

TEXAS HEALTH AND HUMAN SERVICES COMMISSION
OFFICE OF INSPECTOR GENERAL
AUDIT REPORT

**SECURITY CONTROLS OVER
CONFIDENTIAL HHS SYSTEM
INFORMATION AND BUSINESS
CONTINUITY AND DISASTER
RECOVERY PLANS**

Texas Children's Health Plan



July 31, 2019
OIG Report No. AUD-19-025



HHSC OIG

TEXAS HEALTH AND HUMAN
SERVICES COMMISSION
OFFICE OF
INSPECTOR GENERAL

WHY OIG CONDUCTED THIS AUDIT

Texas Children's Health Plan (TCHP) is a licensed managed care organization (MCO) that contracts with the State of Texas to provide Medicaid and Children's Health Insurance Program (CHIP) services through its network of providers. TCHP processes and pays Medicaid and CHIP managed care provider claims, which contain confidential data, including protected health information. TCHP is required to protect and secure confidential Health and Human Services (HHS) System information, such as claims data.

The OIG Audit Division conducted this audit to assess the design and effectiveness, during state fiscal year 2018, of (a) selected security controls over confidential HHS System information stored and processed by TCHP and (b) business continuity and disaster recovery plans for operations relating to the processing and storage of confidential HHS System information by TCHP.

WHAT OIG RECOMMENDS

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

- Perform required reviews to determine whether access, roles, and privileges granted to users are appropriate and make adjustments as needed.
- Automatically disable accounts which have been inactive for more than 90 days.
- Immediately disable terminated user accounts.
- Strengthen its account lockout policy and configurations.
- Conduct required vulnerability scans and timely remediate identified vulnerabilities.

For more information, contact:

OIG.AuditDivision@hhsc.state.tx.us

July 31, 2019

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION AND BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

Texas Children's Health Plan

WHAT OIG FOUND

TCHP complied with HHS Information Security Standards and Guidelines (ISSG) requirements related to workforce training, information security oversight, configuration management, and information systems monitoring.

TCHP also complied with ISSG requirements related to business continuity and disaster recovery planning, with plans designed to ensure continued operations and provision of services to providers and members during incidents. TCHP was able to sustain claims processing, member services, and provider support functions during the Hurricane Harvey event in 2017, and conducted a post-event analysis that identified further improvement opportunities.

TCHP did not always comply with ISSG requirements for user account management and risk management. Specifically, TCHP did not:

- Perform annual reviews of user accounts and associated roles and permissions to ensure access to systems were appropriate and justified.
- Disable all inactive accounts after 60 days of inactivity for privileged accounts and 90 days for non-privileged accounts.
- Immediately disable user accounts of terminated employees.
- Enforce requirements for locking user accounts when unsuccessful logon attempts occurred.

TCHP did not meet ISSG requirements for password configuration settings. However, effective September 1, 2018, HHS Information Security Controls (IS-Controls) replaced ISSG and TCHP met the new IS-Controls standard for compliance.

TCHP did not conduct routine vulnerability scans in accordance with ISSG requirements until April 2018. At the time of the audit, TCHP was in the process of remediating identified vulnerabilities and had started conducting scans of its IT system.

TCHP is required to protect and secure confidential HHS System information, such as claims data, in accordance with requirements established in the ISSG through August 31, 2018, and in IS-Controls starting September 1, 2018.

MCS concurred with the OIG Audit Division recommendation outlined in this report and will coordinate with HHSC IT and require TCHP to address issues identified in this report. TCHP agreed with some of the issues and indicated disagreement with others. Auditor comments follow the TCHP comment letter.

