TEXAS HEALTH AND HUMAN SERVICES COMMISSION

OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Children's Medical Center Health Plan

December 20, 2019
OIG Report No. AUD-20-002

HHSC OIG
TEXAS HEALTH AND HUMAN SERVICES COMMISSION
OFFICE OF INSPECTOR GENERAL

WHY OIG CONDUCTED THIS AUDIT

CMC Health Plan (CMC), an affiliate of Children's Health System of Texas (CHST), provides Medicaid managed care to its members through the State of Texas Access Reform Kids (STAR Kids) program. As an affiliate of CHST, CMC shares information technology (IT) services and IT governance, including IT policy and security, through CHST Corporate Services.

The OIG Audit Division conducted this audit to assess the design and effectiveness, during state fiscal years 2018 and 2019, of (a) selected security controls over confidential HHS System information stored and processed by CMC and (b) business continuity and disaster recovery plans for selected activities related to the delivery of managed care services to HHSC members enrolled with CMC.

WHAT OIG RECOMMENDS

Medicaid and CHIP Services (MCS) should require CMC to:

- (a) disable accounts that have been inactive for more than 90 days, (b) remove user accounts for terminated employees, and (c) periodically review user accounts.
- Enforce approval requirements before granting access to HHS System information.
- Ensure its risk management plan reflects the current information operating system and updates the assessment and plan.
- Improve control activities for documenting baseline configurations for network devices that store and process confidential HHS System information.

For more information, contact:
OIG.AuditDivision@hhsc.state.tx.us

December 20, 2019

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Children's Medical Center Health Plan

WHAT OIG FOUND

Children's Medical Center (CMC) is required to protect and secure confidential HHS System information, such as claims data, in accordance with requirements established in the HHS Information Security Standards and Guidelines (ISSG) through August 31, 2018, and in HHS Information Security Controls (IS-Controls) starting September 1, 2018.

CMC complied with IS-Controls requirements related to the following security control areas: information system monitoring, physical security, systems and communication protection, system and information integrity, incident response, and ensuring the workforce completed security awareness training.

CMC also complied with requirements related to business continuity and disaster recovery planning. The plans were designed to sustain continued operations, including claims processing and the provision of services to providers and members during an emergency event.

CMC did not always comply with IS-Control requirements for user account management and risk management. Specifically, CMC did not:

- Effectively manage user access to information systems that contained confidential HHS System information by timely disabling user accounts in CMC's claims processing and care coordination application after 90 days for non-privileged accounts.
- Ensure access to systems had been authorized by responsible management or immediately disable accounts of terminated users.
- Conduct an annual internal risk assessment to identify the risks and vulnerabilities associated with management information systems and to implement appropriate controls.

The OIG Audit Division also determined that the security plan submitted by CMC and approved by HHS IT did not contain sufficient details supporting implementation of security controls to protect confidential HHS System information.

MCS and CMC concurred with the OIG Audit Division on issues identified and recommendations outlined in this report. In its management response, MCS indicated it will coordinate with HHSC IT and require CMC to address issues identified in this report.

TABLE OF CONTENTS

INTRODUCTION

The Texas Health and Human Services Commission (HHSC) Office of Inspector General (OIG) Audit Division conducted an audit of security controls over confidential Health and Human Services (HHS) System information at Children's Medical Center Health Plan (CMC). CMC, an affiliate of Children's Health System of Texas (CHST), provides Medicaid managed care to its members through the State of Texas Access Reform Kids (STAR Kids) program. As an affiliate of CHST, CMC shares information technology (IT) services and IT governance, including IT policy and security, through CHST Corporate Services.

The OIG Audit Division conducted the audit to determine whether confidential HHS System information in the custody of CMC and its subcontractors was protected from unauthorized access, loss, or disclosure.

Unless otherwise described, any year referenced is the state fiscal year, which covers the period from September 1 through August 31.

Objective and Scope

The audit objectives were to assess the design and effectiveness of:

- Selected security controls over confidential HHS System information stored and processed by CMC.

- Business continuity and disaster recovery plans for selected activities related to the delivery of managed care services to Medicaid STAR Kids members enrolled with CMC.

The audit scope included, for 2018 and 2019:

- IT controls for logical security implemented to protect access to:
  - Active Directory, which controls access to the network and operating system.
  - Cognizant TriZetto QNXT (QNXT), CMC's claims processing and care coordination application.
  - Databases associated with QNXT and business intelligence reporting system.
- System security and risk management plans.
- Security of data in transit and stored.
- Incident response, information system monitoring, and security training.
- Physical security of the IT infrastructure.
- General controls supporting systems backup, contingency planning, and recovery activities.

