Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

SUMMARY OF SECURITY VULNERABILITIES IDENTIFIED AT TWO ARIZONA MANAGED CARE ORGANIZATIONS AND INCONSISTENT TREATMENT OF MEDICAID DATA SECURITY AT THE STATE AGENCY AND MANAGED CARE ORGANIZATIONS

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

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

November 2018
A-18-17-09302

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 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

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.

Report in Brief

Date: November 2018
Report No. A-18-17-09302

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Why OIG Did This Review

The HHS OIG's reviews of information system general controls at two Medicaid managed care organizations (MCOs) in Arizona identified numerous security vulnerabilities. The Arizona Health Care Cost Containment System administers Arizona's Medicaid program and is the State agency responsible for monitoring the operations of its contracted MCOs. The MCOs' systems depend on the effectiveness of information system general controls, which are critical to the confidentiality, integrity, and availability of Medicaid data.

Our objective for this review was to summarize the security vulnerabilities that we identified as audit findings in our reviews of whether the two Arizona Medicaid MCOs adequately protected their Medicaid managed care data and information systems in accordance with the Health Insurance Portability and Accountability Act (HIPAA) guidelines.

How OIG Did This Review

We summarized the security vulnerabilities from our reviews into two core categories of general controls—access controls and configuration management.

Summary of Security Vulnerabilities Identified at Two Arizona Managed Care Organizations and Inconsistent Treatment of Medicaid Data Security at the State Agency and Managed Care Organizations

What OIG Found

This summary report consolidates the findings from our two individual reports while omitting details that could compromise the security of any specific MCO that we audited. Our consolidated findings from the reviews of the MCOs show significant vulnerabilities in the MCOs' information systems, and raise concerns about the integrity of the systems used to process Medicaid managed care claims. Some of the same vulnerabilities were identified at both MCOs, suggesting that other Arizona MCO information systems may be similarly vulnerable. Additionally, existing Federal regulations treat the security of Medicaid data differently depending on whether the data reside at the State agencies or at the MCOs. This disparate application of security requirements for Medicaid data could affect State-MCO relationships nationwide and could increase risk to Medicaid patient data.

What OIG Recommends and CMS Comments

We recommend that CMS: 1) conduct a documented risk assessment and determine how the disparate application of Federal security requirements impacts cybersecurity risk for Medicaid data maintained by MCOs and what actions should be taken to address any oversight gap; and 2) inform all State agencies of the types of vulnerabilities we identified at the Arizona MCOs to enhance nation-wide awareness of cybersecurity weaknesses.

CMS did not concur with our recommendation to conduct a documented risk assessment but did concur with our recommendation to inform all State agencies of the cybersecurity vulnerabilities we identified at the Arizona MCOs. CMS stated that the Medicaid managed care regulations help ensure the security of beneficiaries' data and CMS believes that it is clear that the phrase stated within the regulations "any other applicable Federal and state laws" would require MCOs, under contract with a State, to fully comply with HIPAA security requirements. In addition, CMS stated that a risk assessment is already a requirement under the jurisdiction of the HHS Office for Civil Rights (OCR) and it would be duplicative of existing risk assessment efforts.

Since this issue resides in the Medicaid program and OCR is not responsible for the disparate application of Federal security requirements, OIG believes that CMS is in the best position to ensure that data security regulations are consistently applied to protect Medicaid beneficiaries' data, regardless of where the data resides.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181709302.asp.

TABLE OF CONTENTS

APPENDICES

INTRODUCTION

WHY WE DID THIS REVIEW

The U.S. Department of Health and Human Services (HHS), Office of Inspector General's (OIG's) reviews of information system general controls at two Medicaid managed care organizations (MCOs) in Arizona identified numerous security vulnerabilities. The Arizona Health Care Cost Containment System (State agency) administers Arizona's Medicaid program and is responsible for monitoring the operations of its contracted MCOs. The Medicaid MCOs' systems depend on the effectiveness of information system general controls, which are critical to the confidentiality, integrity, and availability of Medicaid data. Without effective general controls, MCOs may not be able to adequately safeguard sensitive Medicaid managed care systems and data.