TABLE OF CONTENTS

INTRODUCTION	1
AUDIT RESULTS	7
USER ACCOUNT MANAGEMENT	9
Access Controls	
<i>Issue 1.1: TCHP Did Not Review User Accounts for Appropriateness</i>	<i>10</i>
<i>Issue 1.2: TCHP Did Not Timely Disable Inactive Accounts</i>	<i>12</i>
<i>Issue 1.3: TCHP Did Not Disable the User Accounts of Some Terminated Employees and Contractors</i>	<i>15</i>
<i>Issue 1.4: TCHP Did Not Lock User Accounts After Multiple Unsuccessful Logon Attempts</i>	<i>17</i>
Identification and Authentication	
<i>Issue 2: TCHP Did Not Enforce Password Requirements</i>	<i>19</i>
RISK MANAGEMENT	20
<i>Issue 3: TCHP Did Not Conduct Vulnerability Scans Until April 2018 and Did Not Remediate Identified Vulnerabilities.....</i>	<i>21</i>
CONCLUSION.....	24
APPENDICES	26
A: <i>Controls Tested.....</i>	<i>26</i>
B: <i>Texas Children’s Health Plan Comment Letter</i>	<i>28</i>
C: <i>Report Team and Distribution</i>	<i>31</i>
D: <i>OIG Mission, Leadership, and Contact Information</i>	<i>33</i>

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 Texas Children's Health Plan (TCHP). TCHP is a licensed managed care organization (MCO) that contracts with the State of Texas to provide Medicaid and Children's Health Insurance Program (CHIP) services through its network of providers. TCHP processes and pays Medicaid and CHIP managed care provider claims, which contain confidential data, including protected health information. TCHP is required to protect and secure confidential HHS System information, such as claims data.

The OIG Audit Division conducted the audit to determine whether confidential HHS System information in the custody of TCHP 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.

Objectives 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 TCHP.
- Business continuity and disaster recovery plans for operations relating to the processing and storage of confidential HHS System information by TCHP.

The audit scope included, for 2018:

- Information technology (IT) controls related to:
 - Active Directory - TCHP's internal network
 - Cognizant's Trizetto Healthcare product, Touchpoint QNXT (QNXT) - the TCHP claims adjudication and care coordination application
 - HealthTrio - the online web portal for provider and patient account management
- Business continuity and disaster recovery plans

Background

TCHP coordinates health services for members¹ in the Medicaid State of Texas Access Reform (STAR), Medicaid STAR Kids, and CHIP programs, and supports Medicaid and CHIP (a) provider claims processing and (b) provider and member benefits administration. TCHP supports its Medicaid and CHIP operations through its IT infrastructure, including Active Directory² and IT applications, including QNXT, and HealthTrio.

- Active Directory is a network service used to authenticate TCHP's workforce access to IT applications.
- QNXT is a vendor-based, software as a service,³ application used to adjudicate and store provider claims information and to support care coordination.
- HealthTrio is a web portal that provides explanations of benefits to TCHP providers and members.

When working remotely, TCHP's workforce first authenticates to the network via a Virtual Private Network (VPN), and then authenticates through Active Directory. Once authenticated through Active Directory, workforce access the QNXT application using separate credentials. HealthTrio does not require Active Directory authentication for access.

TCHP's data center in Texas provides the facility and IT infrastructure for accessing the QNXT application. The QNXT application and data are housed and operate from Cognizant's primary and secondary data centers located outside of Texas.

Claims information is stored on an Oracle database and replicated daily to TCHP's data warehouses,⁴ where it can be accessed by TCHP's workforce for reporting and data analysis. Claims information is replicated hourly to a mirrored offsite location for backup. Additionally, backups to a tape drive are performed weekly and monthly, and are stored offsite.

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.