Background

CMC coordinates health services for members[1] in the Medicaid STAR, STAR Kids, and CHIP programs, and supports provider (a) claims processing and (b) benefit administration. CMC supports its Medicaid and CHIP operations through its IT infrastructure, including Active Directory[2] and IT applications, including QNXT, and HealthX.

- Active Directory is a network service used to authenticate CMC's workforce access to IT applications.
- QNXT is an application used to adjudicate and store provider claims information and to support care coordination.
- HealthX is a web portal that provides explanations of benefits (EOB) to CMC providers and members.

CMC's workforce, including employees and subcontractors, are authenticated to the network by Active Directory. When working remotely, access to the network is further secured via a virtual private network (VPN) connection. Once authenticated on the network, authorized users can access the QNXT application. CMC utilizes a single sign-on[3] solution for accessing network applications including QNXT.

CMC's primary and secondary data centers are in Texas. The primary data center provides the IT infrastructure for CMC. Claims information is stored on a QNXT SQL database and replicated hourly to the secondary data center. The secondary data center provides a redundant failover backup for both CHST and CMC.

Additionally, the QNXT SQL database performs backups nightly and is automatically restored to (a) a report server utilized for business intelligence reporting and (b) the secondary data center for backup and recovery purposes.

CMC receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP), the Availity clearinghouse, and other third parties through secure file transfers. CMC provides EOBs to members and providers through the HealthX web portal.

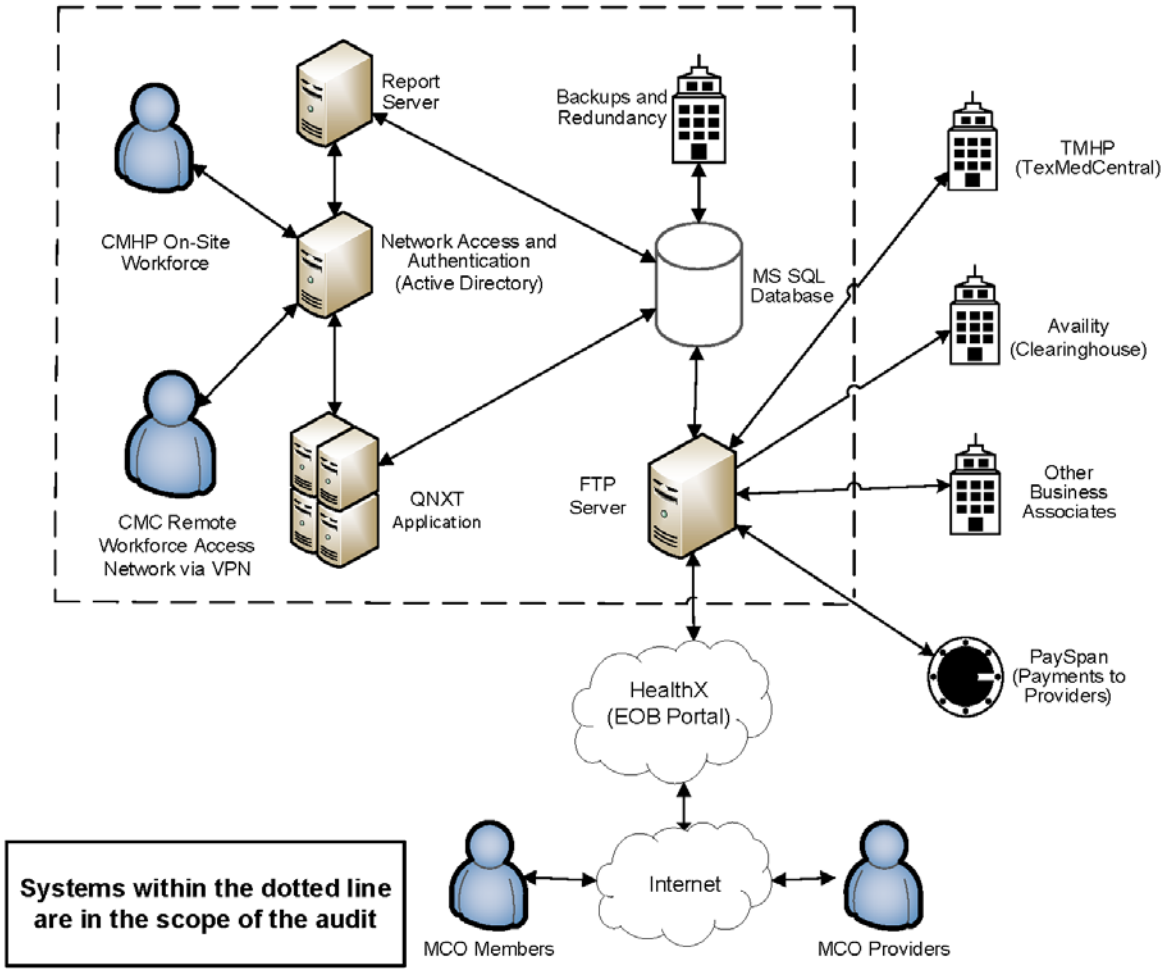
Figure A illustrates the systems and processes.

