Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

WEAKNESSES IN MOLINA MEDICAID SOLUTIONS' INFORMATION SYSTEM GENERAL CONTROLS OVER IDAHO'S MEDICAID CLAIMS PROCESSING SYSTEM INCREASE VULNERABILITIES

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Thomas M. Salmon
Assistant Inspector General
for Audit Services

July 2014
A-09-13-03001

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

Idaho did not ensure that its contractor Molina Medicaid Solutions implemented adequate information system general controls over Idaho's Medicaid Management Information System. We identified 21 reportable weaknesses in access controls, configuration management, and security management.

WHY WE DID THIS REVIEW

The U.S. Department of Health and Human Services (HHS) oversees States' use of various Federal programs, including Medicaid. State agencies are required to establish appropriate computer system security requirements and conduct biennial reviews of computer system security used in the administration of State plans for Medicaid and other Federal entitlement benefits. This review is one of a number of HHS Office of Inspector General (OIG) reviews of States' computer systems used to administer HHS-funded programs.

In a prior OIG audit, we reviewed the security of the Idaho Department of Health and Welfare's (State agency) Medicaid network. As part of the State agency's overall administration of the Medicaid claims processing system, the State agency contracted with Molina Medicaid Solutions (Molina) to operate its Medicaid Management Information System (MMIS). This review focused solely on Molina's information system general controls over the State agency's MMIS.

Our objective was to determine whether the State agency ensured that Molina implemented adequate information system general controls over the State agency's MMIS.

BACKGROUND

The State agency administers the Medicaid program. During fiscal year 2013, the State agency provided Medicaid services to more than 235,000 Medicaid beneficiaries, totaling approximately $1.8 billion in expenditures.

The State agency's MMIS processes Medicaid claims and manages sensitive claims data, such as beneficiary names and Social Security numbers. The State agency uses the State's computer and telecommunications facility to connect to Molina's Boise, Idaho, facility, which provides access to the MMIS computers located at Molina's New Mexico Data Center in Albuquerque, New Mexico.

To accomplish our objective, we reviewed policies and procedures, interviewed staff, and reviewed supporting documentation. Also, we used audit software-scanning programs to determine whether selected network devices and the Medicaid claims database had security-related vulnerabilities.

WHAT WE FOUND

The State agency did not ensure that Molina implemented adequate information system general controls over the State agency's MMIS. Specifically, we identified 21 reportable weaknesses, which we consolidated into 6 findings and grouped into the following categories: access controls, configuration management, and security management.

- **Access controls.** Molina had inadequate logical access security controls, including weak user authentication for remote network access, an inadequate password history policy, and inadequate encryption of network passwords.

- **Configuration management.** Molina had inadequate security settings for network devices, such as allowing the use of insecure network protocols (the language of rules and conventions for communication between network devices) and the use of network services (functions that help networks to operate more efficiently) that were not necessary for Molina's network, and inadequate management of the Medicaid claims database. In addition, Molina did not have written policies for its patch management program.

- **Security management.** Molina had no security control policies and procedures to periodically review and account for inventory of portable devices. In addition, Molina had (1) no policies and procedures for annual security awareness training and (2) inadequate policies and procedures for terminated and transferred employees and for background checks of employees.

We ranked each of the findings as high impact.

Although we did not find evidence that the weaknesses had been exploited, exploitation could result in unauthorized access to, and disclosure of, sensitive information, as well as disruption of critical operations to the Medicaid program. As a result, we believe that the weaknesses are collectively and, in some cases, individually significant and could potentially compromise the integrity of the Medicaid program. In addition, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to obtain access to commit fraud, waste, or abuse or launch attacks against other computer systems and networks.

WHAT WE RECOMMEND

We recommend that the State agency ensure that Molina implements adequate information system general controls over the State agency's MMIS. Specifically, we recommend that the State agency ensure that Molina:

- implements stronger user authentication for remote network access, strengthens its password history policy, and uses a secure method to store its encrypted network passwords;

- implements secure configuration settings for its network devices;

- implements policies and procedures to secure its Medicaid claims database;

- implements policies for its patch management program;

- implements policies and procedures to periodically review and account for inventory of all portable devices and identify the custodian of those devices; and

- implements (1) policies and procedures for annual security awareness training and (2) adequate policies and procedures for terminated and transferred employees and for background checks of employees.

