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 MVP Health Care

Report Number 1C-GA-00-17-010
June 30, 2017

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at MVP Health Care

Report No. 1C-GA-00-17-010 **June 30, 2017**

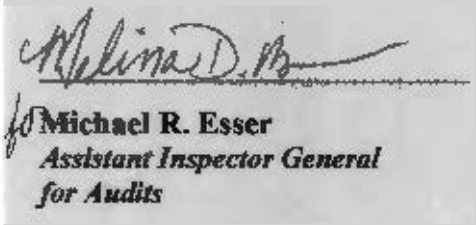
Why Did We Conduct the Audit?

MVP Health Care (MVP) 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 MVP's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by MVP 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 the IT security controls of MVP determined that:

- MVP has established an adequate security management program.
- MVP has implemented a variety of physical and logical access controls. However, we noted several areas of concern related to privileged user access, segregation of duties policies and procedures, physical access reviews, and data center physical access controls.
- MVP has implemented an incident response and network security program. However, we noted several areas of concern related to firewall configuration reviews, work station patching, authenticated vulnerability scanning, system lifecycle management, and network access controls.
- MVP has developed and documented formal configuration management policies and procedures. However, MVP does not have documented security configuration standards and does not perform routine configuration compliance reviews.
- MVP's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. However, MVP does not perform routine business continuity plan testing, and its tape backup encryption key management process could be improved.
- MVP has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

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

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 MVP Health Plan (MVP).

The audit was conducted pursuant to FEHBP contracts CS 2362; 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 MVP's information technology (IT) general and application controls. All MVP personnel that worked with the auditors were helpful and open to ideas and suggestions. 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 MVP's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Configuration management;
- Segregation management;
- Contingency planning; and
- Application controls specific to MVP'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 MVP'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 MVP'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 MVP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Schenectady, New York.

The onsite portion of this audit was performed in October through December of 2016. 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 and application controls in place at MVP as of December 2016.

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

- Gathered documentation and conducted interviews;
- Reviewed MVP's business structure and environment;
- Performed a risk assessment of MVP'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); 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 MVP's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

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

MVP maintains a series of thorough IT security policies and procedures.

MVP has documented policies that outline its enterprise security management framework. MVP has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. We also reviewed MVP's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that MVP does not have 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 of MVP's facilities and data center. We also examined the logical access controls protecting sensitive data on MVP's network environment and claims processing related applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting and removing physical access to facilities and the data center;
- Procedures for appropriately granting, adjusting, and removing logical access; and
- Routinely reviewing user access.

The following sections document opportunities for improvement related to MVP's access controls.

1. Privileged User Authentication

MVP issues dedicated privileged user accounts to system administrators that require access to sensitive systems. [redacted]. Although these accounts do not allow access to information systems over remote connections, we expect all FEHBP contractors to require multi-factor authentication for administrator-level access to information systems.

The Federal government requires multi-factor authentication for all information system users. Although MVP is not a government entity, it does process sensitive healthcare data of Federal employees. Therefore, we recommend that MVP implement this control for privileged users at a minimum. NIST SP 800-53, Revision 4, states that information systems should implement multi-factor authentication for network access to privileged accounts. Failure to implement multi-factor authentication increases the risk that privileged user credentials could be compromised and that unauthorized users could access sensitive and proprietary data.

Recommendation 1

We recommend that [redacted]

MVP Response:

"Privileged user [redacted] Consideration of network impact, processes, and budget will be key factors in the decision. In the interim, MVP will continue to monitor and alert on log activity of privileged users through our security event and information management system."

OIG Comment:

As a part of the audit resolution process, we recommend that MVP provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully

implemented this recommendation. This statement applies to subsequent recommendations in this audit report that MVP agrees to implement.

2. Segregation of Duties

MVP hiring managers are responsible for designating access rights to information systems for new employees. Each year, managers are required to certify that all active accounts are necessary and appropriate. However, MVP does not have any formal guidance that prohibits the assignment of conflicting roles (i.e., a segregation of duties policy and procedures or a roles matrix).