We issued our draft report for the first MCO we reviewed to the State agency and the State agency responded that it was not responsible for MCOs' data security compliance with the Health Insurance Portability and Accountability Act (HIPAA).[1] The State agency further stated that the Centers for Medicare & Medicaid Services' (CMS') regulations do not require States to include data security standards in Medicaid MCO contracts and do not include State responsibility for oversight of Medicaid data security at MCOs. OIG acknowledged the State agency's response, and we subsequently issued both of our reports directly to the MCOs.

In responding to our reports, the MCOs did not concur with half of OIG's findings; however, the MCOs acknowledged most of the findings identified and stated that they were committed to addressing them. This summary report consolidates the findings from our individual reports while omitting details that could compromise the security of any specific MCO we audited.

The information presented in this summary report should lead CMS, States, and MCOs to strengthen the MCOs' system security. Protecting HHS data, systems, and beneficiaries from cybersecurity threats is a top management challenge for HHS. HHS must protect its beneficiaries by fostering a culture of cybersecurity among its partners and stakeholders.

OBJECTIVE

Our objective was to summarize the security vulnerabilities that we identified as audit findings from our reviews of whether two Arizona Medicaid MCOs adequately protected their Medicaid managed care data and information systems in accordance with the HIPAA guidelines.

[1] The State agency also stated that since its arrangement with the MCO was an "organized health care arrangement," which by definition is not a HIPAA business associate relationship, the State agency was not responsible for the MCO's data security.

BACKGROUND

Medicaid Program

The Medicaid program provides medical assistance to low-income individuals and individuals with disabilities. The Federal and State Governments jointly fund and administer the Medicaid program. HHS oversees States' use of Federal entitlement benefits for the program. Federal regulations require State agencies to establish the appropriate computer system security requirements based on recognized industry standards or standards governing security of Federal computer systems or information processing.[2]

Medicaid Managed Care Organizations

Within the Medicaid program, managed care is a model for delivering health care services to beneficiaries that differs from the traditional fee-for-service model. State Medicaid agencies contract with MCOs to provide a specific set of services to Medicaid enrollees in return for a capitated payment. MCOs include health maintenance organizations, prepaid health plans, and comparable organizations. At the time of our initial audits (September 2016), Arizona had 13 MCOs with more than 1.5 million beneficiaries, totaling more than $8 billion in spending for fiscal year 2016.

Information System General Controls

Information system general controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure proper operations of information systems, and create a secure environment for application systems. Some primary objectives of general controls are to safeguard data, protect computer applications, prevent unauthorized access to system software, and ensure continued computer operations after unexpected interruptions. General controls are applied at the entity wide, system, and business process application levels.

The effectiveness of general controls is a significant factor in determining the effectiveness of controls at the business process application level. Without effective general controls at the entity wide and system levels, controls at the business process application level may be more easily circumvented or modified. General controls impact the integrity of the Medicaid program and are critical to ensuring the confidentiality, integrity, and availability of data.

HOW WE CONDUCTED THIS REVIEW

We grouped the security vulnerabilities from our previous reviews of information system general controls at the two MCOs into two core categories of general controls—access controls and configuration management. In addition, we identified an overarching finding based on those reviews.

[2] 45 CFR § 95.621

We conducted the two performance audits 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 contains details of our audit scope and methodology. Appendix B contains a list of the Federal requirements for information security that we evaluated in our reviews of the two MCOs.

FINDINGS

SUMMARY OF VULNERABILITIES IDENTIFIED AT THE TWO MANAGED CARE ORGANIZATIONS REVIEWED

We identified 19 security vulnerabilities in the information system general controls at the two MCOs we reviewed. We grouped the 19 vulnerabilities into 9 security control areas within two information system general control categories: access controls and configuration management.

- In the access controls category, we identified five vulnerabilities related to remote network access, password and login controls, and physical security controls.

- In the configuration management category, we identified 14 vulnerabilities related to configuration of network devices, patch management, antivirus management, server management, database management, and website security.