STATE AGENCY COMMENTS AND OUR RESPONSE

In written comments on our draft report, the State agency concurred with all of our recommendations except for parts of two recommendations. Specifically, the State agency did not concur with parts of our first and sixth recommendations, respectively, that it ensure that Molina implements adequate user authentication for remote network access and implements adequate policies and procedures for terminated and transferred employees. The State agency provided information on actions that it had taken or planned to take to address the recommendations with which it concurred.

After reviewing the State agency's comments, we revised our first recommendation to indicate that the State agency ensure that Molina implements stronger user authentication for remote network access in accordance with Federal guidance. Nothing in the State agency's comments caused us to revise our sixth recommendation.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

The U.S. Department of Health and Human Services (HHS) oversees States' use of various Federal programs, including Medicaid. State agencies are required to establish appropriate computer system security requirements and conduct biennial reviews of computer system security used in the administration of State plans for Medicaid and other Federal entitlement benefits. This review is one of a number of HHS Office of Inspector General (OIG) reviews of States' computer systems used to administer HHS-funded programs.

In a prior OIG audit, we reviewed the security of the Idaho Department of Health and Welfare's (State agency) Medicaid network.[1] As part of the State agency's overall administration of the Medicaid claims processing system, the State agency contracted with Molina Medicaid Solutions (Molina)[2] to operate its Medicaid Management Information System (MMIS). This review focused solely on Molina's information system general controls over the State agency's MMIS.

OBJECTIVE

Our objective was to determine whether the State agency ensured that Molina implemented adequate information system general controls over the State agency's MMIS.

BACKGROUND

Federal Oversight of States' Computer Systems

Federal regulations require State agencies to determine appropriate computer system security requirements based on recognized industry standards or standards governing security of Federal computer systems and information processing (45 CFR part 95). In addition, these regulations require HHS to conduct periodic onsite reviews of State and local agencies to determine the adequacy of computer methods and practices and to ensure that computer equipment and services are used for purposes consistent with proper administration under the Social Security Act.

Idaho Medicaid Program

The State agency administers the Medicaid program. During fiscal year 2013, the State agency provided Medicaid services to more than 235,000 Medicaid beneficiaries, totaling approximately $1.8 billion in expenditures.

---

[1] *Weaknesses in Idaho's Information System General Controls Over Its Medicaid Claims Processing System Increase Vulnerabilities* (A-09-12-03009), issued March 21, 2014.

[2] Molina is a wholly owned subsidiary of Molina Health Systems and provides business processing and information technology administrative services to State Medicaid agencies. As of June 25, 2014, Molina had contracts with Idaho and four other States.

The State agency's MMIS processes Medicaid claims and manages sensitive claims data, such as beneficiary names and Social Security numbers. The State agency uses the State's computer and telecommunications facility to connect to Molina's Boise, Idaho, facility, which provides access to the MMIS computers located at Molina's New Mexico Data Center in Albuquerque, New Mexico.

Information System General Controls

Information system general controls include policies and procedures that apply to an entity's overall computer operations. Some primary objectives of general controls are to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued operations in case of unexpected interruptions.

The Medicaid program depends on general controls, which are critical to ensuring the confidentiality, integrity, and availability of critical information and information systems. In addition, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to obtain access to commit fraud, waste, or abuse or launch attacks against other computer systems and networks.[3]

HOW WE CONDUCTED THIS REVIEW

We reviewed Molina's information system general controls over the State agency's MMIS. To accomplish our objective, we used appropriate procedures from the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM), which provides guidance on evaluating general controls over computer-processed data from information systems. We reviewed policies and procedures, interviewed staff, and reviewed supporting documentation. To perform our tests, we used audit software-scanning programs to identify potential security-related configuration vulnerabilities on two types of network devices and the Medicaid claims database.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A describes our audit scope and methodology.

[3] Fraud represents intentional acts of deception with knowledge that the action or representation could result in an inappropriate gain. Waste includes inaccurate payments for services, such as unintentional duplicate payments. Abuse represents actions inconsistent with acceptable business or medical practices.

