Department of Health and Human Services

**OFFICE OF INSPECTOR GENERAL**

# WEAKNESSES IN IDAHO'S INFORMATION SYSTEM GENERAL CONTROLS OVER ITS 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](mailto:Public.Affairs@oig.hhs.gov).*


Thomas M. Salmon
Assistant Inspector General



March 2014
A-09-12-03009

# *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 implement adequate information system general controls over its Medicaid claims processing system. We identified 19 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 automatic data processing (ADP) security requirements and conduct biennial reviews of ADP 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 reviews of States' ADP systems used to administer HHS-funded programs.

Our objective was to determine whether the Idaho Department of Health and Welfare (State agency) implemented adequate information system general controls over its Medicaid claims processing system.

### BACKGROUND

The State agency administers the Medicaid program. During fiscal year 2012, the State agency provided Medicaid services to over 225,000 Medicaid beneficiaries, totaling more than $1.6 billion in expenditures.

This review covered the State agency's information system general controls over its Medicaid claims processing system. As part of its overall administration of the Medicaid claims processing system, the State agency contracted with Molina Medicaid Solutions (Molina) to operate the Medicaid Management Information System (MMIS). The 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 access the MMIS; therefore, this review focused on the security of the State agency's network. We will review Molina's information system general controls over the MMIS in a separate audit.

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

### WHAT WE FOUND

The State agency did not implement adequate information system general controls over its Medicaid claims processing system. Specifically, we identified 19 reportable weaknesses, which we consolidated into 5 findings and grouped into the following categories: access controls, configuration management, and security management.

- **Access controls.** The State agency had inadequate logical access security controls, including inadequate password settings for securing its network and inadequate encryption of network passwords. In addition, the State agency had inadequate physical access security controls to restrict access to its computer and telecommunications facility to only individuals who need access to the facility to perform their job duties.

- **Configuration management.** The State agency had inadequate 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 the State agency's network.

- **Security management.** The State agency had inadequate security control policies and procedures, including inadequate policies to verify sanitization of data and disposal of devices and no policies and procedures to periodically review and account for inventory of portable devices. In addition, the State agency had inadequate personnel policies and procedures related to security awareness training, training for employees with significant responsibilities for information security, completion of exit documents for transferred and terminated employees, and 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 implement adequate information system general controls over its Medicaid claims processing system. Specifically, we recommend that the State agency:

- implement adequate logical access security controls to enforce the requirement that passwords not be reused and use a secure method to store its encrypted network passwords;

- implement additional physical access security controls to restrict access to its computer and telecommunications facility to only individuals who need access to the facility to perform their job duties;

- implement secure configuration settings for its network devices;

- strengthen policies and follow existing procedures to verify data sanitization and device disposal and implement policies and procedures to periodically review and account for inventory of all portable devices; and

- implement adequate personnel policies and procedures for general security awareness training, training for employees with significant responsibilities for information security, completion of exit documents for transferred and terminated employees, and background checks of employees, including those hired from providers or contractors.

## STATE AGENCY COMMENTS AND OUR RESPONSE

In written comments on our draft report, the State agency concurred with our finding on inadequate logical access controls and provided information on actions taken to address our first recommendation. The State agency also concurred with our second, fourth, and fifth recommendations and provided information on actions that it had taken or planned to take to address our recommendations.

Regarding our third recommendation, the State agency concurred that modifications may be necessary for the identified weaknesses in settings for network devices and stated that changes to configuration settings were in the process of being made. However, the State agency commented that some changes to these settings were not appropriate and provided one example. After reviewing it, we determined that one of the weaknesses was not reportable and removed it from the final report. However, we did not revise the wording of our third 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 automatic data processing (ADP) security requirements and conduct biennial reviews of ADP 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 reviews of States' ADP systems used to administer HHS-funded programs.

## OBJECTIVE

Our objective was to determine whether the Idaho Department of Health and Welfare (State agency) implemented adequate information system general controls over its Medicaid claims processing system.

## BACKGROUND

### Federal Oversight of States' Automatic Data Processing Systems

Federal regulations require State agencies to determine appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP 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 ADP methods and practices and to ensure that ADP 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 2012, the State agency provided Medicaid services to over 225,000 Medicaid beneficiaries, totaling more than $1.6 billion in expenditures.