FISCAM states that "Entity-wide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced." Failure to provide adequate segregation of duties guidance increases the risk that users could be granted access to data and processes inappropriate for their job function.

Recommendation 2

We recommend that MVP develop policies and procedures to ensure that access to information systems is granted with proper segregation of duties.

MVP Response:

"MVP plans to document segregation of duties controls currently in place that are tested on regular basis as part of ongoing audits associated with key business controls. MVP will also evaluate the feasibility of adding segregation of duties controls within its account management and user recertification processes."

3. Physical Access Review

MVP performs regular audits of active access badges for its facilities and datacenter. This review includes controls to identify access cards that were not disabled after an employee's termination. However, we determined that several employees were issued multiple active access cards that allow access to MVP facilities. This occurred because several employees were issued new badges and the old badges were never disabled. MVP subsequently disabled the old badges during the course of this audit.

FISCAM states that "Management should regularly review the list of persons authorized to have physical access to sensitive facilities, including contractors and other third parties." Failure to properly disable active badges that have been replaced due to being lost or stolen could leave the organization's facilities vulnerable to unauthorized access.

Recommendation 3

We recommend that MVP improve its physical access authorization review to include controls to detect duplicate badges.

MVP Response:

"MVP will include controls to detect duplicate badges in the ongoing monthly audits over the physical access system."

4. Data Center Physical Access

MVP's primary data center is located [redacted]; secondary data center operations are outsourced to a vendor. Access to the primary data center is controlled by a proximity access card reader. However, we expect data centers of all FEHBP contractors to also have the following additional controls that were not present at MVP's facility:

- Multi-factor authentication to enter the secure area (e.g., cipher lock or biometric device in addition to an access card); and

- A technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, two door "man traps," etc.).

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 4

We recommend that MVP implement multi-factor authentication and piggybacking prevention controls at its primary data center.

MVP Response:

"MVP is evaluating the implementation of a new building security system. The implementation of a new building security system would include requirements for providing multi-factor authentication for entry into the data center. In the interim, MVP's data center access is limited to a small number of authorized personnel and reviews of access are performed on a quarterly basis. The data center also has 24/7 closed circuit cameras to monitor the points of entry."

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 MVP'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.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A documented incident response program.

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

1) Documented Firewall Policy and Configuration Review

MVP has firewalls placed at its network perimeter and uses an automated tool to scan its firewalls for vulnerabilities. However, MVP has not formally documented a policy that

specifies the types of traffic allowed by the organization and the approved settings that are needed to harden the firewalls within the network.

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

MVP is unable to effectively audit its current firewall configuration without an approved policy or standard for comparison. A firewall policy should be established as a means to compare approved settings to the actual/current settings. Failure to document an approved firewall policy increases the risk that the firewall does not properly manage network traffic. Failure to audit firewall configurations against a firewall policy or configuration standard increases the risk that the firewalls could be compromised and that rules exist which allow unacceptable or unneeded network traffic.

Recommendation 5

We recommend that MVP document and approve a firewall policy and/or configuration standard.

MVP Response:

"MVP Health Care has implemented an approved Firewall Standards document as of March 2017. Please see Appendix 5."

OIG Comment:

The evidence provided by MVP in response to the draft audit report indicates that the Plan has documented an approved firewall configuration standard; no further action is required.

Recommendation 6

We recommend that MVP perform routine audits of its current firewall configurations against an approved firewall policy that is customized to its technical environment. Note –

this recommendation cannot be implemented until the controls from Recommendation 5 are in place.

MVP Response:

"MVP will be implementing a firewall configuration audit process by which external open ports and firewall policy are reviewed on a routine basis."