FINDINGS

The State agency did not ensure that Molina implemented adequate information system general controls over the State agency's MMIS. Specifically, we identified 21 reportable weaknesses, which we consolidated into 6 findings and grouped into the following categories: access controls, configuration management, and security management.

- **Access controls.** Molina had inadequate logical access security controls, including weak user authentication for remote network access, an inadequate password history policy, and inadequate encryption of network passwords.

- **Configuration management.** Molina had inadequate security settings for network devices, such as allowing the use of insecure network protocols (the language of rules and conventions for communication between network devices) and the use of network services (functions that help networks to operate more efficiently) that were not necessary for Molina's network, and inadequate management of the Medicaid claims database. In addition, Molina did not have written policies for its patch management program.

- **Security management.** Molina had no security control policies and procedures to periodically review and account for inventory of portable devices. In addition, Molina had (1) no policies and procedures for annual security awareness training and (2) inadequate policies and procedures for terminated and transferred employees and for background checks of employees.

We ranked each of the findings as high impact.

Although we did not find evidence that the weaknesses had been exploited, exploitation could result in unauthorized access to, and disclosure of, sensitive information, as well as disruption of critical operations to the Medicaid program. As a result, we believe that the weaknesses are collectively and, in some cases, individually significant and could potentially compromise the integrity of the Medicaid program. In addition, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to obtain access to commit fraud, waste, or abuse or launch attacks against other computer systems and networks.

FEDERAL REQUIREMENTS

Federal requirements from the Health Insurance Portability and Accountability Act (HIPAA) Security Rule for access management appear in 45 CFR part 164. For additional requirements, we used Office of Management and Budget (OMB) Circular No. A-130, Appendix III; Federal Information Processing Standards Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*; National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*; NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*; and NIST Special Publication 800-53, Revision 3, *Security and Privacy Controls for Federal Information Systems and Organizations.*

See Appendix B for specific provisions and citations.

MOLINA HAD INADEQUATE ACCESS CONTROLS

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from loss, disclosure, and unauthorized modification. Such controls include both logical and physical controls:

- Logical access controls require users to authenticate themselves (by using passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute.

- Physical access controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment.

In assessing Molina's access controls, we identified weaknesses in its logical access security controls. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service.

Inadequate Logical Access Security Controls

Molina had not implemented adequate logical access security controls. Specifically, we noted the following:

- Molina had weak user authentication for remote network access.[4]

- Molina had an inadequate policy for the password history setting to secure its network.[5]

- Molina did not store its encrypted passwords on its network server using a secure method.

Molina officials stated that they considered their user authentication procedures and password settings secure and compliant with HIPAA requirements and established industry practices. Molina officials also stated that they would store their encrypted passwords using a secure method.

Without strong logical access security controls, there is an increased risk of unauthorized access to sensitive computer systems and data.

[4] Authentication is a process that confirms a user's identity before he or she can access the network.

[5] Password history determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

MOLINA HAD INADEQUATE CONFIGURATION MANAGEMENT

Configuration management provides reasonable assurance that (1) changes to information system resources, such as the settings of devices on the network,[6] are authorized and (2) systems are configured and operated securely and as intended. Configuration management policies and procedures should be developed, documented, and implemented at the entitywide, system (hardware), and application (software) levels to ensure the security of the system.

In assessing Molina's configuration management, we identified weaknesses in its security settings for network devices, its database security controls, and its patch management policies. Weaknesses in these elements increase the risk that network devices are not configured properly and securely; a secure configuration includes appropriate patching levels, disabling of unnecessary services, and protection against viruses and worms.

Inadequate Security Settings for Network Devices

Molina did not adequately configure secure settings for its network devices. We judgmentally selected two types of network devices (three switches and one firewall) for testing and used an audit software-scanning program that queries and extracts information from the devices to identify settings with potential security-related configuration vulnerabilities. We identified a total of nine weaknesses in this area: five related to switches and four related to switches and the firewall. For example, Molina allowed the use of insecure network protocols[7] to manage network devices and did not adequately protect logging information on some of its network devices.

Molina officials agreed to review device configurations and remove potential security-related configuration vulnerabilities.