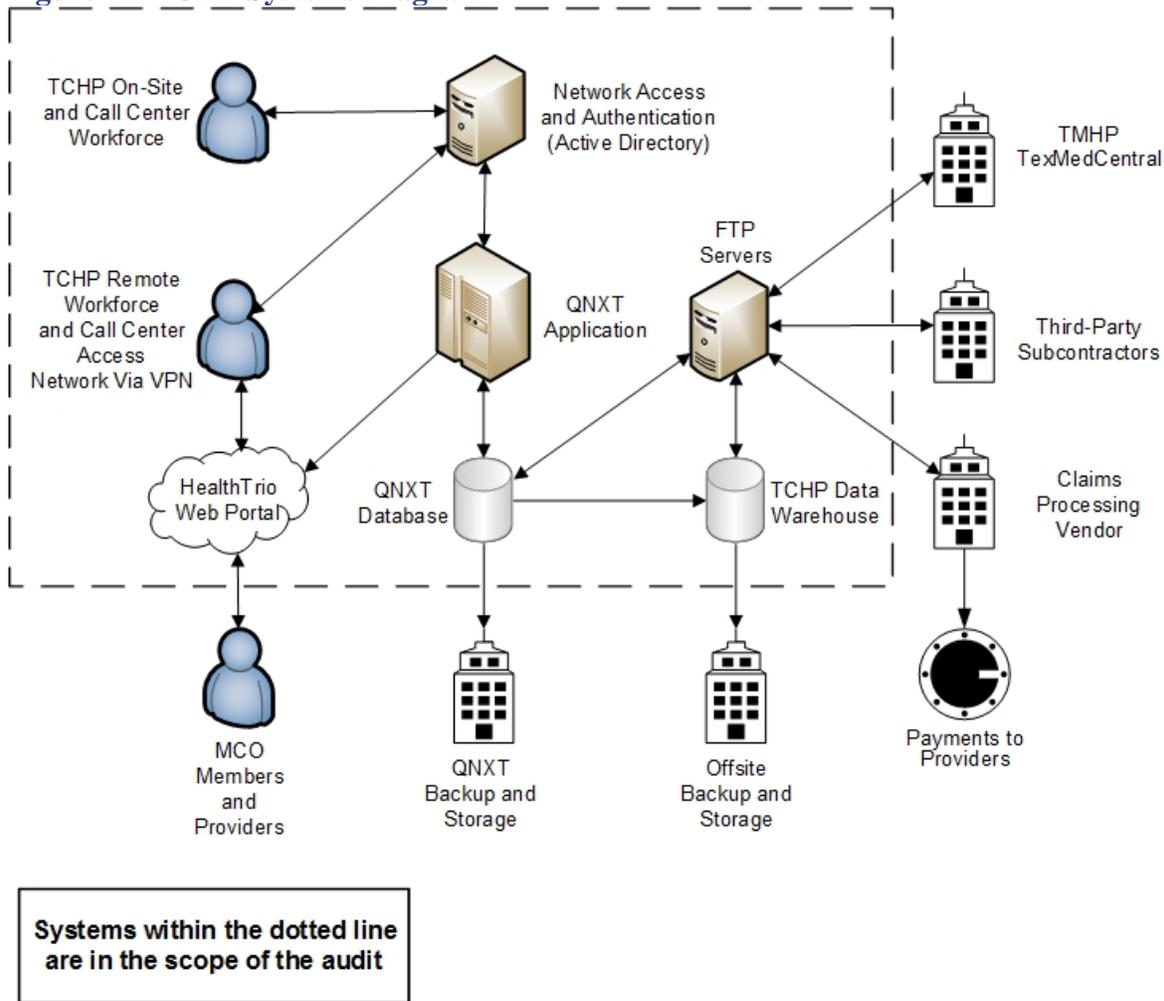
³ "Software as a service" is a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.

⁴ A "data warehouse" is a system that stores, retrieves, and manages large volumes of data.

TCHP receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) through TexMedCentral, its claims processing vendor, and other third parties through secure file transfers.

A diagram of these, and related systems and processes, is illustrated in Figure A.

