

NETWORK SECURITY

Internal Network Segmentation - Recommendation 3

We recommend that GlobalHealth complete its project to place externally accessible systems in the DMZ.

GlobalHealth Response	Agreed with findings
Action Plan	A DMZ was created and external-facing services have been moved into it.

Internal Network Segmentation - Recommendation 4

We recommend that GlobalHealth [redacted]

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth will be [redacted]. The results will be presented to the Executive Compliance Committee for review and acceptance no later than second quarter of 2020.

Multifactor Authentication - Recommendation 5

We recommend that GlobalHealth require [redacted]

GlobalHealth Response	Agreed with findings
Action Plan	[redacted]

Network Access Control - Recommendation 6

We recommend that GlobalHealth implement [redacted]

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth is expanding its [redacted]

Firewall Policy - Recommendation 7

We recommend that GlobalHealth document approved security configuration standards for firewalls deployed in its technical environment.

GlobalHealth Response	Agreed with findings
Action Plan	We have budgeted for and are currently reviewing baselining software with the intent of implementing this in 2020.

Firewall Policy - Recommendation 8

We recommend that GlobalHealth implement a process to document and track firewall configuration settings that deviate from the approved firewall configuration standard. Note –This recommendation cannot be implemented until the controls from Recommendation 7 are in place.

GlobalHealth Response	Partially agreed with findings
Action Plan	We have matured our Change Control process and are documenting firewall configuration. We are recording any request for change and recording the change activity using [redacted]. We are currently setting the baseline for the firewall.

Firewall Auditing - Recommendation 9

We recommend that GlobalHealth perform routine audits of its current firewall configurations against an approved policy. Note –this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

GlobalHealth Response	Agreed with findings
Action Plan	An Information Security Auditor position has been approved to resolve this issue. We anticipate the auditor will be hired by end of second quarter or third quarter 2020.

Data Exfiltration - Recommendation 10

We recommend that GlobalHealth implement technical controls to [redacted].

GlobalHealth Response	Agreed with findings
Action Plan	We are currently evaluating and testing several solutions based on our [redacted] environment to determine if this can be done with our current technology. If we are unable to use our current technology, we plan implement another solution.

Data Exfiltration - Recommendation 11

We recommend that GlobalHealth implement technical controls to prevent [redacted].

GlobalHealth Response	Agreed with findings
Action Plan	Due to recent changes to the [redacted] platform, we are evaluating if this can be done with our existing environment. If not, we will implement a new DLP solution.

Vulnerability Management - Recommendation 12

We recommend that GlobalHealth develop a process to routinely conduct credentialed vulnerability scans on all systems, track weaknesses, and remediate weaknesses in a timely manner.

GlobalHealth Response	Agreed with findings
Action Plan	Currently, the staff is engaged in mitigating discovered vulnerabilities. As part of our ongoing effort, the new Security Administrator and Engineer will be tasked with scanning and mitigating any weakness discovered.

Vulnerabilities Identified by OIG Scans - Recommendation 13

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

GlobalHealth Response	Agreed with findings
Action Plan	The high-risk items are currently being addressed. This effort will be facilitated with additional headcount being hired.

SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Network Monitoring - Recommendation 14

We recommend that GlobalHealth implement a comprehensive process to monitor internal network activity.

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth has budgeted for and is currently evaluating internal monitoring software.

Incident Response Procedures - Recommendation 15

We recommend that GlobalHealth develop and implement incident response procedures in accordance with NIST SP 800-53, Revision 4

GlobalHealth Response	Agreed with findings
Action Plan	GlobalHealth has begun the process of re-evaluating on incident response. As we progress in becoming HITRUST certified, we will be incorporating NIST standards.

Incident Response Procedures - Recommendation 16

We recommend that GlobalHealth routinely test its incident response plan and that any lessons learned are incorporated into the plan and relevant policies. Note –This recommendation cannot be implemented until the controls from recommendations 15are in place.

GlobalHealth Response	Partially agreed with findings
Action Plan	GlobalHealth has a basic Incident Response plan. GlobalHealth conducted a baseline tabletop exercise in November of 2019. It focused on a response to a [redacted] attack. We are documenting the outcome and our AVPs have requested that managers from different departments go through the same exercise by the end of the first quarter of 2020. The outcome of the exercise is assuring alignment with NIST standards, having corporate-wide incidence plans for business-facing departments and updating the IT disaster recovery plan

CONFIGURATION MANAGEMENT

Security Configuration Standards - Recommendation 17

We recommend that GlobalHealth document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

GlobalHealth Response	Agreed with findings
Action Plan	Configuration baseline software has been budgeted and is being evaluated.

Security Configuration Standards - Recommendation 18

We recommend that GlobalHealth implement a process to document and track configuration settings that deviate from the approved security configuration standards. Note –This recommendation cannot be implemented until the controls from recommendation 17 are in place.

GlobalHealth Response	Agreed with findings
Action Plan	A solution will be implemented after controls from recommendation 17 are in place.

Security Configuration Auditing - Recommendation 19

We recommend that GlobalHealth implement a process to routinely audit server security configuration settings against an approved security configuration standard. Note –this recommendation cannot be implemented until the controls from Recommendation 18 are in place.

GlobalHealth Response	Agreed with findings
Action Plan	A solution will be implemented after controls from recommendation 18 are in place.

Thank you for the opportunity to respond.

Sincerely,

Kyle Hager
AVP, Operations
GlobalHealth Holdings, LLC

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