In three of the security control areas, which accounted for 10 of the 19 vulnerabilities, we noted that the vulnerabilities were similar in both MCOs' information systems, which indicated that the vulnerabilities identified may be systemic.[3] We performed the same audit steps to assess each MCO's general controls; however, because of how the MCOs managed the configuration settings of their information systems, we could not conclude that all Medicaid managed care information system security environments have similar vulnerabilities.

Although we did not identify evidence that the vulnerabilities had been exploited, exploitation could result in unauthorized access to, and disclosure of, sensitive information, as well as disruption of critical operations at the two MCOs. As a result, the vulnerabilities were collectively—and in some cases, individually—significant, and could have potentially compromised the integrity of the Medicaid data at the MCOs.

[3] Each of the MCOs had similar vulnerabilities in the following three security control areas: configuration of network devices, database management, and website security.

The Table below summarizes the vulnerabilities we identified and total number by security control area and MCO for each category of general controls.

Table: Vulnerabilities by Security Control Area and Managed Care Organization for Each Category of General Controls

Security Control Areas	MCO		Total No. of Vulnerabilities
	A	B	
Access Control			
Remote network access	2	0	2
Password and login controls	2	0	2
Physical security controls	1	0	1
Subtotal	**5**	**0**	**5**
Configuration Management			
Configuration of network devices	2	2	4
Patch management	1	0	1
Antivirus management	1	0	1
Server security management	2	0	2
Database management	1	2	3
Website security	2	1	3
Subtotal	**9**	**5**	**14**
Grand Total	**14**	**5**	**19**

ACCESS CONTROLS

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limits access of authenticated users to files, resources, and actions that they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. Access controls should be formally developed, documented, disseminated, and periodically updated to provide reasonable assurance that information security resources are protected against unauthorized modification, disclosure, loss, or impairment. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. It is fundamental that control techniques for both logical and physical access controls be risk-based (i.e., identify the associated risks if controls are ineffective and the critical elements that should be achieved for information system controls to be effective).

We identified five access control vulnerabilities at one MCO and grouped these vulnerabilities into three security control areas.

Remote Network Access—Two Vulnerabilities Identified

The use of remote access to connect users with an MCOs' secure network via the internet places Medicaid systems at a higher risk of compromise than those systems that restrict access to internal network users only. To enhance controls for remote network access, the information system should use two-factor authentication, which adds another layer of security that makes it harder for potential intruders to gain access to a network. Two-factor authentication requires using two of the following three factors to achieve authentication: (1) something you know, such as a password or personal identification number; (2) something you have, such as a cryptographic identification device or token; or (3) a unique means of physical identification, such as a biometric fingerprint or retinal scan.

We identified two vulnerabilities related to remote network access. As an example, the remote access policy did not specify the use of two-factor authentication for remote network access. The MCO officials stated that they were not aware of the vulnerability. Without the use of two-factor authentication for remote access, there is an increased risk of unauthorized access to sensitive computer systems and data.

Password and Login Controls—Two Vulnerabilities Identified

User authentication establishes the validity of a user's claimed identity, typically when the user accesses a system or an application. An organization must implement procedures to authenticate a person or an entity seeking access to sensitive data. Furthermore, an organization should disable or remove inactive accounts and accounts for terminated individuals in a timely manner.

We identified two vulnerabilities related to password and login controls. As an example, the MCO did not disable user accounts for terminated employees in a timely manner even though the MCO's policies and procedures stated that access should be disabled promptly after the user's termination. According to an MCO official, the delays in disabling user accounts were caused by (1) a manager failing to inform the Human Resources (HR) department of an employee's termination and (2) HR failing to process in a timely manner an employee's termination after the manager informed HR. Without strong password and login controls, there is an increased risk of unauthorized access to sensitive data.

Physical Security Controls—One Vulnerability Identified

Physical security controls that are commensurate with the risks of physical damage or access should be established. Access to facilities should be limited to personnel having a legitimate need for access to perform their duties. Physical security controls depend on the effectiveness

of the entity's policies and practices pertaining to the overall facility and to areas housing sensitive information technology components and may include identification cards, keycards, smartcards, passkeys, and other entry devices.