2) Workstation Patching

We performed credentialed vulnerability and configuration compliance scans on a sample of user workstations in the MVP environment. Our scan results indicated that several workstations were missing numerous software patches. We believe that the issues were widespread enough to indicate a flaw in MVP's patch management methodology, but we were not able to identify the exact cause.

NIST 800-53, Revision 4, states that the organization should identify, report, and correct information system flaws. Security relevant software and firmware updates including patches, service packs, hotfixes, and anti-virus signatures should be updated. Failure to apply security patches increases the risk that vulnerabilities will not be remediated and systems are left vulnerable to malicious activity.

Recommendation 7

We recommend that MVP improve its patch management methodology to ensure that workstation patches are applied in a timely manner.

MVP Response:

"MVP has implemented authenticated scanning on a subset of workstations in order to help prioritize patching and ensure timely remediation. The subset of workstations acts as a representative of the entire enterprise, as it is a cross-section of our workstation landscape. The workstations scans have been rolled into our routine vulnerability scanning schedule as of March 2017. Please see Appendix 7."

OIG Comment:

The evidence provided by MVP in response to the draft audit report indicates that the Plan has improved its patch management methodology to ensure that workstations are applied in a timely manner; no further action is required.

3) System Lifecycle Management

MVP's computer server inventory indicates that numerous servers are running unsupported versions of operating systems. Software vendors typically announce projected dates for when they will no longer provide support or distribute security patches for their products (known as end-of-life dates). In order to avoid the risk associated with operating unsupported software, organizations must have a methodology in place to phase out software before it reaches its end-of-life date.

We were told that MVP was aware of these unsupported operating systems but that they are necessary to run certain older applications used within the company. We were also provided evidence that MVP had formally accepted the risk of these outdated systems operating in its network environment. However, we continue to have concerns with MVP's system lifecycle management methodology. Based on the inventory provided to us, almost 10 percent of MVP's servers are running unsupported operating systems and several systems have not been supported for over six years. This high number of unsupported servers causes us to question the effectiveness of the risk assessments that MVP performed.

NIST SP 800-53, Revision 4, recommends that 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 system software leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 8

We recommend that MVP update and/or enforce its system lifecycle methodology to ensure that information systems are [redacted]

MVP Response:

"MVP has implemented the following processes to improve our System Lifecycle methodology: [redacted]

4) Authenticated Vulnerability Scans

MVP's documented vulnerability scanning methodology requires vulnerability scans to be run against all systems on a monthly basis. We were told that MVP performs vulnerability scans using valid credentials on all hosts. However, we determined that MVP does not perform authenticated scans on user workstations or on four operating platforms used in the MVP environment. Note – the names of the four specific operating platforms were disclosed in the draft audit report, but will not be included in this final report.

MVP does not perform credentialed vulnerability scanning on all hosts.

NIST SP 800-53, Revision 4, states that administrative credentials should be used for automated vulnerability scans so that the scanning tool can access all necessary information, and therefore run a more thorough vulnerability scan. Failure to perform authenticated scans increases the risk that undetected vulnerabilities may exist on systems.

Recommendation 9

We recommend that MVP perform authenticated vulnerability scans on its entire network inventory.

MVP Response:

"MVP has begun to extend authenticated vulnerability scans to other operating systems. [Operating platform 1] and Workstation authenticated scans have been implemented as of March 2017. Please see Appendix 9. [Operating platform 2, 3, and 4] authenticated scans will be implemented in May 2017."

OIG Comment:

The evidence provided by MVP in response to the draft audit report indicates that the Plan has made progress extending its vulnerability scanning program. We recommend that MVP provide OPM's Healthcare and Insurance Audit Resolution Group with evidence that it has fully implemented the recommendation and performs authenticated vulnerability scans on its entire network environment.

5) OIG Vulnerability Scanning

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in MVP's network environment. The specific vulnerabilities that we identified were provided to MVP in the form of an audit inquiry, but will not be detailed in this report. Our scans detected MVP systems that were missing operating system and third party patches that were older than the grace period allowed by MVP's patching policy. MVP acknowledged that they were aware of most of the vulnerabilities that we identified and have remediation plans in place.