Because Molina's network devices are integral to ensuring the security of the State agency's MMIS, failure to adequately secure the devices exposes the network and its resources to attacks on the confidentiality, integrity, and availability of sensitive information, such as electronic protected health information (ePHI). Such information includes names, addresses, birth dates, Social Security numbers, and medical information.

Inadequate Database Security Controls

Molina did not adequately secure its Medicaid claims database. Specifically, we noted the following:

- Molina did not have written policies and procedures for database management.

[6] Devices used to secure networks include (1) switches that forward information among segments of a network, (2) firewalls that prevent unauthorized access to or from a network, and (3) routers that filter and forward data along the network.

[7] Network protocols define a language of rules and conventions for communication between network devices.

- Molina did not regularly review database logs to ensure the integrity and security of system access, system configurations, and access to ePHI.

- Molina did not adequately encrypt its Medicaid claims database.

- Molina did not properly configure access to the Medicaid claims database. We used an audit software-scanning program that queries and extracts information from the database to identify potential security-related configuration vulnerabilities. We identified some Molina database users and groups that had more privileges than were necessary for their job functions.

Molina officials stated that they are developing policies and procedures for database management, reviewing database logs when necessary, and testing a new database encryption technology. Molina officials also stated that some database users were given excess privileges on the database when it was built and that the privileges were not later removed.

Because the security of Molina's Medicaid claims database is essential to protecting sensitive claims data, inadequate security controls expose the database to attacks on the confidentiality, integrity, and availability of ePHI:

- Without written policies and procedures for database management, there is an increased risk of unauthorized access to sensitive data housed in the database.

- Without regular reviews of database logs, an entity has limited ability to establish accountability, ensure compliance with security policies, and investigate violations.

- Without adequate database encryption, there is an increased risk of unauthorized users getting access to, and possibly altering, the contents of sensitive Medicaid data, such as ePHI, including names, addresses, birth dates, Social Security numbers, and medical information.

- Without proper database access configurations, users and groups that have more privileges than necessary may be able to obtain unauthorized access to sensitive data housed in the database.

No Patch Management Policies

Molina did not have written policies for its patch management program.[8] However, Molina had adequate procedures to test and deploy patches.

Molina officials stated that they had identified a gap in their policies and are developing a formal patch management policy based on their current procedures.

[8] A patch is a piece of software designed to fix problems in or update a computer program.

Without adequate patch management policies to address software vulnerabilities, an entity cannot be sure that patches have been effectively applied and that there are not any configuration discrepancies, which could allow an attacker to gain unauthorized access to sensitive information, such as ePHI.

MOLINA HAD INADEQUATE SECURITY MANAGEMENT

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection on senior management's commitment to addressing security risks.

In assessing Molina's entitywide security program, we identified weaknesses in the following critical elements: (1) documenting and implementing security control policies and procedures and (2) implementing effective security awareness and other security-related personnel policies and procedures. Weaknesses in these elements increase the risk of unauthorized use, disclosure, modification, or loss of sensitive information and information systems supporting the agency's mission.

Inadequate Security Control Policies and Procedures

Molina had not implemented adequate security control policies and procedures. Specifically, we noted that Molina did not have specific inventory policies and procedures for portable devices, such as laptop computers and Universal Serial Bus storage devices, and did not periodically review and account for inventory of these devices. In addition, Molina did not identify the custodian of portable devices.

Molina officials stated that they did not know it was necessary to periodically review the inventory and identify the custodian of portable devices. Molina officials also stated that they believed the software they used to track the connection of devices to the network was sufficient to review and account for portable devices.

Without adequate inventory controls for all portable devices, Molina is at risk of a data breach. Portable devices costing as little as $50 could contain ePHI and be easily lost or stolen, making Molina potentially liable for millions of dollars because of a data breach.[9]

Inadequate Security-Related Personnel Policies and Procedures

Molina had not implemented adequate security-related personnel policies and procedures. Specifically, we noted the following:

- Molina did not have policies and procedures that required its employees to complete general security awareness training annually. We judgmentally selected five Molina employees and found that none of them had completed general security awareness training in over a year.

[9] The Ponemon Institute's report entitled *2013 Cost of Data Breach Study: United States* indicated that the average cost of a data breach for an organization in 2012 was $5.4 million.