This review covered the State agency's information system general controls over its Medicaid claims processing system. As part of its overall administration of the Medicaid claims processing system, the State agency contracted with Molina Medicaid Solutions (Molina) to operate the Medicaid Management Information System (MMIS). The 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 access the MMIS; therefore, this review focused on the security of the State agency's network. We will review Molina's information system general controls over the MMIS in a separate audit.

### 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.[1]

## HOW WE CONDUCTED THIS REVIEW

We reviewed the State agency's information system general controls over its Medicaid claims processing system. 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 an audit software-scanning program and judgmentally selected two types of network devices for testing to identify security-related configuration vulnerabilities.

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.

## FINDINGS

The State agency did not implement adequate information system general controls over its Medicaid claims processing system. Specifically, we identified 19 reportable weaknesses, which we consolidated into 5 findings and grouped into the following categories: access controls, configuration management, and security management.

- **Access controls.** The State agency had inadequate logical access security controls, including inadequate password settings for securing its network and inadequate encryption of network passwords. In addition, the State agency had inadequate physical

[1] 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.

access security controls to restrict access to its computer and telecommunications facility to only individuals who need access to the facility to perform their job duties.

- **Configuration management.** The State agency had inadequate 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 the State agency's network.

- **Security management.** The State agency had inadequate security control policies and procedures, including inadequate policies to verify sanitization of data and disposal of devices and no policies and procedures to periodically review and account for inventory of portable devices. In addition, the State agency had inadequate personnel policies and procedures related to security awareness training, training for employees with significant responsibilities for information security, completion of exit documents for transferred and terminated employees, and 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 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; National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*; and NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

See Appendix B for Federal and other requirements related to information system general controls.

## STATE AGENCY 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 the State agency's access controls, we identified weaknesses in its logical and physical 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**

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

- The State agency had an inadequate password setting for securing its network. Although the State agency's password history policy prohibited password reuse, the State agency did not enforce this requirement on its network password setting.[2]

- The State agency did not store its encrypted passwords on its network server using a secure method.

State agency officials said that their password history setting would be changed to prohibit password reuse and they planned to use a secure method to store encrypted network passwords.

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

**Inadequate Physical Access Security Controls**

The State agency had not implemented adequate physical access security controls to restrict access to its computer and telecommunications facility, which contained equipment that connected to the MMIS. Specifically, we noted that more than 60 individuals, including the Governor, law enforcement, and the fire department, had access to the facility but did not need access to perform their job duties.

A State agency official agreed that too many individuals had access to the computer and telecommunications facility and stated that he believed that State law required certain individuals, such as the Governor, law enforcement, and the fire department, to have access. We asked the official to provide us with the law that required those individuals to have access. The official stated that he asked two other State officials and neither could find such a law.

---

[2] 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.

If access to the computer and telecommunications facility is not restricted to individuals who need access to perform their job duties, there is an increased risk that computer resources and sensitive information, such as electronic protected health information (ePHI), may not be protected from intentional or unintentional loss or damage.

## STATE AGENCY 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,[3] 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.

### Inadequate Settings for Network Devices

The State agency did not adequately configure the security of its network devices. We judgmentally selected two types of network devices (one router and two switches) for testing and used an audit software-scanning program that queries and extracts information from the devices to identify potential security-related configuration vulnerabilities. We identified a total of 10 weaknesses in this area: 5 related to a router, 3 related to a switch, and 2 related to both. For example, the State agency allowed the use of insecure network protocols[4] to manage network devices. In addition, the State agency did not restrict services on network devices, such as Maintenance Operations Protocol used to connect to remote systems, which were not necessary for the State agency's network. Manufacturers configure devices with default settings that are not needed for every network.

State agency officials said that the devices had been configured a long time ago and had not been updated.

Because the State agency's network devices are integral to ensuring the security of the claims processing system, 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 ePHI. Such information includes names, addresses, birth dates, Social Security numbers, and medical information.

## STATE AGENCY 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.

[3] Devices used to secure networks include (1) routers that filter and forward data along the network and (2) switches that forward information among segments of a network.