NIST SP 800-53, Revision 4, states that organizations 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 hackers could exploit system weaknesses for malicious purposes.

Recommendation 10

We recommend that MVP remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided to MVP.

MVP Response:

"MVP has remediated the majority of the specific vulnerabilities outlined in the OIG scan results. We will continue to investigate and evaluate remediation for any remaining issues."

6) Network Access Controls

MVP does not have controls in place to prevent non-authorized devices (e.g., personal equipment) from connecting to its internal network.

NIST 800-53, Revision 4, states that an information system should uniquely identify and authenticate devices before establishing a network connection. Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

Recommendation 11

We recommend that MVP implement network access controls to prevent non-authorized devices from connecting to its internal network.

MVP Response:

"MVP will evaluate implementation of a network access control (NAC) solution next year. Consideration on network impact, processes, and budget will be key factors in the decision."

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

- Documented configuration management policy; and
- Documented system change control process.

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

1) Security Configuration Standards

MVP has not documented formal security configuration standards for its computer server operating systems. A security configuration standard is a formally approved document that contains details on how security settings should be configured for specific operating platforms.

MVP does not maintain documented security configuration standards.

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, states that an organization must develop, document, and maintain a current baseline configuration of the information system. Failure to establish approved system configuration settings increases the risk that systems may not be configured in a secure manner.

Recommendation 12

We recommend that MVP document approved security configuration settings for all operating platforms deployed in its technical environment.

MVP Response:

"MVP will be publishing Security Standards documents for all operating platforms by May 2017."

2) Security Configuration Auditing

As noted above, MVP does not maintain approved security configuration standards for its operating platforms, and therefore it cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings).

MVP has a scanning tool in place that is currently used for vulnerability scanning. We were told that MVP intends to use the tool for compliance scanning in the future. Documenting security configuration settings and using the tool to conduct compliance audits will help ensure that MVP servers are appropriately configured.

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 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 13

We recommend that MVP implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 11 are in place.

MVP Response:

"MVP will be implementing a process to perform Policy Compliance scans on Production servers on a routine basis based on the Standards created from Recommendation 12. The process will be implemented after the standards documents are published."

E. CONTINGENCY PLANNING

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

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." MVP has identified and prioritized the systems and resources that are critical to business operations, and have developed detailed procedures to recover those systems and resources.

The following sections describe areas for improvement related to MVP's contingency planning controls.

1) Business Continuity Plan Testing

MVP performs routine disaster recovery testing to recover its critical infrastructure. However, MVP does not perform business continuity plan testing on a routine basis to determine the effectiveness of the plan and the organizational readiness to execute the plan.

NIST SP 800-34, Revision 1, states that contingency plan testing "helps to evaluate the viability of plan procedures, determine the ability of recovery staff to implement the plan, and identify deficiencies in the plan. Testing should occur [at least annually] and when significant changes are made to the [IT] system, supported business process(s), or the [IT contingency plan]." NIST SP 800-53, Revision 4, states that the organization must review the contingency plan test results and initiate corrective action.

Failure to test the business continuity plan increases the risk that MVP will not be able to continue business operations if unexpected events occur.

Recommendation 14

We recommend that MVP routinely test its business continuity plan, document the results, and use the results to update and improve the business continuity plan.

MVP Response:

"MVP has implemented an annual Business Unit Continuity Plan review and sign-off process. All critical Business Units will have reviewed, validated, and updated continuity plans for their areas by the end of 2017."

2) Backup Data Protection

MVP performs full application and data backups to tape media on a [redacted] basis. Backups are [redacted]. Although the backup tapes are encrypted, the keys to unencrypt the data are stored alongside the tapes during transport to the offsite storage facility.