- Molina did not have adequate policies and procedures for terminated or transferred employees. We judgmentally selected six terminated employees and one transferred employee and found that Molina had not completed exit documents for any of the seven employees. Exit documents show the steps to be completed when an employee is terminated or transferred, including collecting keys and electronic keycards and notifying network administrators to remove the employee's network access. In addition, Molina's policies and procedures required the completion of exit documents only for employees being terminated, not for those being transferred.

- Molina did not have adequate policies and procedures to ensure that employee background checks were performed. We judgmentally selected 10 employees who had access to ePHI and found that Molina did not have background check documentation for 2 of them.

Molina officials stated that they were not aware that annual refresher training on general security awareness was required. Molina officials agreed that exit documents should be completed for all employees being terminated or transferred; they also stated that exit documents were not completed for terminated employees and were not required to be completed for transferred employees because of an administrative oversight. Molina officials stated that they could not find the background check documentation for two employees.

Without policies and procedures requiring employees to complete general security awareness training annually, there is an increased risk that employees with access to the MMIS may not be appropriately trained to fulfill their security responsibilities.

Without adequate policies and procedures on completion of exit documents, Molina runs the risk of failing to remove transferred and terminated employees' physical and logical access, which could result in unauthorized access to ePHI, compromising of data, or sabotaging of information systems.

Without adequate policies and procedures on performing background checks of employees, an organization runs the risk of hiring unqualified or untrustworthy individuals. In addition, background checks help determine whether an individual is suitable for a given position.

RECOMMENDATIONS

We recommend that the State agency ensure that Molina implements adequate information system general controls over the State agency's MMIS. Specifically, we recommend that the State agency ensure that Molina:

- implements stronger user authentication for remote network access, strengthens its password history policy, and uses a secure method to store its encrypted network passwords;

- implements secure configuration settings for its network devices;

- implements policies and procedures to secure its Medicaid claims database,

- implements policies for its patch management program;

- implements policies and procedures to periodically review and account for inventory of all portable devices and identify the custodian of those devices; and

- implements (1) policies and procedures for annual security awareness training and (2) adequate policies and procedures for terminated and transferred employees and for background checks of employees.

STATE AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, the State agency concurred with all of our recommendations except for parts of two recommendations. Specifically, the State agency did not concur with part of our first recommendation that it ensure that Molina implements adequate user authentication for remote network access, stating that Molina's remote network access is HIPAA-compliant and meets current standards for security and privacy controls. Also, the State agency did not concur with part of our sixth recommendation that it ensure that Molina implements adequate policies and procedures for terminated and transferred employees, stating that Molina uses an electronic ticket system instead of a single paper exit document. The State agency provided information on actions that it had taken or planned to take to address the recommendations with which it concurred.

The State agency's comments are included as Appendix C. We redacted information that we considered to be sensitive.

To help secure ePHI, NIST Special Publication 800-53, Revision 3, recommends using two-factor authentication for network access. Therefore, we revised our first recommendation to indicate that the State agency ensure that Molina implements stronger user authentication for remote network access. Molina's Policy and Procedure No. 5.0, section III, states that an out-processing checklist is to be completed for terminated employees. The State agency did not provide us with paper documents or show us a feature in the electronic ticket system that represented a completed out-processing checklist for any of the terminated or transferred employees that we judgmentally selected. Nothing in the State agency's comments caused us to revise our sixth recommendation.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed Molina's information system general controls over the State agency's MMIS. We did not perform penetration testing or review Molina's overall internal control structure.

We conducted our audit from November 2012 to August 2013. We performed our fieldwork at Molina's facility in Boise, Idaho, and at its New Mexico Data Center in Albuquerque, New Mexico.

METHODOLOGY

To accomplish our objective, we used appropriate procedures from FISCAM, which provides guidance on evaluating general controls over computer-processed data from information systems. We reviewed policies and procedures, interviewed staff, and reviewed supporting documentation. To perform our tests, we used audit software-scanning programs to identify potential security-related configuration vulnerabilities and judgmentally selected two types of network devices and the Medicaid claims database.