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

In assessing the State agency'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**

The State agency had not implemented adequate security control policies and procedures. Specifically, we noted the following:

- The State agency did not have adequate policies to verify sanitization of data[5] and disposal of devices, such as hard drives. Also, the State agency did not follow its procedures to:
    - document that data could not be recovered from sanitized devices,
    - identify the method used to remove data from discarded devices,
    - obtain the name and signature of the supervisor responsible for data sanitization, and
    - identify the disposal method for devices.

- The State agency did not have specific inventory policies and procedures for portable devices, such as laptop computers and Universal Serial Bus storage devices, and did not account for these devices.

State agency officials stated that they were in the process of approving a policy to verify that data could not be recovered from sanitized equipment and discarded devices. State agency officials were not aware that the contractor was not following procedures to sanitize State data on devices and to dispose of devices.

State agency officials stated that there were general inventory policies and procedures for items costing more than $2,000. However, State agency officials had not yet developed and implemented standard agencywide policies and procedures to inventory portable devices costing less than $2,000.

Without adequate policies and procedures for verifying data sanitization and device disposal, the State agency cannot ensure that State data are properly sanitized and devices are properly disposed of.

Without adequate inventory controls for all portable devices, the State agency is at risk of a data breach. Portable devices costing as little as $50 could contain ePHI and be easily lost or stolen, making the State potentially liable for millions of dollars because of a data breach.[6]

---

[5] Sanitization is the process of deliberately and irreversibly removing or destroying data on a device.

[6] 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.

## Inadequate Personnel Policies and Procedures

The State agency had not implemented adequate personnel policies and procedures. Specifically, we noted the following:

- The State agency did not provide periodic refresher training on general security awareness to employees with access to the MMIS. The State agency provided security awareness training only to new employees.

- The State agency did not have policies to ensure that all employees with significant responsibilities for information security obtain training in their security responsibilities. We judgmentally selected five employees and found that while all five had received training within the last year, one of those five had not received any training in the prior 20 years.

- The State agency did not have policies to ensure that exit documents were completed for all transferred and terminated employees. We judgmentally selected five terminated employees and found that the State agency did not have exit documents for three of them. Exit documents show the steps to be completed when an employee is transferred or terminated, including collecting keys and electronic keycards and notifying network administrators to remove the employee's network access.

- The State agency did not have adequate policies for background checks of employees who had access to ePHI. We judgmentally selected 10 employees who had access to ePHI and found that the State agency did not perform background checks for 3 employees and did not have adequate documentation for 1 employee.

State agency officials stated that they were not aware that periodic refresher training on general security awareness was required. Although State agency officials stated that employees with significant responsibilities received training, there were no policies requiring it. State agency officials stated that individual units within the State agency did not always document completion of termination procedures.

State agency officials stated that they recruited individuals from providers and contractors that had worked with the State agency. Because the officials were already familiar with these individuals, they did not perform background checks.

Without adequate policies and procedures on training, there is an increased risk that employees with access to the MMIS may not be appropriately trained to fulfill their security responsibilities. In addition, employees with significant responsibilities for information security may not be able to remain up to date with the latest information and tools to help protect sensitive information.

Without adequate policies and procedures on completion of exit documents, the State agency 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, including individuals whom an organization is already familiar with, 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:

- implement adequate logical access security controls to enforce the requirement that passwords not be reused and use a secure method to store its encrypted network passwords;

- implement additional physical access security controls to restrict access to its computer and telecommunications facility to only individuals who need access to the facility to perform their job duties;

- implement secure configuration settings for its network devices;

- strengthen policies and follow existing procedures to verify data sanitization and device disposal and implement policies and procedures to periodically review and account for inventory of all portable devices; and

- implement adequate personnel policies and procedures for general security awareness training, training for employees with significant responsibilities for information security, completion of exit documents for transferred and terminated employees, and background checks of employees, including those hired from providers or contractors.

## STATE AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, the State agency concurred with our finding on inadequate logical access controls and provided information on actions taken to address our first recommendation. The State agency also concurred with our second, fourth, and fifth recommendations and provided information on actions that it had taken or planned to take to address our recommendations.