We identified one vulnerability related to physical security controls. The MCO did not adequately secure its use of temporary keycards. Although the MCO had physical access policies and procedures, they did not address tracking the use of temporary keycards. This allowed a situation in which an official was using a temporary keycard. He received the temporary keycard from a terminated temporary worker, but the official mistakenly turned in his own keycard instead of the temporary one. An MCO official stated that temporary keycards were not adequately tracked and were reissued to employees without being reviewed, allowing the mix-up in keycards to continue. Inappropriate physical access to a facility increases the risk of unauthorized access to sensitive data.

CONFIGURATION MANAGEMENT

Configuration management provides reasonable assurance that (1) changes to information system resources, such as the settings of devices on the network, 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 entity-wide, system (hardware), and application (software) levels to ensure the security of the system.

We identified 14 configuration management control vulnerabilities between the two MCOs and grouped these vulnerabilities into six security control areas.

Configuration of Network Devices—Four Vulnerabilities Identified

Organizations must implement policies and procedures to protect sensitive data from improper alteration or destruction and implement technical security measures to guard against unauthorized access to sensitive data that is transmitted over an electronic communications network.

We identified four vulnerabilities related to configuration of network devices. As an example, both MCOs did not securely configure the setting for the firewall's Secure Shell (SSH)[4] session timeout. Only administrators should have access to this setting and use it to determine whether an SSH session is no longer being used, enabling a device to determine when a connection can be automatically disconnected. The default timeout session for this firewall was set at 5 minutes. However, at one MCO it was changed to 30 minutes, which allowed more time for a potential attacker to access the system using an authenticated administrator session that had not been properly ended. An attacker could have obtained information on the configuration settings and performed malicious activities acting as the previously authenticated administrator user. Because network devices are integral to ensuring the security of the claims

[4] The SSH protocol is commonly used to manage devices remotely using encryption.

processing system, failure to adequately secure these devices exposes a network and its resources to attacks on the confidentiality, integrity, and availability of sensitive information. The MCO officials acknowledged the vulnerability and changed the timeout settings on the firewall that we tested before we completed our fieldwork.

Patch Management—One Vulnerability Identified

Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. Patch management includes acquiring and testing patches, applying patches to a computer system, and monitoring those patches. Organizations should deploy patches to all systems that have vulnerabilities, even for those systems that are not at immediate risk of exploitation.

We identified one vulnerability related to patch management. The MCO did not have adequate procedures to ensure that software patches for its workstations were applied in a timely manner. MCO officials acknowledged that they did not have adequate procedures to ensure that patching was current on all workstations. The officials stated that patching required users to restart their workstations before patches were applied, and some users were not restarting their workstations. Officials also stated that they would look into options to force reboots to ensure patches would be installed in a timely manner. Without adequate patch management, an attacker may be able to gain unauthorized access to sensitive data and personally identifiable information on a network. For example, in May 2017, the WannaCry ransomware worldwide cyberattack targeted unpatched computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments.

Antivirus Management—One Vulnerability Identified

Virus-scanning software should be provided at critical entry points to a network, such as the network's production servers. Organizations must implement policies and procedures to protect sensitive data from improper alteration or destruction.

We identified one vulnerability related to antivirus management. Specifically, an MCO had Windows production servers with antivirus software installed that did not have current antivirus definitions. MCO officials stated that recent changes had been made to the software that deployed the antivirus definitions, and officials later discovered that about half of the servers had not received the definition updates. Without current antivirus definitions, antivirus software may become out of date and no longer protect against current viruses.

Server Security Management—Two Vulnerabilities Identified

Organizations should keep software current by establishing effective programs for patch management, virus protection, and other emerging threats. In addition, software should be scanned and updated frequently to guard against known vulnerabilities.

We identified two vulnerabilities related to server security management at one MCO. As an example, the MCO had three production servers supporting the claims processing system that used software for which the vendor no longer issued security updates. MCO officials stated that the MCO was in the process of decommissioning the servers running the outdated software. Without a vendor-supported operating system, the production servers supporting the claims processing system was vulnerable to known exploits. This increased the risk that the system or some part of the system could become compromised or stop functioning.

Database Management—Three Vulnerabilities Identified

General controls over databases are important to adequately protect access to the underlying data. Organizations should keep their databases 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.