To determine the potential impact of each finding, we used information described in FIPS Publication 199, which defines the following three levels of potential impact should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability):

- **low** if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals;

- **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals; and

- **high** if the loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: REQUIREMENTS RELATED TO INFORMATION SYSTEM GENERAL CONTROLS

GENERAL FEDERAL REQUIREMENTS

Federal regulations (45 CFR part 95) require State agencies to determine appropriate computer system security requirements based on recognized industry standards or standards governing security of Federal computer systems and information processing. In addition, these regulations require HHS to conduct periodic onsite reviews of State and local agencies to determine the adequacy of computer methods and practices and to ensure that computer equipment and services are used for purposes consistent with proper administration under the Social Security Act.

Federal requirements from the HIPAA Security Rule for access management appear in 45 CFR part 164.

ACCESS CONTROLS

Federal regulations state that for person and entity authentication, covered entities must "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed" (45 CFR § 164.312(d)).

NIST Special Publication 800-53, Revision 3, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F, section IA-2, states that to enhance controls, the information system should use multifactor authentication for network access to privileged and nonprivileged accounts such that one of the factors is provided by a device separate from the information system being accessed.

Molina's password policies and procedures, as contained in Password Management document IS-80.60, provide general requirements for passwords, including password history.

Microsoft's TechNet document "Enforce password history," under best practices, recommends a password history setting of 24 generations.

Federal regulations (45 CFR § 164.312(a)(1)) state that a covered entity must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

CONFIGURATION MANAGEMENT

Federal regulations state that covered entities must "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network" (45 CFR § 164.312(e)(1)) and also must "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate" (45 CFR § 164.312(e)(2)(ii)).

Molina's password policies and procedures, as contained in Password Management document IS-80.60, provide general requirements for passwords, including network devices.

NIST Special Publication 800-53, Revision 3, section AT-5, recommends that organizations stay up to date with the latest recommended security practices, techniques, and technologies. Current industry best practices include developing and implementing policies and procedures for securing databases.

NIST Special Publication 800-53, Revision 3, Appendix F, section AU-6, states that organizations review and analyze information system audit records. Specifically, the information system provides the capability to centrally review and analyze audit records from multiple components within the system.

Federal regulations state that a covered entity must "[i]mplement a mechanism to encrypt and decrypt electronic protected health information" (45 CFR § 164.312(a)(2)(iv)).

Federal regulations (45 CFR § 164.312(a)(1)) state that a covered entity must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

Federal regulations state that a covered entity must "[i]mplement policies and procedures to protect electronic protected health information from improper alteration or destruction" (45 CFR § 164.312(c)(1)).

NIST Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, section 2.7, states:

> Organizations should deploy vulnerability remediations [patches] to all systems that have the vulnerability, even for those systems that are not at immediate risk of exploitation. … Applying patches to multiple systems is a constant administrative challenge that may seem especially daunting when implementing patches on hundreds or thousands of servers and desktop systems. This task can be made less burdensome with the use of applications that automatically distribute updates to end-user computers.

SECURITY MANAGEMENT

Federal regulations state that a covered entity must "[i]mplement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility" (45 CFR § 164.310(d)(1)).

NIST Special Publication 800-53, Revision 3, section MP-5, states that organizations document activities associated with the transport of information system media and that a custodian of the media should be identified at all times.

OMB Circular No. A-130, Appendix III, section A.3.a.(2)(b), states that training controls ensure that "all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system … and periodic refresher training shall be required for continued access to the system."

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, section 3.3, states that at a minimum the entire workforce should be exposed to awareness material annually.

Federal regulations state that a covered entity must "[i]mplement policies and procedures to protect electronic protected health information from improper alteration or destruction" (45 CFR § 164.312(c)(1)).

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, section 10.2.5.1, states that, because terminations can be expected regularly, a standard set of procedures for outgoing or transferred employees should be put in place. These procedures are part of the standard employee separation process that is in place to ensure that system accounts are removed in a timely manner. The separation process also includes the control of keys; the briefing on the responsibilities for confidentiality and privacy; and several other functions not necessarily related to information security, such as the return of property.

Molina's Policy and Procedure No. 5.0, Termination and/or Separation, section III.B, step 8, states that, for offsite employees, the supervisor/manager completes an out-processing checklist and forwards it to Human Resources. Step 9 states that, for onsite employees, Human Resources completes an out-processing checklist.