[1] A "member" is an individual who is enrolled with a state contracted Medicaid or CHIP MCO as a subscriber or dependent.

[2] "Active Directory" is a network authorization and authentication service utilized by Windows operating systems.

[3] "Single sign-on" allows a single authentication to provide access to multiple applications by passing the authentication token seamlessly to configured applications.

Figure A: CMC Systems Diagram



Source: OIG Audit Division

The OIG Audit Division examined the QNXT application and the associated infrastructure, operating system, and database that process and store claims detail information.

CMC's data centers provide the facility and IT infrastructure for the QNXT application. The OIG Audit Division performed a physical security review at both the primary and secondary data centers and evaluated the business continuity and disaster recovery plans for readiness in the event of a federal or state-declared disaster or other operational disruptions.

Medicaid and CHIP Services (MCS), HHSC IT, and CMC share accountability for safeguarding confidential HHS System information from accidental or unauthorized access, loss, or disclosure. The Uniform Managed Care Contract (UMCC) provides the terms and conditions to which each MCO must adhere in order to conduct business in Texas. The UMCC requires MCOs to submit a set of management information system (MIS) deliverables to MCS. MIS deliverables

include business continuity plan, disaster recovery plan joint interface plan, risk management plan, systems quality assurance plan, and a security plan. The plans are submitted annually for HHSC's review and approval.[4] The security plan contains data classifications and security control baselines sufficient to protect the information systems processing and storing the data.[5] The final security baseline is documented in the security plan. Security control baselines must follow guidance provided in HHS Information Security Controls (IS-Controls),[6] which is based on the National Institute of Standards and Technology security standards.

The OIG Audit Division applied criteria from IS-Controls and CMC's security policies and procedures and business continuity and disaster recovery plans to develop audit tests to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by CMC. HHS Information Security office has classified the MCO systems that process and store confidential HHS system information as requiring the IS-Controls baseline of "Moderate" with a HIPAA requirement overlay. Therefore, the audit work performed only tested moderate IS-Controls requirements.

Methodology

The OIG Audit Division reviewed key security controls protecting confidential HHS System information in the custody of CMC, primarily the QNXT application. Table 1 identifies the key control areas and the associated control groups tested during the audit. Control groups are the IS-Controls–defined groupings of baseline security controls. Each control group contains multiple control baselines, which can be layered based on data risks, to provide customized controls for information security.

[4] Uniform Managed Care Manual, Consolidated Deliverables Matrix, v. 2.5 (Mar. 1, 2017) and v. 2.6 (Apr. 15, 2019).

[5] HHS Information Security Controls § 2.1.3, v. 1.0 (Feb. 9, 2018).

[6] HHS Information Security Controls § 2.1.4, v. 1.0 (Feb. 9, 2018).

Table 1: Key Control Areas and Control Groups

Key Control Areas Selected for Audit	IS-Controls Groups	Issue Number
User Account Management	Access Controls (AC) Identification and Authentication (IA) Personnel Security (PS)	1.1, 1.2
Workforce Training	Awareness and Training (AT)	N/A
Information Security Oversight	Audit and Accountability (AU) Security Assessment and Authorization Controls (CA) Planning (PL)	4
Configuration Management	Configuration Management (CM) Systems and Communications Protection (SC)	3
Business Continuity and Disaster Recovery Planning	Contingency Planning (CP)	N/A
Information Systems Monitoring	Incident Response (IR)	N/A
Risk Management	Risk Assessment (RA)	2
Physical Security	Physical and Environmental Protection Controls (PE) Media Protection (MP)	N/A

Source: Prepared by the OIG Audit Division based on IS-Controls

An overview of all control areas tested in this audit is presented in Appendix A. The OIG Audit Division examined the IT security controls and relevant activities supporting data security at CMC by (a) reviewing policies and procedures in detail to gain an understanding of the design of controls, (b) visiting CMC to interview key personnel, (c) observing security controls and the physical protection of assets, and (d) testing the effectiveness of key controls designed to protect or recover information processed and stored by CMC.

The OIG Audit Division presented audit results, issues, and recommendations to MCS and to CMC in a draft report dated October 17, 2019. Each was provided with the opportunity to study and comment on the report. The MCS management responses to the audit recommendations contained in the report are included in the report following each recommendation.

