Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HIGH-RISK SECURITY VULNERABILITIES IDENTIFIED DURING REVIEWS OF INFORMATION SYSTEM GENERAL CONTROLS AT THREE CALIFORNIA MANAGED-CARE ORGANIZATIONS RAISE CONCERNS ABOUT THE INTEGRITY OF SYSTEMS USED TO PROCESS MEDICAID CLAIMS

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

Thomas M. Salmon
Assistant Inspector General
for Audit Services

November 2015
A-09-15-03004

Office of Inspector General

http://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 http://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 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

High-risk security vulnerabilities that we identified during reviews of information system general controls at three Medicaid managed-care organizations in California raise concerns about the integrity of the systems used to process Medicaid claims.

This summary report provides an overview of the results of the U.S. Department of Health and Human Services (HHS), Office of Inspector General's (OIG) reviews of three Medicaid managed-care organizations (MCOs) in California. This summary report consolidates the findings from our individual reports while omitting specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We provided more detailed information and recommendations to officials responsible for the MCOs so that they could address the issues we identified. Our findings reflect the state of system security at the MCOs when we reviewed them; their systems may have changed since our reviews.

WHY WE DID THESE REVIEWS

OIG's reviews of information system general controls at three MCOs in California identified pervasive high-risk security vulnerabilities. California's Department of Health Care Services (State agency) administers the Medicaid program, known as Medi-Cal, and is responsible for monitoring and oversight of MCOs. The integrity of the State agency's Medi-Cal managed-care systems depends on the effectiveness of information system general controls, which are critical to the reliability, confidentiality, and availability of Medi-Cal data. Without effective general controls, the State agency is not able to adequately safeguard sensitive Medi-Cal managed-care systems and data.

In responding to OIG's work and agreeing with the vast majority of OIG's recommendations in the three reports on the MCOs' controls, the State agency acknowledged the vulnerabilities identified and stated that it was committed to addressing them. The information presented in this summary report may lead the Centers for Medicare & Medicaid Services (CMS) and all States to strengthen MCOs' system security. OIG has identified the security of health information systems as a top challenge facing HHS, its contractors, and States.

Our objective was to summarize the high-risk security vulnerabilities that we identified as audit findings in our reviews of information system general controls at three California Medi-Cal MCOs.

BACKGROUND

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 entitywide, system, and business process application levels.

We conducted our reviews of the information system general controls at the three MCOs from calendar years 2012 through 2015 using selected procedures from the Government Accountability Office's *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. Our reports made recommendations to the State agency regarding the vulnerabilities that we had identified, most of which were high risk. (According to Federal guidance, "high risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.") In almost all cases, the State agency agreed with our recommendations and described corrective actions that it had taken or planned to take. We restricted the distribution of these reports to the MCOs, the State agency, and the CMS action official because of the sensitivity of the vulnerabilities, which could have left the MCOs' information systems susceptible to exploitation or attack. As of May 2015, California had 87 MCOs with more than 9.5 million beneficiaries.

WHAT WE FOUND

We identified 74 high-risk security vulnerabilities in the information system general controls at the 3 Medi-Cal MCOs we reviewed. We grouped these 74 vulnerabilities into 14 security control areas within 3 information system general control categories: access controls, configuration management, and security management. In 6 of the 14 security control areas, all 3 MCOs had vulnerabilities, which accounted for 53 of the 74 vulnerabilities. Accordingly, we determined that most of the 74 vulnerabilities were significant and pervasive.

- In the access controls category, we identified 31 vulnerabilities related to portable and backup media, database security controls, password and login controls, wireless local area network controls, remote network access, and physical security controls.

- In the configuration management category, we identified 29 vulnerabilities related to configuration of network devices, patch management, antivirus management, and out-of-date software.

- In the security management category, we identified 14 vulnerabilities related to contingency planning, required system security plan elements, sanitization of data and disposal of devices, and background checks.