We identified three vulnerabilities related to database security controls at both MCOs. As an example, one MCO did not encrypt its claims processing database to ensure the security of sensitive data. MCO officials stated that they understood the importance of encryption; however, because the data center supported multiple clients, officials stated that they relied on compensating controls[5] to protect data residing in their databases. We did not review these controls because compensating controls cannot be as effective as encryption in protecting sensitive Medicaid managed care data. Without adequate policies and procedures for securing databases, there is an increased risk of unauthorized access to sensitive data.

Website Security—Three Vulnerabilities Identified

Web applications may present significant additional information system risks. Improperly configured web applications can expose the application and the entity's internal network resources, including sensitive systems, to unauthorized access.

We identified three vulnerabilities related to website security at both MCOs. As an example, one MCO did not adequately secure its website for providers. The MCO stated that when it tried to upgrade to a more secure protocol, providers had trouble accessing the MCO's website, resulting in significant business problems. An inadequately secured website for providers could allow attackers to execute malicious code and obtain sensitive data.

FEDERAL REQUIREMENTS FOR STATES AND MANAGED CARE ORGANIZATIONS

Federal regulations require the State Medicaid plan to safeguard applicants' and beneficiaries' information (42 CFR §§ 431.300, 433.112). Federal regulations (42 CFR § 431.303) dictate that

[5] Compensating controls include using stronger authentication to prevent automated processes from getting past network defenses, limiting the number of privileged accounts, and using strong physical controls within the data center.

"the [State] Medicaid agency must have authority to implement and enforce the provisions in this subpart for safeguarding information about applicants and recipients." The types of information to be safeguarded include, but are not limited to names and addresses, medical services provided, and medical data (42 CFR § 431.305). However, Federal regulations for managed care programs neither require the MCOs to meet the same Federal regulations as the State Medicaid agencies nor require States to provide oversight of the security of Medicaid data and information systems at the MCOs.

At the Federal level, CMS oversees the Medicaid managed care program. Federal regulations state that CMS must review and approve all MCO contracts (42 CFR § 438.3).[6] Proposed final contracts must be submitted in the form and manner established by CMS (42 CFR § 438.3). However, these Federal regulations for managed care programs do not include a specific requirement that States adopt data security standards or conduct oversight of the security of Medicaid managed care data and information systems (42 CFR § 438).

In addition, Federal regulations require States to ensure through their contracts that each MCO uses and discloses individually identifiable health information in accordance with the privacy requirements in 45 CFR parts 160 and 164, subparts A (HIPAA Security and Privacy General Provisions) and E (HIPAA Privacy Rule), to the extent that they are applicable (42 CFR § 438.224). The regulations do not include a specific requirement that States ensure compliance with 45 CFR part 164, subpart C, which contains the HIPAA security requirements.

After completing the review of the first Arizona MCO, we issued a draft report to the State agency. The State agency informed us that it is not responsible for the contracted MCOs' compliance with the security requirements of the HIPAA Security Rule (45 CFR part 164, subpart C) because the Federal regulations do not require this compliance as a contract element.[7] However, when we discussed this issue with CMS, CMS officials stated that CMS does not agree with the State agency's position.

CONCLUSION

Our consolidated findings from the reviews of the MCOs show significant vulnerabilities in the MCOs' information systems and raise concerns about the integrity of the systems used to process Medicaid managed care claims. The fact that some of the same vulnerabilities were identified at both MCOs suggests that other Arizona Medicaid MCOs may be similarly vulnerable. This report is intended to provide information to assist CMS, the State agency, and the MCOs in strengthening the MCOs' system security.

[6] This includes those risk and nonrisk contracts that on the basis of their value are not subject to the prior approval requirement in 42 CFR § 438.806.

[7] Arizona stated that its relationship with its MCO is an organized health care arrangement, a HIPAA-defined term that is not a HIPAA business associate relationship. See 45 CFR §160.103 Definition of Business Associate subsection (4)(iv).