MCS concurred with the OIG Audit Division recommendations outlined in this report and will coordinate with HHSC IT and require CMC to address issues identified in this report.

Criteria

The OIG Audit Division used the following criteria, which were in effect during the scope of the audit, to evaluate the information provided:

- 1 Tex. Admin. Code, § 202.1 and § 202.3 and Subchapter B (2015) and (2016)
- Uniform Managed Care Contract, v. 2.24 (2017) through v. 2.26 (2018)
- STAR Kids Contract, v. 1.5 (2017) through v. 1.6 (2018)
- HHS Information Security Standards and Guidelines Controls Catalog (ISSG), v. 6 (2015)
- HHS Information Security Controls (IS-Controls), v. 1.0 (2018)

Beginning on September 1, 2018, CMC was required to follow IS-Controls, which replaced the HHS Information Security Standards and Guidelines (ISSG). The OIG Audit Division focused the security controls and recommendations in the report on compliance with IS-Controls standards. The IS-Controls system categorization process designates the systems in this review as moderate.

Auditing Standards

GAGAS

The OIG Audit Division conducted this audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the issues and conclusions based on our audit objectives. The OIG Audit Division believes the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

ISACA

The OIG Audit Division performs work in accordance with the IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals published by ISACA.

AUDIT RESULTS

CMC complied with IS-Control requirements related to workforce training, information system monitoring, and physical security.

CMC also complied with ISSG and IS-Control requirements related to business continuity and disaster recovery planning. Since a review of CMC business continuity and disaster recovery plans for operations relating to the processing and storage of confidential HHS System information by CMC was a specific objective of this audit, further details follow.

Business continuity and disaster recovery planning are part of the contingency planning control group. Contingency planning involves establishing, maintaining, and effectively implementing plans for emergency response, backup operations, and post-disaster recovery to ensure the availability of critical information resources and continuity of operations in the event of an emergency or other business disruption. Additionally, the UMCC requires that MCOs have plans in place to provide member services and process claims should disasters interrupt normal business.[7] CMC's business continuity and disaster recovery planning and related activities specific to claims processing, member services, and supporting functions, are summarized below.

Policies

CMC maintained, and periodically reviewed and updated, contingency planning policies and procedures that address the purpose, scope, roles, responsibilities, and management commitment to ensure the continuation of business practices.

Plans

CMC maintained, and periodically reviewed and updated, business continuity and disaster recovery plans. Additionally, CMC plans included processes to, during emergency and disaster events, (a) ensure members have access to managed care services, (b) process prior authorizations, and (c) allow claim-processing exceptions by specific locations.

Training

CMC annually trained personnel on their responsibilities during a disaster.

[7] Uniform Managed Care Contract, Attachment B-1, § 8.1.29, v. 2.24 (Sept. 1, 2017) through v. 2.28 (Mar. 1, 2019).

Testing

CMC tested its business continuity and disaster recovery plans annually and updated its plans based on results.

Offsite Storage

CMC maintains a mirror image of its production environment in a secondary data center in Austin, Texas.

Alternate Processing Site

CMC maintains alternate processing sites, including office space at the CHST corporate headquarters.

Alternate Telecommunications Site

A secondary call center provides CMC with the capability to maintain member services and provider support in the event the primary call center is unable to operate.

Information System Backup

CMC conducted backups of key operating systems every 60 minutes. Backups were tested periodically and were available for restoration to production in the event of loss or corruption during an emergency.

There were exceptions related to IS-Controls requirements related to:

- User Account Management
- Configuration Management
- Risk Management
- Information Security Oversight

USER ACCOUNT MANAGEMENT

User account management consists of procedures to request, establish, suspend, modify, and deactivate access to systems and confidential information. The procedures apply to all account types, including application end users, system administrators, and other privileged accounts assigned to both internal and external users. Access controls limit access to systems and applications. Access is restricted to authorized users, and authorized users are further limited to the types of transactions and functions the users may perform. Personnel security includes access controls related to approving and terminating user account roles and privileges, periodic user account reviews, disabling inactive accounts, disabling

accounts for terminated users, and locking user accounts for excessive unsuccessful logon attempts.

Disabling Inactive and Terminated Users Accounts

Inactive accounts are accounts that have not been accessed for a period, which indicates a user's access to an application may not be needed. IS-Controls requires information systems automatically disable non-privileged accounts after 90 days.[8]

Issue 1.1: CMC Failed to Disable Inactive and Terminated User Accounts

CMC did not disable inactive accounts in QNXT after 90 days for non-privileged users. Additionally, terminated users were not always timely removed.