In six of the security control areas, we noted similar vulnerabilities in all three MCOs' information systems, which indicated that the vulnerabilities identified were systemic and pervasive across the MCOs. We performed the same audit steps to assess each MCO's general controls; however, because of minor differences in the types of information systems at each MCO, we cannot conclude that all Medi-Cal managed-care information system security environments have similar vulnerabilities.

WHAT WE CONCLUDE

Our consolidated findings from the individual reports show significant vulnerabilities in the three MCOs' information systems and raise concerns about the integrity of the systems used to process

Medicaid managed-care claims. The State agency informed us, in comments on the individual reports on the MCOs' information system general controls, that it was addressing these vulnerabilities. The fact that some of the same vulnerabilities were identified at all three MCOs suggests that other California Medi-Cal managed-care information systems may be similarly vulnerable. This summary report is intended to provide information to assist the State agency and CMS in strengthening MCOs' system security.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THESE REVIEWS

The U.S. Department of Health and Human Services (HHS), Office of Inspector General's (OIG) previous reviews of information system general controls at three Medicaid managed-care organizations (MCOs) in California identified pervasive high-risk security vulnerabilities. California's Department of Health Care Services (State agency) administers the Medicaid program, known as Medi-Cal, and is responsible for monitoring and oversight of MCOs. The integrity of the State agency's Medi-Cal managed-care systems depends on the effectiveness of information system general controls, which are critical to the reliability, confidentiality, and availability of Medi-Cal data. Without effective general controls, the State agency is not able to adequately safeguard sensitive Medi-Cal managed-care systems and data.

In responding to OIG's work and agreeing with the vast majority of OIG's recommendations in the three reports on the MCO's controls, the State agency acknowledged the vulnerabilities identified and stated that it was 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 may lead the Centers for Medicare & Medicaid Services (CMS) and all States to strengthen MCOs' system security. OIG has identified the security of health information systems as a top challenge facing HHS, its contractors, and States.

OBJECTIVE

Our objective was to summarize the high-risk security vulnerabilities that we identified as audit findings in our reviews of information system general controls at three California Medi-Cal MCOs.

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 on the basis of recognized industry standards and standards governing security of Federal computer systems and information processing (45 CFR part 95).

Medicaid Managed-Care Organizations

Within the Medicaid program, managed care is a model for delivering health care services to beneficiaries, which differs from the traditional fee-for-service model. State Medicaid agencies contract with MCOs to provide a specific set of services to Medicaid enrollees, usually in return for a predetermined periodic payment per enrollee. MCOs include health maintenance

organizations, prepaid health plans, and comparable organizations. As of May 2015, California had 87 MCOs with more than 9.5 million beneficiaries.

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 entitywide, system, and business process application levels.

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

Office of Inspector General Reviews of Information System General Controls at California's Medi-Cal Managed-Care Organizations

We conducted our reviews of the information system general controls at the three MCOs from calendar years (CYs) 2012 through 2015 using selected procedures from the Government Accountability Office's (GAO) *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. Our reports made recommendations to the State agency regarding the vulnerabilities that we had identified, most of which were high risk.[1] In almost all cases, the State agency agreed with our recommendations and described corrective actions that it had taken and planned to take. We restricted the distribution of these reports to the MCOs, the State agency, and the CMS action official because of the sensitivity of the vulnerabilities, which could have left the MCOs' computer systems susceptible to exploitation or attack.

HOW WE CONDUCTED THESE REVIEWS

We grouped the high-risk security vulnerabilities from our previous reviews of information system general controls at three MCOs into three core categories of general controls: access controls, configuration management, and security management. All of the vulnerabilities presented in this summary report were noted in the previous audit reports.

We conducted the three performance audits in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[1] According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, revision 1, *Guide for Conducting Risk Assessments*, "high risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation" (Appendix I, Table I-3, Assessment Scale—Level of Risk).

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, and Appendix B contains a list of the Federal requirements for information security that we evaluated in our reviews of the three MCOs.

FINDINGS

We identified 74 high-risk security vulnerabilities in the information system general controls at the 3 Medi-Cal MCOs we reviewed. We grouped these 74 vulnerabilities into 14 security control areas within 3 information system general control categories: access controls, configuration management, and security management. In 6 of the 14 security control areas, all 3 MCOs had vulnerabilities, which accounted for 53 of the 74 vulnerabilities. Accordingly, we determined that most of the 74 vulnerabilities were significant and pervasive.