Regarding our third recommendation, the State agency concurred that modifications may be necessary for the identified weaknesses in settings for network devices and stated that changes to configuration settings were in the process of being made. However, the State agency commented that some changes to these settings were not appropriate and provided one example. After reviewing it, we determined that one of the weaknesses was not reportable and removed it from the final report. However, we did not revise the wording of our third recommendation.

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

# APPENDIX A: AUDIT SCOPE AND METHODOLOGY

## SCOPE

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

We conducted our audit from September 2012 to January 2013. We performed our fieldwork at the State agency's office in Boise, Idaho.

## 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 an audit software-scanning program and judgmentally selected two types of network devices for testing to identify security-related configuration vulnerabilities.

To determine the potential impact of each finding, we used information described in Federal Information Processing Standards 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 ADP security requirements based on recognized industry standards or standards governing security of Federal ADP 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 ADP methods and practices and to ensure that ADP equipment and services are used for purposes consistent with proper administration under the Social Security Act.

Federal requirements from the Health Insurance Portability and Accountability Act Security Rule for access management appear in 45 CFR part 164.

### ACCESS CONTROLS

Microsoft policies and procedures, as contained in the *Windows XP Security Guide,* provide recommendations for passwords.

The State agency's password policy, Policy Memorandum No. 05-06, section 4.2, states that passwords are not to be reused.

Federal regulations state that a covered entity must implement procedures to control and validate a person's access to facilities based on their role or function (45 CFR § 164.310(a)(2)(iii)).

### 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)).

### SECURITY MANAGEMENT

NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, section MP-6, states that the organization must track, document, and verify media sanitization and disposal actions.

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, Appendix F, section CM-8, recommends that the organization develop, document, and maintain an inventory of information system components that includes information deemed necessary to achieve effective property accountability. In addition, section CM-8 states that information necessary to achieve property accountability can include hardware inventory specifications, such as manufacturer, model, serial number, and component owner.

OMB Circular No. A-130, Appendix III, section A.3.a.2.b, indicates that individuals are to be appropriately trained in how to fulfill their security responsibilities before allowing them access to the system, and periodic refresher training is required for continued access to the system.

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, section 1.5.2, states that chief information officers should work with the agency information-technology (IT) security program manager to ensure that agency personnel with significant security responsibilities obtain sufficient training in their security responsibilities. Section 1.5 explains that one way to help ensure that an IT security program matures is to develop and document in policy the training responsibilities for those key positions on which the success of the program depends.

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.

OMB Circular No. A-130, Appendix III, section A.3.a.2.c, indicates 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

December 12, 2013

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-90-12-03009

Dear Ms. Ahlstrand:

In response to the draft findings detailed in Report Number A-09-12-03009, please find the Department's responses below.

**OIG Finding: Inadequate Logical Access Security Controls-** The State agency had an inadequate password setting for securing its network. Although the State agency's password history policy prohibited password reuse, the State agency did not enforce this requirement on its network password setting.

**OIG Recommendation:** Implement adequate logical access security controls to enforce the requirement that passwords not be reused and use a secure method to store its encrypted network passwords.

**State Response:** We concur with the finding and have implemented the OIG's recommendations regarding enforcement of password history, minimum and maximum age, length and complexity requirements.

**OIG Finding: Inadequate Logical Access Security Controls-** The State agency did not store its encrypted passwords on its network server using a secure method.

**OIG Recommendation:** Use a secure method to store its encrypted network passwords.

**State Response:** We concur with the finding and have implemented the OIG's recommendation to discontinue [redacted] [7]

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

**OIG Finding: Inadequate Physical Access Security Controls-** The State agency had not implemented adequate physical access security controls to restrict access to its computer and telecommunications facility, which contained equipment that connected to the MMIS. Specifically, we noted that more than 60 individuals, including the Governor, law enforcement, and the fire department, had access to the facility but did not need access to perform their job duties.

**OIG Recommendation:** Implement additional physical access security controls to restrict access to its computer and telecommunications facility to only individuals who need access to the facility to perform their job duties.

**State Response:** We concur with this specific recommendation. The Department is in the process of working with our building security team to restrict access to the computer and telecommunications facility to individuals who need access to perform their job duties.