According to CMC system-generated reports of last logon activity, 13 QNXT non-privileged user accounts were not disabled after 90 days of inactivity. Of the 13, four accounts belonged to terminated employees whose access should have been removed immediately upon termination.[9]

CMC did not periodically review user accounts in QNXT for inactivity and relied upon the deactivation of Active Directory network accounts to prevent access to the QNXT application.

Disabled Active Directory accounts reduce the risk that a terminated individual could continue to access QNXT. However, the risk that an internal user could exploit unused active accounts remains. Failure to disable inactive and terminated user accounts within QNXT places confidential HHS System information at risk of being viewed, modified, or deleted without authorization.

Recommendation 1.1

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel CMC to implement control processes to (a) disable non-privileged accounts that been inactive for more than 90 days, (b) remove user accounts for terminated employees, and (c) perform periodic reviews of user accounts for all systems and applications that create, process, transfer, or store confidential HHS System information.

[8] HHS Information Security Controls, Appendix B, AC-02(03), v. 1.0 (Feb. 9, 2018).

[9] HHS Information Security Controls, Appendix B, PS-04, v. 1.0 (Feb. 9, 2018).

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require CMC to implement control processes to (a) disable non-privileged accounts that been inactive for more than 90 days, (b) remove user accounts for terminated employees, and (c) perform periodic reviews of user accounts for all systems and applications that create, process, transfer, or store confidential HHS System information.

MCS will allow CMC 20 business days from receipt of the final audit report to submit a corrective action plan (CAP).

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP as HHSC IT.

Responsible Managers

Director, Managed Care Compliance and Operations
Director, IT Medicaid and CHIP Systems

Target Implementation Date

May 30, 2020

User Account Provisioning

Account provisioning processes are control standards to ensure only appropriate, authorized end users have access to information systems. Provisioning controls include requiring (a) defined personnel approve requests to create information system accounts, (b) established conditions for roles, such as job responsibilities, and (c) notification processes for accounts that are no longer required.[10]

Issue 1.2: CMC Did Not Have an Effective Process for Provisioning User Accounts

CMC did not consistently (a) maintain documentation to demonstrate authorization of account privileges and roles prior to granting access to members based on their position within the organization or (b) deactivate QNXT accounts upon termination of employment.

For one of five sampled employees hired during the scope of the audit, the CMC Access Request Form was not signed by an individual authorized to approve access. For a second employee in the sample, a signed CMC Access Request Form was not provided at all.

Additionally, for five sampled terminated employees, a CMC Access Request Form did not indicate specific applications or reference access roles and user responsibilities from which to remove access, as required by IS-Controls.[11] The notification of employee termination through the CMC Access Request Form only triggered the termination of the network Active Directory account.

IS-Controls requires that account creation and access be authorized and approved by defined personnel.[12] CMC policy states procedures to obtain approval for access to information shall include authorization from someone in the same department who is at least a team leader, supervisor, or manager and at least one level above the requestor.[13]

CMC did not follow policy and processes consistently in all sampled cases. Failing to require managerial approval before granting user access to HHS System information may place confidential HHS Information at risk of being viewed, modified, or deleted without authorization. Termination requests that do not indicate relevant accounts, roles, or privileges assigned to a user may result in accounts with access to HHS System information not being timely deactivated, and

[10] HHS Information Security Controls, Appendix B, AC-02, v. 1.0 (Feb. 9, 2018).

[11] HHS Information Security Controls, Appendix B, AC-02, v. 1.0 (Feb. 9, 2018).

[12] HHS Information Security Controls, Appendix B, AC-02, v. 1.0 (Feb. 9, 2018).

[13] Children's Health System Policy: Access Control, Policy AD9.16 User Provisioning, (Nov. 1, 2010).

may result in subsequent unauthorized access, modification, or deletion of confidential information.

Recommendation 1.2

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel CMC to consistently enforce managerial approval requirements before granting access to HHS System information and update procedures to ensure accounts are deactivated upon termination.

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require CMC to consistently enforce managerial approval requirements before granting access to HHS System information and update procedures to ensure accounts are deactivated upon termination.

MCS will allow CMC 20 business days from receipt of the final audit report to submit a corrective action plan (CAP).

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP as HHSC IT.

Responsible Managers

Director, Managed Care Compliance and Operations
Director, IT Medicaid and CHIP Systems

Target Implementation Date

May 30, 2020

RISK ASSESSMENT

Risk assessment is a structured and systematic process to identify potential security weaknesses and analyze the impact to the confidentiality, integrity, and availability of information in the event a weakness was exploited.

As part of an effective risk management program, CMC was required to: [14]

- Assess risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits.

- Document risk assessment results in the applicable security plan.