Figure A: TCHP Systems Diagram



Source: OIG Audit Division

During 2016 and 2017, TCHP underwent major changes in IT oversight, operations, and management. Changes included physical relocation of servers and hardware, new vendors for operations, backup, and maintenance, revisions to policies and procedures related to security of confidential HHS System information, and changes to IT executive management. TCHP merged its Active Directory with the Active Directory of its parent organization, Texas Children’s Hospital, prior to the start of the audit. At the start of fieldwork in June 2018, many of these changes were in progress, but were not yet completed. The OIG Audit Division focused the evaluation of logical security controls on 2018, and did

not evaluate physical security as intended because the data center was in the process of being relocated to a new location.

HHSC Medicaid and CHIP Services (MCS), HHSC IT, and TCHP share accountability for safeguarding confidential HHS System information from accidental or unauthorized access, loss, or disclosure.

Methodology

The OIG Audit Division reviewed relevant security controls protecting confidential HHS System information in the custody of TCHP, primarily the QNX application. The key control areas and the associated control groups tested during the audit are identified in Table 1. Key control areas for information security contain controls that are required in order to provide reasonable assurance that material errors will be prevented or detected in a timely manner. Control groups are HHS Information Security Standards and Guidelines (ISSG)-defined groupings of security controls. Each control group contains multiple controls, which can be layered, based on data risks, to provide customized controls for information security.

Table 1: Key Control Areas and Control Groups

Key Control Areas Selected for Audit	ISSG Controls Groups	Issue Number
User Account Management	Access Controls (AC) Identification and Authentication (IA) Personnel Security (PS)	1.1, 1.2, 1.3, 1.4, and 2
Workforce Training	Awareness and Training (AT)	N/A
Information Security Oversight	Security Assessment and Authorization Controls (CA) Planning (PL)	NA
Configuration Management	Configuration Management (CM) System and Communications Protection (SC) Maintenance (MA)	N/A
Business Continuity and Disaster Recovery Planning	Contingency Planning (CP)	N/A
Information Systems Monitoring	Incident Response (IR)	N/A
Risk Management	Risk Assessment (RA)	3

Source: Prepared by the OIG Audit Division based on ISSG

An overview of all control areas tested in this audit is presented in Appendix A.

The OIG Audit Division examined IT security controls and relevant activities supporting data security at TCHP by conducting (a) detailed tests of activities, supporting technologies, and data and (b) a site visit to the location where key activities were performed.

The OIG Audit Division reviewed TCHP's business continuity and disaster recovery plans and related activities for member and provider services, claims processing, and associated support functions by (a) determining whether business continuity and disaster recovery plans were in place and tested at least annually, (b) reviewing TCHP reports on the emergency action plan discussed after the Hurricane Harvey event, (c) interviewing TCHP staff responsible for business continuity and disaster recovery activities, and (d) reviewing independent assessments of TCHP's IT environment, including security and recovery capabilities of TCHP data warehouses.

Criteria

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

- The Health Insurance Portability and Accountability Act of 1996
- 45 C.F.R. Part 160 and Part 164, Subparts A and C (2013)
- 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. 2.25 (2018)
- STAR Kids Contract, v. 1.5 (2017) through v. 1.6 (2018)
- HHS Information Security Standards and Guidelines Controls Catalog, v. 6 (2015)

Beginning on September 1, 2018, TCHP was required to follow HHS Information Security Controls (IS-Controls)⁵ instead of ISSG. Because of this, the recommendations in the report are focused on compliance with IS-Controls requirements, and the relevant IS-Controls criteria is included before each recommendation. 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

⁵ HHS Information Security Controls, v. 1.0 (Feb. 9, 2018).

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.

The OIG Audit Division presented audit results, issues, and recommendation to MCS and to TCHP in a draft report dated June 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 recommendation outlined in this report and will coordinate with HHSC IT and require TCHP to address issues identified in this report. TCHP agreed with some of the issues and indicated disagreement with others. Auditor comments follow the TCHP comment letter.

TCHP's comments are included in Appendix B. TCHP agreed with some of the issues and indicated disagreement with others. Auditor comments follow the TCHP comment letter.