NIST SP 800-34, Revision 1, states that "A solid key management process must be established so encrypted data is available as needed. Keying material, which is the data used to establish and maintain the keys, needs to be managed, ideally at a central location in the organization. These keys should be stored separate from, but accessible to, the primary encrypted backup data." Failure to store the encryption keys separately from the encrypted tape backups increases the risk of unauthorized disclosure of confidential data.

Recommendation 15

We recommend that MVP implement a process to ensure that encryption keys for tape backups are stored separately from the backup tapes.

MVP Response:

"MVP is currently evaluating alternative solutions to replace the current backup and recovery process. As part of that effort, security of the data and storage of the encryption keys will be addressed."

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting MVP's claims adjudication process. MVP prices and adjudicates claims using a commercially available claims processing application called [redacted]. We reviewed the following processes related to the claims adjudication process: application configuration management, claims processing, member enrollment, and provider debarment.

1) Application Configuration Management

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

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

- Policies and procedures that allow modifications to be tracked throughout the change process;

- Unit, integration, and quality assurance testing are conducted in accordance with industry standards; and

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

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

2) Claims Processing System

We evaluated the input, processing, and output controls associated with MVP's claims processing system. We determined that MVP has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail processing facilities are tracked to ensure timely processing;

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

- Claims scheduled for payment are actually paid.

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

3) Enrollment

We evaluated MVP's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and is manually entered into their claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

Nothing came to our attention to indicate that MVP has not implemented adequate controls over the enrollment process.

4) Debarment

MVP has documented procedures for reviewing provider files for debarments and suspensions. MVP Data Analysts within the Credentialing Department download the OPM OIG debarment list monthly and compare it to the provider information system. If a match is confirmed, a flag is then added in the claims system that will suspend any claim submitted by the debarred provider. Claims submitted by a debarred provider adjudicate through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial.

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

APPENDIX

MVP HEALTH CARE
625 State Street, PO Box 2207
Schenectady, NY 12301-2207
mvphealthcare.com

April 07, 2017

Via E-mail

[redacted]
Senior Team Leader
Information Systems Audits Group
U.S Office of Personnel Management
Washington, DC 20415

RE: Draft Audit Report, Audit of Information Systems General and Application Controls at MVP Health Care – Report Number 1C-GA-00-17-010, dated February 15, 2017

Dear Mr. [redacted]:

The following is in response to the draft audit report, dated February 15, 2017, detailing the results of the information technology audit of MVP Health Plan, Inc. (MVP) that was performed by the U.S. Office of Personnel Management (OPM) of the Inspector General. The responses to the specific recommendations contained in the Draft Report are set forth below.

SUMMARY OF RECOMMENDATIONS

B. Access Level Controls

Recommendation 1: We [redacted]

MVP RESPONSE: Privileged user [redacted]. Consideration of network impact, processes, and budget will be key factors in the decision. In the interim, MVP will continue to monitor and alert on log activity of privileged users through our security event and information management system.

Recommendation 2: We recommend that MVP develop policies and procedures to ensure that access to information systems is granted with proper segregation of duties.

MVP RESPONSE: MVP plans to document segregation of duties controls currently in place that are tested on regular basis as part of ongoing audits associated with key business controls. MVP will also evaluate the feasibility of adding segregation of duties controls within its account management and user recertification processes.

Recommendation 3: We recommend that MVP improve its physical access authorization review to include controls to detect duplicate badges.

MVP RESPONSE: MVP will include controls to detect duplicate badges in the ongoing monthly audits over the physical access system.

Recommendation 4: We recommend that MVP implement multi-factor authentication and piggybacking prevention controls at its primary data center.

MVP RESPONSE: MVP is evaluating the implementation of a new building security system. The implementation of a new building security system would include requirements for providing multi-factor authentication for entry into the data center. In the interim, MVP's data center access is limited to a small number of authorized personnel and reviews of access are performed on a quarterly basis. The data center also has 24/7 closed circuit cameras to monitor the points of entry.