- In the access controls category, we identified 31 vulnerabilities related to portable and backup media, database security controls, password and login controls, wireless local area network controls, remote network access, and physical security controls.

- In the configuration management category, we identified 29 vulnerabilities related to configuration of network devices, patch management, antivirus management, and out-of-date software.

- In the security management category, we identified 14 vulnerabilities related to contingency planning, required system security plan elements, sanitization of data and disposal of devices, and background checks.

In six of the security control areas, we noted similar vulnerabilities in all three MCOs' information systems, which indicated that the vulnerabilities identified were systemic and pervasive across the MCOs. We performed the same audit steps to assess each MCO's general controls; however, because of minor differences in the types of information systems at each MCO, we cannot conclude that all Medi-Cal managed-care information system security environments have similar vulnerabilities.

The table on the following page summarizes the high-risk vulnerabilities we identified and totals them by security control area and MCO for each category of general controls.

Table: High-Risk 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	C	
Access Control				
Portable and backup media	5	3	2	10
Database security controls	4	3	1	8
Password and login controls	3	1	1	5
Wireless local area network controls	1	4	0	5
Remote network access	0	1	1	2
Physical security controls	0	1	0	1
Subtotal	**13**	**13**	**5**	**31**
Configuration Management				
Configuration of network devices	10	8	6	24
Patch management	1	1	1	3
Antivirus management	1	0	0	1
Out-of-date software	0	1	0	1
Subtotal	**12**	**10**	**7**	**29**
Security Management				
Contingency planning	5	0	0	5
Required system security plan elements	2	0	2	4
Sanitization of data and disposal of devices	1	1	1	3
Background checks	0	2	0	2
Subtotal	**8**	**3**	**3**	**14**
Grand Total	**33**	**26**	**15**	**74**

Each of the three MCOs had vulnerabilities in the following six security control areas: portable and backup media, database security controls, password and login controls, configuration of network devices, patch management, and sanitization of data and disposal of devices.

ACCESS CONTROLS

Access controls include logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files, and physical controls, such as keeping computers in locked rooms to limit physical access. 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.

We identified 31 access control vulnerabilities at the 3 MCOs and grouped these vulnerabilities into 6 security control areas.

Portable and Backup Media—10 Vulnerabilities Identified

The storage of electronic protected health information (ePHI) on portable media, such as Universal Serial Bus (USB) flash drives,[2] is a risky practice. The ability to store and transport substantial volumes of data on portable devices creates an additional risk that confidential information will be compromised. Organizations must implement mechanisms to encrypt and decrypt ePHI, including ePHI on portable devices. Encryption should be considered for backup media that are sent offsite for storage to secure data that could be lost or stolen in transit or at an alternate site.

We identified 10 vulnerabilities related to portable and backup media. For example, one MCO did not protect portable devices containing ePHI with appropriate encryption. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used should be compliant with Federal Information Processing Standards (FIPS).[3] Without such encryption, there is an increased risk of unauthorized access to ePHI stored on portable media.

Database Security Controls—Eight Vulnerabilities Identified

General controls over databases and operating systems are important to adequately protect access to the underlying data. Organizations should stay up to date with the latest recommended security practices, techniques, and technologies. Current industry best practices include reviewing logs and developing and implementing policies and procedures for securing databases.

We identified eight vulnerabilities related to database security controls. For example, one MCO did not encrypt its claims processing database to ensure the security of ePHI. Without adequate policies and procedures for securing databases, there is an increased risk of unauthorized access to sensitive data.

Password and Login Controls—Five Vulnerabilities Identified

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

We identified five vulnerabilities related to password and login controls. For example, one MCO did not disable user accounts for terminated employees in a timely manner. Without strong password and login controls, there is an increased risk of unauthorized access to sensitive data.

[2] A USB flash drive is a plug-and-play portable storage device that is lightweight enough to attach to a keychain.