- Review risk assessment results in accordance with the IS-Controls implementation requirements:

  - On an annual basis, the information owner will:
    - Review the compliance status of all security and privacy controls required per the system categorization of the information system.
    - Ensure required vulnerability scans are conducted.
    - Document the current implementation status of the controls in the security plan.

  - When significant changes are made to the system or environment of operation (including identification of new threats and vulnerabilities) or other conditions that may threaten the security of the system, the information owner will:
    - Complete a full review for compliance of all affected security and privacy controls required, per the system categorization.
    - Document the current implementation status of the controls in the security plan. Ensure required vulnerabilities scans are conducted.
    - Receive a new security authorization prior to moving the significant changes to production.

- Disseminate risk assessment results to applicable senior officials.

- Update its risk assessment according to implementation requirements.

The risk assessment drives the approach to risk mitigation strategies intended to reduce risk to an acceptable level. For risks identified, management may choose to

[14] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 RA-3, (Sept. 21, 2015) and HHS Information Security Controls, Appendix B, RA-03, v. 1.0 (Feb. 9, 2018).

implement controls to mitigate or reduce risk, take no action and accept the risk, or outsource the risk to another organization.

UMCC requires CMC to submit, for HHS IT review and approval, a risk management plan.[15] Additionally, HHS IT utilizes a checklist to evaluate the risk management plan. A key component of the risk management plan is the information systems risk assessment to categorize applications and the information contained.

Issue 2: CMC Did Not Conduct an Annual Risk Assessment

CMC did not conduct an annual internal risk assessment in 2018 or 2019. CMC engaged a third-party consultant to assess IT systems in 2017; however, the assessment was incomplete and did not address the risks, likelihoods, and impacts for information systems.

ISSG and IS-Controls require the organization to conduct an annual assessment of risk, including the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it process and stores.[16] The assessment of risk is documented in the security plan and provides the basis for applying security and privacy controls.

Without an annual internal risk assessment that reflects the current environment, CMC may not be aware of potential risks or vulnerabilities, and, as a result, could fail to implement appropriate mitigation strategies to protect the confidentiality and integrity of confidential HHS System information.

Recommendation 2

MCS, through its contract oversight responsibilities, should require CMC to conduct and maintain an annual internal risk assessment for ensuring its risk management plan reflects the current information operating system and updates the assessment and plan.

[15] Uniform Managed Care Contract, Attachment A, § 8.1.18.2, v. 2.24 (Sept. 1, 2017) through v. 2.26 (Sept. 1, 2018).

[16] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 RA-3, (Sept. 21, 2015) and HHS Information Security Controls, Appendix B, RA-03, v. 1.0 (Feb. 9, 2018).

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require CMC to conduct and maintain an annual internal risk assessment for ensuring its risk management plan reflects the current information operating system and updates the assessment and plan.

MCS will allow CMC 20 business days from receipt of the final audit report to submit a corrective action plan (CAP).

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP as HHSC IT.

Responsible Managers

Director, Managed Care Compliance and Operations
Director, IT Medicaid and CHIP Systems

Target Implementation Date

May 30, 2020

CONFIGURATION MANAGEMENT

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. One key component of configuration management is baseline configurations.

Baseline configurations serve as a basis for future builds, releases, or changes to information systems. Baseline configurations include information about information system components, network topology, and the local placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organization information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Issue 3: CMC Did Not Maintain Baseline Configurations for Servers that Stored Confidential HHS System Information

CMC did not maintain documented baseline configurations for its servers containing HHS information. IS-Controls requires the organization to develop, document, and maintain a current baseline of the information system's configuration controls.[17]

Documented server configurations are an essential component to minimize system security weaknesses, develop repeatable server builds, implement efficient change management, and assist in troubleshooting security events or incidents. Documented baseline configuration settings for new server installations and server rebuilds help ensure that services, ports, and default accounts, once implemented, are appropriately maintained to protect confidential HHS System information and can be replicated in the event settings are inadvertently changed or lost.

CMC stated that it was in the process of establishing system configuration baselines, but previously utilized the baselines as provided by the software and hardware vendors. Because it did not maintain baseline configurations, CMC may deploy servers that do not meet security standards and may be unable to efficiently and effectively replace existing hardware or recover from a security incident.

Recommendation 3

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should require CMC to improve control activities for documenting baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require CMC to improve control activities for documenting baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

MCS will allow CMC 20 business days from receipt of the final audit report to submit a corrective action plan (CAP).

[17] HHS Information Security Controls, Appendix B, CM-02, v. 1.0 (Feb. 9, 2018).

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP as HHSC IT.