Existing Federal regulations treat the security of Medicaid data differently depending on whether the data reside at the State agencies or at the MCO. The State Medicaid agencies must follow Federal security requirements for their Medicaid data, yet the MCOs handling the States' Medicaid data do not have to follow the same Federal security regulations. In addition, there are no Federal regulations requiring States to provide oversight for ensuring MCOs comply with Federal security requirements related to Medicaid data. Further, depending on the type of arrangement involved, the State may not have to include HIPAA data security standards in MCOs' contracts or ensure MCO compliance with those standards. This disparate application of security requirements for Medicaid data could affect State-MCO relationships nationwide and could increase risk to Medicaid patient data.

RECOMMENDATIONS

We recommend that CMS:

- conduct a documented risk assessment and determine how the disparate application of Federal security requirements impacts cybersecurity risk for Medicaid data maintained by MCOs and, what actions should be taken to address any oversight gap (e.g., include an additional requirement in the State Plan that obligates States to be specifically responsible for ensuring data at MCOs is protected); and

- inform all State agencies of the types of vulnerabilities we identified at the Arizona MCOs to enhance nation-wide awareness of cybersecurity weaknesses.

CMS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS COMMENTS

In written comments, CMS stated that they not did not concur with our recommendation to conduct a documented risk assessment but did concur with our recommendation to inform all State agencies of the cybersecurity vulnerabilities we identified at the Arizona MCOs. CMS stated that a risk assessment is already a requirement under the jurisdiction of the HHS Office for Civil Rights (OCR), and it would be duplicative of existing risk assessment efforts. CMS believed that it would be more effective to work with OCR to remind States and MCOs of their existing responsibilities for risk analysis and management under the HIPAA security regulations. CMS also provided technical comments to support their position. CMS' official comments are included as Appendix C.

OFFICE OF INSPECTOR GENERAL RESPONSE

OIG disagrees that CMS conducting a risk assessment would be duplicative of existing risk assessment efforts. OIG is concerned that the Medicaid MCO regulations do not include data security. As mentioned earlier in this report, if the State agency processed the Medicaid claims, the State would be required to establish appropriate system security requirements based on

recognized industry standards or standards governing security of Federal systems or information processing.[8] CMS could then hold the state accountable for data security. By having no data security requirements in the Medicaid MCO regulations, CMS risks disparate protection of Medicaid beneficiaries' data.

For that reason, OIG recommended CMS perform a documented risk assessment. OIG did not recommend that the MCO's conduct a risk assessment of the MCO's data security, which CMS addressed in their response. OIG recommended that CMS conduct a documented risk assessment and determine how the disparate application of Federal requirements impacts cybersecurity risk for Medicaid data maintained by MCOs. The OCR could remind States and MCOs of their existing responsibilities as HIPAA covered entities under the HIPAA security regulations, but OCR is not responsible for the disparate application of Federal security requirements for Medicaid data maintained by the State versus MCOs. Since this issue resides in the Medicaid program, we believe that CMS is in the best position to ensure that data security regulations are consistently applied to protect Medicaid beneficiaries' data, regardless of where the data resides.

We maintain that our findings and recommendations remain valid.

[8] 45 CFR § 95.621

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We summarized the security vulnerabilities from our reviews of information system general controls at two Arizona MCOs into two core categories of general controls—access controls and configuration management. All of the vulnerabilities identified at the MCOs and presented in the table (page 4) of this report, were noted in the individual MCO reviews, which we performed from CYs 2015 to 2017.

METHODOLOGY

We conducted reviews of the information security general controls at the two MCOs in Arizona using selected procedures from GAO's *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. However, the selected procedures performed at the MCOs varied; we did not review all of the security control areas at both organizations. We conducted these reviews by observing information security operations, interviewing personnel, testing hardware and software configurations, and analyzing system security reports.

We conducted these performance audits 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: FEDERAL REQUIREMENTS FOR INFORMATION SYSTEM SECURITY

The principal Federal requirements evaluated in our reviews of the two MCOs:

- 42 CFR § 438.3(f)(1), "Managed Care: Standard Contract Requirements;"
- 42 CFR § 438.224, "Managed Care: Confidentiality;"
- 45 CFR part 164, subpart C, "Security Standards for the Protection of Electronic Protected Health Information;"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*;
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-40, revision 3.0, *Guide to Enterprise Patch Management Technologies*;
- NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- NIST SP 800-92, *Guide to Computer Security Log Management*; and
- Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*.