[3] FIPS Publication 140-2 (as amended) specifies the security requirements for encryption to protect sensitive information.

Wireless Local Area Network Controls—Five Vulnerabilities Identified

Before organizations select wireless local area network (WLAN) equipment, they should review their existing identity management infrastructure, authentication requirements, and security policy. Organizations should establish a usage policy that specifies which user communities are authorized to use WLAN technology and for what purposes. In addition, organizations should develop a program of audit processes and procedures to help ensure that they can detect unauthorized behavior and security breaches on wireless systems.

We identified five vulnerabilities related to WLAN controls. For example, one MCO did not manage its WLAN to restrict access to inappropriate Web sites and did not log its WLAN activity. Without adequate WLAN controls, sensitive information may not be protected from intentional or unintentional loss or damage.

Remote Network Access—Two Vulnerabilities Identified

The use of remote access to connect users with MCOs' secure networks via the Internet places Medi-Cal 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. For example, one MCO's remote access policy did not specify the use of two-factor authentication for remote network access. Without the use of two-factor authentication for remote access, there is an increased risk of unauthorized access to sensitive computer systems and data.

Physical Security Controls—One Vulnerability Identified

Physical controls should be implemented to limit unauthorized access to digital media removed from the information system and during pickup, transport, and delivery to authorized users. Organizations should use lockable physical containers to protect information system components, such as tapes, from unauthorized physical access.

We identified one vulnerability related to physical security controls. Specifically, one MCO did not adequately secure its backups of system and claim data stored at an offsite storage facility. Without properly securing backups of system and claim data, there is an increased 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 entitywide, system (hardware), and application (software) levels to ensure the security of the system.

We identified 29 configuration management control vulnerabilities at the 3 MCOs and grouped these vulnerabilities into 4 security control areas.

Configuration of Network Devices—24 Vulnerabilities Identified

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

We identified 24 vulnerabilities related to configuration of network devices. For example, one MCO did not securely configure its router.[4] The router had a clear text protocol[5] enabled, which allowed network administrators to use passwords to access systems and applications and to monitor and manage network devices. An attacker monitoring this protocol would have been able to intercept and view data, such as passwords. Because network devices are integral to ensuring the security of the claims 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, such as ePHI.

Patch Management—Three Vulnerabilities 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 vulnerability remediations (patches) to all systems that have vulnerabilities, even for those systems that are not at immediate risk of exploitation.

We identified three vulnerabilities related to patch management. For example, one MCO did not have adequate procedures to ensure that software patches for its workstations were applied in a timely manner. Without adequate patch management, an attacker may be able to gain unauthorized access to ePHI and personally identifiable information on a network.

[4] A router is a device that connects two or more networks and forwards data between them.

[5] A protocol defines a language of rules and conventions for communications between network devices. Clear text is the unencrypted text or message in its human-readable form.

Antivirus Management—One Vulnerability Identified

Virus-scanning software should be provided at critical entry points, such as each desktop system on the network. Organizations must implement policies and procedures to protect ePHI from improper alteration or destruction.

We identified one vulnerability related to antivirus management. Specifically, one MCO did not follow its policy and procedures related to the timely updating of antivirus software on its desktop computers. Without an adequate antivirus management program, antivirus software may become out of date and no longer protect against current viruses.

Out-of-Date Software—One Vulnerability Identified

Software should be scanned and updated frequently to guard against known vulnerabilities. In addition to periodically looking for software vulnerabilities and fixing them, organizations should keep software current by establishing effective programs for patch management, virus protection, and other emerging threats. Organizations must implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network.

We identified one vulnerability related to out-of-date software. Specifically, one MCO did not have the latest version of an email program installed on its system. This version had a flaw that allowed man-in-the-middle attacks[6] and allowed remote attackers to bypass access restrictions. Without the latest versions of software installed, an organization is vulnerable to these types of attacks and attackers.

SECURITY MANAGEMENT

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The entitywide information security management program should establish a framework and continuous cycle for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without effective entitywide general controls, business process application-level controls may be made ineffective by circumvention or modification.