AUDIT RESULTS

TCHP complied with ISSG requirements related to workforce training, information security oversight, configuration management, and information systems monitoring.

TCHP also complied with ISSG requirements related to business continuity and disaster recovery planning. Since a review of TCHP business continuity and disaster recovery plans for operations relating to the processing and storage of confidential HHS System information by TCHP was a specific objective of this audit, further detail, along with information about TCHP's response during Hurricane Harvey, 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 situation or other business disruption. TCHP's business continuity and disaster recovery planning and related activities specific to claims processing, member services, and supporting functions, are summarized below.

Policies

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

Plans

TCHP maintained, and periodically reviewed and updated, business continuity and disaster recovery plans.

Training

TCHP periodically trained its workforce personnel on their responsibilities during a disaster.

Testing

TCHP tested its business continuity and disaster recovery plans annually with an emphasis on preparation for the hurricane season, and updated its plans based on testing results.

Offsite Storage

TCHP maintained its backup tapes at an out-of-state subcontractor location during the period under review. For the QNXT application, TCHP coordinated with the subcontractor to maintain offsite storage of backups at a separate out-of-state location.

Alternate Processing Site

TCHP's third-party claims processing vendor's primary and secondary sites were located out-of-state and supported the continued claims processing operations of the QNXT application.

TCHP also maintained secondary network environments out-of-state to minimize the impact to business operations caused by a disruption to the primary environment.

Alternate Telecommunications Site

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

Information System Backup

TCHP conducted daily backups of key operating systems and coordinated with vendors to ensure that data hosted on third-party networks was also periodically backed up in accordance with policy. Backups were tested periodically and were available for restoration to production in the event of loss or corruption during an emergency.

The following summarizes TCHP activities related to claims processing, member services, and supporting functions, during the Hurricane Harvey disaster, and some lessons learned TCHP identified.

TCHP Response to Hurricane Harvey

There was minimal disruption to services provided by TCHP during Hurricane Harvey.

TCHP was able to maintain member services relating to claims processing and supporting functions during the hurricane and its aftermath. The switch-over to the back-up call center located in another city provided uninterrupted services to both members and providers. The information systems were unaffected by the hurricane, in part because the system servers and claims processing data were housed out-of-state.

Subsequent review of the results of the disaster by TCHP identified lessons learned for improvements that included (a) strengthening communication and polling to verify availability of staff who may be able to contribute remotely (b) improving support for members during hurricane events by gathering and publishing shelter information and verifying and communicating the status of network providers available to serve members, and (c) expanding communication efforts with providers so TCHP would be aware when providers whose offices were closed during the disaster resumed normal operations in their offices, so that TCHP could notify its members.

There were exceptions related to ISSG requirements related to:

- User Account Management
 - Access Controls
 - Identification and Authentication
- Risk Management

Details of these exceptions are included in the sections that follow.

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.

Details for issues related to two control groups within user account management, (a) access controls and (b) identification and authentication, follow.

Access Controls

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 they are permitted to exercise. Access controls include those related to user account reviews, disabling inactive accounts, disabling accounts for terminated users, and locking user accounts for excessive unsuccessful logon attempts.

User Account Reviews

User access to systems and applications should be appropriate, which means access should be limited to allow a user access only to transactions and functions that are necessary for the user to accomplish assigned tasks in accordance with assigned business responsibilities. This is based on the principle of least privilege.⁶ To accomplish least privilege access control practices, roles are created for various job functions, and the permissions to perform certain operations are assigned to specific roles. System users are assigned particular roles, and through those role assignments acquire the permissions to perform functions within the system. Permissions are not assigned to users directly, but rather are granted to certain role assignments.