APPENDIX C: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: SEP - 7 2018

TO: Daniel R. Levinson
Inspector General

FROM: Seema Verma
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: Summary of Security Vulnerabilities Identified at Two Arizona Managed Care Organizations and Possible Inconsistent Oversight of Data Security at Medicaid Managed Care Organizations (A-18-17-09302)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report. CMS takes seriously its responsibility to protect and secure Medicaid beneficiary data.

CMS administers the Medicaid program, a joint federal-state health program for low-income and disabled beneficiaries, which states operate primarily through either a fee-for-service delivery system or a managed care delivery system. In a fee-for-service delivery system, states make payments to participating providers for the delivery of Medicaid services to beneficiaries. In a managed care delivery system, states contract with managed care plans and require that the plans provide or arrange for a specified package of Medicaid services for enrolled beneficiaries. When states contract with managed care plans that offer a comprehensive package of Medicaid benefits, the plans are referred to as managed care organizations (MCOs). Under the contracts between the state and its MCOs, the MCOs are paid a fixed, prospective, monthly payment for each enrolled beneficiary.

States have primary responsibility for operating their programs, including contracting with MCOs to provide Medicaid services in a manner that complies with state and Federal laws. CMS oversees states' operations, including the responsibilities and activities contractually delegated to MCOs. Specifically, CMS reviews and approves states' contracts with MCOs for compliance with Federal Medicaid requirements. In addition, CMS has published guidance that is intended to provide transparency on the criteria for contract approvals and to help states verify that contracts with Medicaid managed care entities meet all CMS requirements.

CMS' Medicaid managed care regulations[1] help ensure the security of beneficiaries' data when they receive Medicaid services through an MCO. The Medicaid managed care regulations require that the state's contract with an MCO comply with all applicable Federal and state laws and regulations.[2] State Medicaid Agencies and MCOs have been required to comply with

[1] 42 CFR part 438
[2] 42 CFR 438.3(f)(1)

HIPAA privacy and security requirements and would understand that it is an applicable Federal law.

The Medicaid managed care regulations also require that states must ensure that each MCO complies with any other applicable Federal and state laws.[3] Based on State Medicaid Agencies' and MCOs' long-standing requirement to comply with HIPAA, CMS believes that it is clear that the phrase, "any other applicable Federal and state laws" would require MCOs, under contract with a state, to fully comply with HIPAA security requirements.

OIG's recommendations and CMS' responses are below.

OIG Recommendation

The OIG recommends that CMS conduct a documented risk assessment and determine how the disparate application of Federal security requirements impacts cybersecurity risk for Medicaid data maintained by MCOs and, what actions should be taken to address any oversight gap.

CMS Response

CMS does not concur with OIG's recommendation. CMS believes that the privacy and security of Medicaid beneficiaries' data is critical, and the protection of the data should be a high priority for MCOs, states, and CMS. As stated above, CMS' Medicaid managed care regulations help ensure the security of beneficiaries' data when they receive Medicaid services through an MCO.

However, Federal requirements for state Medicaid agencies and their contracted MCOs to conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information[4] is already a requirement under the jurisdiction of the Department of Health and Human Services Office for Civil Rights. CMS is concerned that conducting a risk assessment would be duplicative of existing risk assessment efforts. CMS believes that it would be more effective to work with the Office for Civil Rights to remind States and MCOs of their existing responsibilities for risk analysis and management under the HIPAA security regulations.

OIG Recommendation

The OIG recommends that CMS inform all State agencies of the types of vulnerabilities we identified at the Arizona MCOs to enhance nation-wide awareness of cybersecurity weaknesses.

CMS Response

CMS concurs with OIG's recommendation. CMS will inform all state agencies of the types of vulnerabilities identified at the Arizona MCOs to enhance nation-wide awareness of cybersecurity weaknesses.

CMS thanks the OIG for their efforts on this issue and looks forward to working with the OIG on this and other issues in the future.

[3] 42 CFR 438.100(d)
[4] See 45 CFR 164.308(a)(1)(ii)(A)