OMB Circular No. A-130, Appendix III, section A.3.a.(2)(c), states that background check screening must occur before an individual is authorized to bypass significant technical and operational security controls and periodically thereafter.

APPENDIX C: STATE AGENCY COMMENTS

IDAHO DEPARTMENT OF
HEALTH & WELFARE

C.L. "BUTCH" OTTER – Governor
RICHARD M. ARMSTRONG – Director

PAUL J. LEARY - Administrator
DIVISION OF MEDICAID
Post Office Box 83720
Boise, Idaho 83720-0009
PHONE: (208) 334-5747
FAX: (208) 364-1811

May 12, 2014

Ms. Lori A. Ahlstrand
Regional Inspector General
Office of Audit Services, Region IX
Department of Health and Human Services
90 - 7th Street, Ste 3-650
San Francisco, CA 94103

RE: Report Number A-09-13-03001

Dear Ms. Ahlstrand:

In response to your letter of April 25, 2014, below are the Department's responses to the draft recommendations in Report Number A-09-13-03001, *Weaknesses in Molina Medicaid Solutions' Information System General Controls Over Idaho's Medicaid Claims Processing System Increase Vulnerabilities.*

1. **Report Recommendation:**
   The State agency ensure that Molina (a) implements adequate user authentication for remote network access, (b) strengthens its password history policy, and (c) uses a secure method to store its encrypted network passwords

   Department Response: Do not concur item (a) concur items (b) & (c)

   (a)**We do not concur** because Molina's remote network access is HIPAA compliant and meets current industry standards for security and privacy controls. However, as suggested by the auditor, Molina is currently analyzing the enhancement of their controls by [redacted] which was recently recommended by the National Institute of Standards and Technology (NIST).

   (b) **We concur** with this recommendation. The Department will request that Molina strengthen its password history [redacted] as recommended by the OIG.

   (c) **We concur** with this recommendation. [redacted][10] as recommended by the OIG.

[10] Office of Inspector General Note - The deleted text has been redacted because it is sensitive information.

2. **Report Recommendation:**
   The State agency ensure that Molina implements secure configuration settings for its network devices.

   Department Response: Concur
   Although the OIG [redacted] findings do show vulnerabilities on some network settings, these are considered low impact [redacted][11]. However, Molina's Network team will address this recommendation as part of the upcoming upgrade of their network devices.

3. **Report Recommendation:**
   The State agency ensure that Molina implements policies and procedures to secure its Medicaid claims database

   Department Response: Concur
   Molina's database security policies and procedures were in the process of being documented at the time of the OIG Audit. This document has since been published and is in use.

4. **Report Recommendation:**
   The State agency ensure that Molina implements policies for its patch management program.

   Department Response: Concur
   Molina's patch management policy has been published subsequent to the OIG audit.

5. **Report Recommendation:**
   The State agency ensure that Molina implements policies and procedures to periodically review and account for inventory of all portable devices and identify the custodian of those devices.

   Department Response: Concur
   Molina's Asset Inventory Policy is in the process of being documented and will be published shortly.

6. **Report Recommendation:**
   The State agency ensure that Molina implements (a) policies and procedures for annual security awareness training and (b) adequate policies and procedures for terminated and transferred employees and (c) for background checks of employees.

   Department Response: Concur with items (a) & (c); do not concur item (b)
   (a) **We concur** because the annual requirement was not in place at the time of the auditor's visit. Molina now requires all its employees to take the following security and privacy awareness trainings annually:

[11] Office of Inspector General Note - The deleted text has been redacted because it is sensitive information.

1) [redacted]

2) [redacted].

(b) **We do not concur** because although Molina does not have a single paper exit document, they have an electronic ticket system that performs the same function more effectively. When an employee is terminated, a [redacted] Remote employees cannot [redacted]. Transferring employees do not [redacted].

(c) **We concur** because Molina could not provide the background check documentation. This shortcoming has been brought to the Molina HR department's attention and procedures have since been reinforced to ensure this will not happen in the future.

If you have any questions regarding the Department's responses to these recommendations, please contact [redacted] at [redacted].[12]

Sincerely,

PAUL J. LEARY
Administrator
Division of Medicaid
Department of Health and Welfare

[12]Office of Inspector General Note - The deleted text has been redacted because it is sensitive information.