ISSG requires MCOs to review account access levels, at a minimum, every 12 months for appropriateness and, when needed based on the results of the reviews, to modify, disable, or remove individuals' access to systems or applications.⁷

Issue 1.1: TCHP Did Not Review User Accounts for Appropriateness

TCHP did not perform annual reviews of user accounts and associated roles and permissions to ensure access to Active Directory and the HealthTrio application was appropriate and justified. While TCHP conducted user account reviews for the QNXT application twice a year, the process failed to identify (a) accounts that were not accessed recently and (b) terminated users, as identified in issues below.

Reviews of Active Directory and HealthTrio accounts were not performed because TCHP did not follow its policy addressing the performance of required reviews to determine, based on the job responsibilities of an individual, whether (a) access to applications was warranted and (b) roles and privileges granted to individual users were appropriate.

⁶ HHS Information Security Standards and Guidelines Controls Catalog, § 7.1, AC-6, v. 6 (Sept. 21, 2015).

⁷ HHS Information Security Standards and Guidelines Controls Catalog, § 7.1, AC-2(f), v. 6 (Sept. 21, 2015).

User accounts that have access to more permissions than necessary to perform job responsibilities violates the principal of least privilege and can impact the integrity and security of confidential HHS System information.

TCHP provided evidence of conducting a user account review in June 2018 for the HealthTrio application prior to the completion of this report and evidence of account remediation.

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires accounts to be reviewed for compliance with account management requirements at least every 365 days.⁸

Recommendation 1.1

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel TCHP to perform required reviews to determine whether access, roles, and privileges granted to users are appropriate and make adjustments as needed.

Management Response

Action Plan

Medicaid and CHIP Services Department (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require TCHP perform required reviews to determine whether access, roles, and privileges granted to users are appropriate and make adjustments as needed.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

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

Target Implementation Date

January 2020

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

Disabling Inactive Accounts

Inactive accounts are accounts that have not been accessed for a period of time, and indicate that a user's access to an application may not be needed.

ISSG requires that information systems automatically disable inactive privileged accounts after 60 days and non-privileged accounts after 90 days.⁹

Privileged accounts have escalated access within the computer system, which allows permission to edit or create user accounts, data, or settings within the operating system, application, or database. User account management needs to accommodate the special needs of privileged accounts to include provisioning, authentication, authorization, password management, auditing, and access controls over shared or generic (non-unique) privileged accounts. Many shared or generic privileged accounts are built-in system accounts created automatically when an operating system, application, or database is first installed.

Issue 1.2: TCHP Did Not Timely Disable Inactive Accounts

TCHP did not disable inactive accounts in Active Directory, HealthTrio, and QNXT after 60 days of inactivity for privileged accounts and after 90 days for non-privileged accounts.

The following accounts, according to TCHP system-generated last logon activity reports, did not meet ISSG requirements for disabling inactive accounts because the accounts were enabled and had previous logon activity. These accounts had more than 60 days of inactivity for privileged accounts and more than 90 days of inactivity for non-privileged accounts.

- 88 of 3,346 (2.63 percent) Active Directory accounts
- 120 of 689 (17.42 percent) HealthTrio accounts
- 46 of 882 (5.22 percent) QNXT accounts

TCHP did not timely disable these inactive accounts because its policy and practices were not aligned with ISSG requirements. TCHP policy states that accounts with no activity for over 90 days are to be disabled automatically by the system.¹⁰ This did not align with the requirement for privileged accounts to be disabled after 60 days of inactivity. In addition, TCHP did not have processes in

⁹ HHS Information Security Standards and Guidelines Controls Catalog, § 7.1, AC-2(3), v. 6 (Sept. 21, 2015).

¹⁰ TCHP Policy: Managing User Access to Texas Children's Information Policy, Policy 990(6), v. 2 (Mar. 1, 2018).

place to automatically disable inactive accounts in Active Directory, QNXT, or HealthTrio.