**OIG Finding: Inadequate Settings for Network Devices-** We identified a total of 11 weaknesses in this area: related to a router, 4 related to a switch, and 2 related to both. For example, the State agency allowed the use of insecure network protocols to manage network devices. In addition, the State agency did not restrict services on network devices, such as Maintenance Operations Protocol used to connect to remote systems, which were not necessary for the State agency's network. Manufacturers configure devices with default settings that are not needed for every network.

**OIG Recommendation:** Implement secure configuration settings for its network devices.

**State Response:** We concur that modifications may be necessary for the identified weaknesses. Changes to configuration settings that do not disrupt MMIS business processes are in the process of being made. To date, our analysis has shown that some OIG recommendations are not appropriate. For example, [redacted] [8]

**OIG Finding: Inadequate Security Control Policies and Procedures-** The State agency did not have adequate policies to verify sanitization of data and disposal of devices, such as hard drives. Also, the State agency did not follow its procedures to:

- document that data could not be recovered from sanitized devices,
- identify the method used to remove data from discarded devices,
- obtain the name and signature of the supervisor responsible for data sanitization, and identify the disposal method for devices.

**OIG Recommendation:** Strengthen policies and follow existing procedures to verify data sanitization and device disposal.

**State Response:** We concur with this specific recommendation. ITSD will update Policy - 300-34 Digital Media Sanitization Policy, to add the requested clarification. Procedures will be created to support the updated policy.

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

**OIG Finding: Inadequate Security Control Policies and Procedures-** The State agency did not have specific inventory policies and procedures for portable devices, such as laptop computers and USB storage devices, and did not account for these devices.

**OIG Recommendation:** Implement policies and procedures to periodically review and account for inventory of all portable devices.

**State Response:** We concur with this specific recommendation. IT will create a policy and supporting procedures to account for and review the inventory of portable devices.

**OIG Finding: Inadequate Personnel Policies and Procedures-** The State agency did not provide periodic refresher training on general security awareness to employees with access to the MMIS. The State agency provided security awareness training only to new employees.

**OIG Recommendation:** Implement adequate personnel policies and procedures for general security awareness training.

**State Response:** We concur with this specific recommendation. IT will research available training to support this requirement and implement initial and periodic training.

**OIG Finding: Inadequate Personnel Policies and Procedures-** The State agency did not have policies to ensure that all employees with significant responsibilities for information security obtain training in their security responsibilities. We judgmentally selected five employees and found that while all five had received training within the last year, one of those five had not received any training in the prior 20 years.

**OIG Recommendation:** Implement adequate personnel policies and procedures for training for employees with significant responsibilities for information security.

**State Response:** We concur with this specific recommendation. IT, for the department will research available training to support this requirement.

**OIG Finding: Inadequate Personnel Policies and Procedures-** The State agency did not have policies to ensure that exit documents were completed for all transferred and terminated employees. We judgmentally selected five terminated employees and found that the State agency did not have exit documents for three of them. Exit documents show the steps to be completed when an employee is transferred or terminated, including collecting keys and electronic keycards and notifying network administrators to remove the employee's network access.

**OIG Recommendation:** Implement adequate personnel policies and procedures for transferred and terminated employees.

**State Response:** We concur with the finding and are in the process of formalizing and implementing expanded policies and procedures to ensure exit documents are completed for all transferred and terminated employees as recommended.

**OIG Finding: Inadequate Personnel Policies and Procedures**- The State agency did not have adequate policies for background checks of employees who had access to ePHI. We judgmentally selected 10 employees who had access to ePHI and found that the State agency did not perform background checks for 3 employees and did not have adequate documentation for 1 employee.

**OIG Recommendation:** Implement adequate personnel policies and procedures for background checks of employees, including those hired from providers or contractors.

**State Response:** We concur with the recommendation. The Department has existing policies and procedures addressing background checks in its HR Policy and Procedures Manual, Section 11B2. The Department will implement additional internal checks to ensure compliance with the policy and OIG's recommendations.

If you have any questions regarding the Department's responses to these findings, please contact Lisa Hettinger, Chief, Bureau of Financial Operations at (208) 287-1141.

Sincerely,

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

PJL/ksl