Responsible Managers

Director, Managed Care Compliance and Operations
Director, IT Medicaid and CHIP Systems

Target Implementation Date

May 30, 2020

INFORMATION SECURITY OVERSIGHT

Effective information security oversight requires ongoing coordination between MCS and HHS IT to provide adequate review and approval of the security plan and associated annual deliverables. Oversight coordination is essential to allow each department to provide knowledge and expertise in the review and approval of security plans and ensure CMC complies with state, HHS System, and contractual obligations for the protection of confidential HHS System information.

UMCC requires CMC to submit a security plan annually.[18] MCS, as the contract manager, collaborates with the HHS Information Security Officer to evaluate whether the security plan submitted by CMC is complete in accordance with the system security plan requirements.

Issue 4: Approved CMC Security Plan Did Not Contain All Required Information

The security plan submitted by CMC as part of the UMCM MIS deliverables did not identify the IS-Controls implemented to protect data as required.

CMC submitted the security plan and other required deliverables for 2018 and 2019. The deliverables were reviewed and accepted by HHS IT. IS-Controls requires that CMC identify and, based on security categorization, describe the security controls in place to comply with the control requirements, including a rationale for the tailoring and supplementation decisions.[19]

[18] Uniform Managed Care Contract, Attachment A, § 8.1.18.2, v. 2.24 (Sept. 1, 2017) through v. 2.26 (Sept. 1, 2018).

[19] HHS Information Security Controls, § 2.3; and Appendix B, PL-02, v. 1.0 (Feb. 9, 2018).

The review process for MIS deliverables did not detect the absence of the security control requirements, nor was CMC required to modify and resubmit security plans containing the necessary controls.

Three prior OIG audit reports included similar issues related to oversight and review of MIS deliverables. HHS IT and MCS created action plans to remediate deficiencies; however, according to HHS IT, organizational changes have delayed implementation of the action plans. HHS IT and MCS have indicated that process improvements will be completed and available by 2021.

Recommendation 4

MCS should continue efforts to coordinate with HHS IT to improve the review process of annual MIS deliverables within established timelines.

Management Response

Action Plan

As noted in the report, HHS IT and MCS worked together to create action plans to remediate deficiencies with MCO's security plans and associated deliverables. These process improvements are expected to be implemented in FY 2021.

Until that time, HHS IT has updated the review process for the security plans. HHS IT will review for each NIST control being named for the FY 2020 deliverables and future deliverables until the new security policies are implemented.

Responsible Managers

Director, Managed Care Compliance and Operations
Director, IT Medicaid and CHIP Systems

Target Implementation Dates

October 2019: Complete revision of Security Plan Checklist
January 2020: Implementation of new review processes for security plans

CONCLUSION

The OIG Audit Division completed an audit of selected security controls over confidential HHS System information in the custody of CMC. The audit included an evaluation of IT security controls over the care coordination and claims processing application, QNXT, and the operating environment. The OIG Audit Division conducted a site visit at CMC in April 2019.

The OIG Audit Division concluded:

- CMC complied with ISSG and IS-Controls requirements related to workforce training, business continuity and disaster recovery planning, information system monitoring, and physical security.
- CMC did not effectively manage user access to information systems that contained confidential HHS System information by timely disabling user QNXT accounts after 90 days for non-privileged accounts.
- CMC did not consistently provision user accounts based on the established control processes.
- CMC did not conduct an annual internal risk assessment to identify the risks and vulnerabilities associated with MIS and to implement appropriate controls.
- MCS processes were not effective to ensure a sufficient review of security plans provided by CMC.

The OIG Audit Division offered recommendations, which, if implemented, will result in CMC having:

- Strengthened controls over user accounts with access to confidential HHS System information.
- Improved understanding of the inherent risks and vulnerabilities of the IT infrastructure and security, and enhanced reporting of efforts to mitigate discovered and known risks to stakeholders.
- Improved oversight of organization activities relating to the security of HHS System information.

The OIG Audit Division thanks the management and staff of MCS, HHS Information Systems Security, and CMC for their cooperation and assistance during this audit.

Appendix A: Controls Tested

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
Access Control (AC)			
AC-01	Access Control Policy and Procedures		N/A
AC-02	Account Management	CD, CE	1.1 and 1.2
AC-03	Access Enforcement		N/A
AC-06	Least Privilege		N/A
Audit and Accountability(AU)			
AU-01	Audit and Accountability Policy and Procedures		N/A
AU-02	Audit Events		N/A
Awareness and Training (AT)			
AT-01	Security Awareness Training Policy and Procedures		N/A
AT-02	Security Awareness Training		N/A
Security Assessment and Authorization Control (CA)			
CA-01	Security Assessment and Authorization Policy and Procedures		N/A
CA-02	Security Assessments		N/A
CA-03	System Interconnections		N/A
Configuration Management (CM)			
CM-01	Configuration Management Policy and Procedures		N/A
CM-02	Baseline Configuration	CD, CE	3
CM-10(01)	Open Source Software		N/A
Contingency Planning (CP)			
CP-01	Contingency Planning Policy and Procedures		N/A
CP-02	Contingency Plan		N/A
CP-03	Contingency Training		N/A
CP-04	Contingency Plan Testing		N/A
CP-06	Alternate Storage Site		N/A
CP-07	Alternate Processing Site		N/A
CP-08	Telecommunications Services		N/A
CP-09	Information System Backup		N/A
Identification and Authentication (IA)			
IA-01	Identification and Authentication Policy and Procedures		N/A
IA-02	Identification and Authentication [Organization Users]		N/A
IA-05	Authenticator Management		N/A