In addition to the 88 Active Directory and 120 HealthTrio enabled accounts noted above that had not been disabled, TCHP last logon activity reports also indicated there were:

- 510 Active Directory accounts that were enabled but were never accessed
- 67 HealthTrio accounts that were enabled but were never accessed

TCHP indicated that a system merger between the Active Directory environments at TCHP and Texas Children's Hospital in 2017 contributed to the high number of enabled accounts that were not accessed after the merger, because the merger failed to import the Active Directory fields such as the date the account was disabled and the last logon time stamp.

TCHP requests that accounts be created in HealthTrio by the vendor for use by members, providers, and workforce personnel. Though accounts are created they are not always needed by the user as duties and responsibilities may allow the user to utilize QNXT or other methods to access the same information. Consequently, accounts may be created but may never be accessed.

Subsequent to the OIG Audit Division's completion of audit fieldwork, TCHP performed a review of Active Directory, QNXT, and HealthTrio accounts and provided evidence that it had disabled inactive user accounts that no longer required access to the applications.

Failing to disable inactive user accounts placed confidential HHS System information at risk of unauthorized viewing, modification, or deletion.

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires that information systems automatically disable inactive accounts within 90 days.¹¹

Recommendation 1.2

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel TCHP to implement a control process to automatically disable accounts that have been inactive for more than 90 days for all systems and applications that create, process, transfer, or store confidential HHS System information.

¹¹ HHS Information Security Controls, Appendix B, AC-02(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 TCHP implement a control process to automatically disable accounts that have been inactive for more than 90 days for all systems and applications that create, process, transfer, or store confidential HHS System information.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

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

Target Implementation Date

January 2020

Disabling Accounts for Terminated Users

ISSG requires that management disable information system access immediately upon termination of employment and revoke any authenticators or credentials associated with the terminated individual.¹²

Issue 1.3: TCHP Did Not Disable the User Accounts of Some Terminated Employees and Contractors

TCHP did not immediately disable Active Directory and QXNT user accounts for some terminated individuals.

There were 3 Active Directory user accounts and 55 QXNT user accounts that were not disabled when the individuals (employees or contractors) were terminated. These accounts could have allowed continued access by the terminated individual.

Additionally, 2 of the 3,346 Active Directory user accounts and 2 of the 55 QNXT user accounts that were not disabled were accessed after the date of termination. TCHP did not indicate that confidential HHS System information was inappropriately accessed. There were no active HealthTrio user accounts assigned to terminated users.

Table 3: Summary of Terminated Accounts

	Active Directory	QNXT
Total Accounts	3,346	882
Active Accounts of Terminated Individuals	3	55
Accounts Accessed Post Termination	2	2

Source: *OIG Audit Division*

TCHP used an identity management application as the solution for provisioning and de-provisioning user accounts in Active Directory. The IT service desk disabled Active Directory accounts and updated the expiration date field upon notification from the terminated individual’s supervisor. Once disabled, the identity management solution was programmed to delete the disabled Active Directory accounts after 120 days.

The active accounts for terminated individuals were not disabled because, in some instances, supervisors did not notify the IT service desk to initiate the established process for disabling the user account. In addition, for QNXT accounts, the IT service desk must contact the vendor supporting QNXT to request that user accounts be disabled. Sometimes, the IT service desk failed to request that the QNXT vendor disable user accounts for terminated individuals.

¹² HHS Information Security Standards and Guidelines Controls Catalog, § 7.14, PS-4, v. 6 (Sept. 21, 2015).

Active Directory and QNXT accounts belonging to terminated individuals that are not disabled can be used to gain unauthorized access to the TCHP network and other resources available on the network.

Subsequent to the completion of audit fieldwork, TCHP provided evidence to the OIG Audit Division that it had disabled the terminated user accounts described above.

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires system access to be revoked prior to or during the employee termination process or action, and any authenticators or credentials associated with that individual to be revoked.¹³

Recommendation 1.3

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel TCHP to implement control processes to immediately disable user accounts for terminated employees and contractors.