We identified 14 security management control vulnerabilities at the 3 MCOs and grouped these vulnerabilities into 4 security control areas.

[6] A man-in-the-middle attack is a form of eavesdropping on a network "conversation" between users in which an attacker impersonates one or both users and uses that information to do something malicious, such as obtaining sensitive information.

Contingency Planning—Five Vulnerabilities Identified

Contingency planning refers to interim measures to recover information technology services following an emergency or a system disruption. The contingency plan should be reviewed and updated regularly to ensure that new information is documented. Also, testing of the contingency plan should be conducted in an environment as close to an operating environment as possible, and every component of the plan, including the disaster recovery plan, should be tested to confirm the effectiveness of individual recovery procedures.

We identified five vulnerabilities related to inadequate contingency planning. For example, one MCO did not update its disaster recovery plan or perform system recovery tests at an alternate site. Without an updated contingency plan, employees would not know of the most current procedures. Without testing the contingency plan and having backups of systems and data stored offsite, continuity of operations could be adversely affected in the event of an unforeseen disaster.

Required System Security Plan Elements—Four Vulnerabilities Identified

System security plans should be formalized at the system and application levels for networks, facilities, and systems or groups of systems, as appropriate. These plans and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the State agency's computer system resources.

We identified four vulnerabilities related to system security plans, including both inadequate and nonexistent required security plan elements. For example, one MCO did not have a security plan and had not performed a security controls review of the claims processing system. Without a security plan, the Medi-Cal claims processing system may not be adequately secured. Without a periodic security controls review, significant risks to sensitive information may not be identified, and actions required to reduce risks may not be taken.

Sanitization of Data and Disposal of Devices—Three Vulnerabilities Identified

Organizations must track, document, and verify media sanitization[7] and disposal actions; test sanitization equipment and procedures to verify correct performance; and sanitize portable, removable storage devices, such as USB flash drives.

We identified three vulnerabilities related to sanitization of data and disposal of devices. For example, one MCO did not track, document, or verify that it had sanitized and disposed of various devices, such as USB flash drives. Without adequate controls, an organization may not be able to account for missing devices, and there is an increased risk of unauthorized access to ePHI.

[7] Sanitization refers to the general process of removing data so that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Background Checks—Two Vulnerabilities Identified

A background check must be performed before an individual is authorized to bypass significant technical and operational security controls and periodically thereafter.

We identified two vulnerabilities related to background checks. For example, one MCO did not have documentation to show that it performed background checks of two individuals, one of whom was the director of technology and security. Without performing adequate background checks, an organization runs the risk of hiring unqualified or untrustworthy individuals and allowing inappropriate access to and disclosure of confidential information, such as ePHI.

CONCLUSION

Our consolidated findings from the individual reports show significant vulnerabilities in the three MCOs' information systems and raise concerns about the integrity of the systems used to process Medicaid managed-care claims. The State agency informed us, in comments on the individual reports on the MCOs' information system general controls, that it was addressing these vulnerabilities. The fact that some of the same vulnerabilities were identified at all three MCOs suggests that other California Medi-Cal managed-care information systems may be similarly vulnerable. This summary report is intended to provide information to assist the State agency and CMS in strengthening MCOs' system security.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We grouped the high-risk security vulnerabilities from our previous reviews of information system general controls at three MCOs into three core categories of general controls: access controls, configuration management, and security management. All of the vulnerabilities presented in this summary report were noted in those reviews, which we performed from CYs 2012 to 2015.

METHODOLOGY

We conducted reviews of the information security general controls at the three MCOs in California 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 three MCOs varied; we did not review all of the security control areas at all three organizations. We conducted these reviews by observing information security operations, interviewing personnel, testing hardware and software configurations, and analyzing system security reports.

We conducted the three 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 three MCOs were the following:

- 45 CFR parts 95 and 164;
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources";
- NIST 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, version 2.0, *Creating a Patch and Vulnerability Management Program*;
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*;
- NIST SP 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*;
- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*;
- NIST SP 800-123, *Guide to General Server Security*; and
- FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*.