C. Network Security

Recommendation 5: We recommend that MVP document and approve a firewall policy and/or configuration standard.

MVP RESPONSE: MVP Health Care has implemented an approved Firewall Standards document as of March 2017. Please see Appendix 5.

Recommendation 6: We recommend that MVP perform routine audits of its current firewall configuration against an approved firewall policy that is customized to its technical environment. Note – this recommendation cannot be implemented until the controls from Recommendation 5 are in place.

MVP RESPONSE: MVP will be implementing a firewall configuration audit process by which external open ports and firewall policy are reviewed on a routine basis.

Recommendation 7: We recommend that MVP improve its patch management methodology to ensure that workstation patches are applied in a timely manner.

MVP RESPONSE: MVP has implemented authenticated scanning on a subset of workstations in order to help prioritize patching and ensure timely remediation. The subset of workstations acts as a representative of the entire enterprise, as it is a cross-section of our workstation landscape. The

workstations scans have been rolled into our routine vulnerability scanning schedule as of March 2017. Please see Appendix 7.

Recommendation 8: We recommend that MVP update and/or enforce it systems lifecycle methodology to ensure that information systems are [redacted]

MVP RESPONSE: MVP has implemented the following processes to improve our System Lifecycle methodology: [redacted].

Recommendation 9: We recommend that MVP perform authenticated vulnerability scans on its entire network inventory.

MVP RESPONSE: MVP has begun to extend authenticated vulnerability scans to other operating systems. [Operating platform 1] and Workstation authenticated scans have been implemented as of March 2017. Please see Appendix 9. [Operating platform 2, 3, and 4] authenticated scans will be implemented in May 2017.

Recommendation 10: We recommend that MVP remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided to MVP.

MVP RESPONSE: MVP has remediated the majority of the specific vulnerabilities outlined in the OIG scan results. We will continue to investigate and evaluate remediation for any remaining issues.

Recommendation 11: We recommend that MVP implement network access controls to prevent non-authorized devices from connecting to its internal network.

MVP RESPONSE: MVP will evaluate implementation of a network access control (NAC) solution next year. Consideration on network impact, processes, and budget will be key factors in the decision.

D. Configuration Management

Recommendation 12: We recommend that MVP document approved security configuration settings for all operating platforms deployed in its technical environment.

MVP RESPONSE: MVP will be publishing Security Standards documents for all operating platforms by May 2017.

Recommendation 13: We recommend that MVP implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 12 are in place.

MVP RESPONSE: MVP will be implementing a process to perform Policy Compliance scans on Production servers on a routine basis based on the Standards created from Recommendation 12. The process will be implemented after the standards documents are published.

E. Contingency Planning

Recommendation 14: We recommend that MVP routinely test its business continuity plan, document the results, and use the results to update and improve the business continuity plan.

MVP RESPONSE: MVP has implemented an annual Business Unit Continuity Plan review and sign-off process. All critical Business Units will have reviewed, validated, and updated continuity plans for their areas by the end of 2017.

Recommendation 15: We recommend that MVP implement a process to ensure that encryption keys for tape backups are stored separately from the backup tapes.

MVP RESPONSE: MVP is currently evaluating alternative solutions to replace the current backup and recovery process. As part of that effort, security of the data and storage of the encryption keys will be addressed.

Please contact me at (518) 386-[redacted] if you would like to discuss the action that management has taken or plans to take to comply with the recommendations contained in the Draft Report.

Very truly yours,

Peter Molloy
Director, Account Management
MVP Health Care

Cc: James Poole, VP and CIO/CISO Information and Technology
Augusta Martin, VP Client Engagement

Mathew Wendel, Director IT Controls and Assurance
Rico Viscusi, Director Internal Audit
Dan Murphy, Internal Audit

Report No. 1C-GA-00-17-010

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

Report No. 1C-GA-00-17-010