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
IA-08	Identification and Authentication [Non-organizational Users]		N/A
Incident Response (IR)			
IR-01	Incident Response Policy and Procedures		N/A
IR-02	Incident Response Training		N/A
IR-03	Incident Response Testing		N/A
IR-08	Incident Response Plan		N/A
Media Protection (MP)			
MP-06	Media Sanitization		N/A
Physical and Environmental Protection Controls (PE)			
PE-01	Physical and Environmental Protection Policy and Procedure		N/A
PE-02	Physical Access Authorization		N/A
PE-03	Physical Access Control		N/A
Planning Controls (PL)			
PL-01	Security Planning Policy and Procedures		N/A
PL-02	System Security Plan	CD, CE	4
Personnel Security (PS)			
PS-04	Personnel Termination	CD, CE	1.1
Risk Assessment Control (RA)			
RA-01	Risk Assessment Policy and Procedures		N/A
RA-02	Security Categorization		N/A
RA-03	Risk Assessment	CE	2
RA-05	Vulnerability Scanning		N/A
System and Information Integrity (SI)			
SC-01	System and Communications Protection Policy and Procedures		N/A
SC-08	Transmission Confidentiality and Integrity		N/A
SC-28	Protection of Information at Rest		N/A
Systems and Communications Protection (SC)			
SI-01	System and Information Integrity Policy and Procedures		N/A
SI-04	Information System Monitoring		N/A
SI-05	Security Alerts, Advisories, and Directives		N/A

Appendix B: Report Team and Distribution

Report Team

OIG staff members who contributed to this audit report include:

- Audrey O'Neill, CIA, CFE, CGAP, Deputy IG for Audit
- Kacy VerColen, CPA, Interim Assistant Deputy IG for Audit
- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Melissa Larson, CIA, CISA, CFE, IT Audit Manager
- Daniel Graf, CISA, IT Project Manager
- Carolyn Cadena, Staff Auditor
- Mo Brantley, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Dr. Courtney N. Phillips, Executive Commissioner
- Cecile Erwin Young, Chief Deputy Executive Commissioner
- Victoria Ford, Chief Policy Officer
- Karen Ray, Chief Counsel
- Nicole Guerrero, Director of Internal Audit
- Stephanie Muth, State Medicaid Director, Medicaid and CHIP Services
- Grace Windbigler, Director, Managed Care Compliance and Operations, Medicaid and CHIP Services
- Ricardo Blanco, Interim Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Ivan Hovey, Director, HHSC IT Applications
- Thuy Cao, HHS Chief Information Security Officer
- P. J. Fritsche, HHSC IT Director, Medical and Social Services Applications

Children's Medical Center Health Plan

- Doris Hunt, Executive Director Health Plan
- Joshua Malone, Director of Compliance

Appendix C: OIG Mission, Leadership, and Contact Information

The mission of OIG is to prevent, detect, and deter fraud, waste, and abuse through the audit, investigation, and inspection of federal and state taxpayer dollars used in the provision and delivery of health and human services in Texas. The senior leadership guiding the fulfillment of OIG's mission and statutory responsibility includes:

- Sylvia Hernandez Kauffman, Inspector General
- Susan Biles, Chief of Staff
- Dirk Johnson, Chief Counsel
- Christine Maldonado, Chief of Operations and Workforce Leadership
- Quinton Arnold, Chief of Inspections and Investigations
- Steve Johnson, Chief of Medicaid Program Integrity

To Obtain Copies of OIG Reports

- OIG website: https://oig.hhsc.texas.gov/reports

To Report Fraud, Waste, and Abuse in Texas HHS Programs

- Online: https://oig.hhsc.texas.gov/report-fraud
- Phone: 1-800-436-6184

To Contact OIG

- Email: OIGCommunications@hhsc.state.tx.us
- Mail: Texas Health and Human Services Commission
  Office of Inspector General
  P.O. Box 85200
  Austin, Texas 78708-5200
- Phone: 512-491-2000