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require TCHP implement control processes to immediately disable user accounts for terminated employees and contractors.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

Director, Managed Care Compliance and Operations

Director, IT Medicaid and CHIP Systems

Target Implementation Date

January 2020

¹³ HHS Information Security Controls, Appendix B, PS-04, v. 1.0 (Feb. 9, 2018).

Locking User Accounts for Excessive Unsuccessful Logon Attempts

ISSG requires the information system to enforce a limit of 3 consecutive invalid access attempts by a user within a 60-minute period and automatically lock the account for 30 minutes or until released by an account administrator when the maximum number of unsuccessful attempts is exceeded.¹⁴

Issue 1.4: TCHP Did Not Lock User Accounts After Multiple Unsuccessful Logon Attempts

TCHP did not enforce requirements for locking accounts when unsuccessful logon attempts occurred. Limiting the number of consecutive logon attempts within specific timeframes reduces the probability a brute force attack¹⁵ or similar cyber-attack successfully enters passwords.

Detailed results of this issue are confidential under Texas Government Code Sections 552.139(b) and 2054.077(c), and are therefore not included in this report. The confidential, detailed results have been provided separately to responsible HHS System personnel and TCHP staff authorized to receive computer vulnerability information.

TCHP provided evidence that it had corrected the requirements for locking accounts when unsuccessful logon attempts occurred prior to the issuance of this report.

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires the information system to lock-out the user account automatically after 3 consecutive invalid login attempts during a 60-minute time period and automatically disable or lock the account for 30 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.¹⁶

Recommendation 1.4

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should compel TCHP to strengthen its account lock-out policy and configurations to be in accordance with IS-Controls requirements.

¹⁴ HHS Information Security Standards and Guidelines Controls Catalog, § 7.1, AC-7, v. 6 (Sept. 21, 2015).

¹⁵ “Brute force attacks” are repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found.

¹⁶ HHS Information Security Controls, Appendix B, AC-07, 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 TCHP strengthen its account lock-out policy and configurations to comply with IS-Controls requirements.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

Director, Managed Care Compliance and Operations

Director, IT Medicaid and CHIP Systems

Target Implementation Date

January 2020

Identification and Authentication

ISSG requires the identification and authentication (verification) of information system users, processes, or devices as a prerequisite for allowing access to the HHS information system.¹⁷ Controls include password management and password configuration settings, authenticator management to verify users and machines, and encryption protocols to protect the transmission of data between identified users and equipment.

¹⁷ HHS Information Security Standards and Guidelines Controls Catalog, § 7.7, IA, v. 6 (Sept. 21, 2015).

Password Configuration Settings

ISSG requires that password configuration settings enforce password requirements for information systems.¹⁸ Requirements include:

- Enforcing minimum password complexity of eight characters and one item from each of the following categories:
 - Upper case alpha
 - Lower case alpha
 - Number
 - Special character
- Enforcing a minimum of four changed characters when a new password is created.
- Storing and transmitting only cryptographically protected passwords.
- Enforcing password lifetime restrictions with a minimum of one day for all accounts and a maximum of 60 days for privileged accounts, 90 days for non-privileged accounts, and 180 days for system accounts.
- Prohibiting password reuse for six generations.
- Allowing the use of a temporary password for system logons with an immediate change to a permanent password.

Issue 2: TCHP Did Not Enforce Password Requirements

TCHP's password requirements did not meet ISSG requirements.

Improving password complexity reduces the probability a brute force attack or similar cyber-attack successfully determines passwords.

¹⁸ HHS Information Security Standards and Guidelines Controls Catalog, § 7.7, IA-5(1), v. 6 (Sept. 21, 2015).

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires TCHP to:¹⁹

- Enforce minimum password complexity of eight characters with one character from the following categories:
 - Upper case alpha
 - Lower case alpha
 - Number
 - Special character
- Enforce a minimum of four changed characters when a new password is created.
- Store and transmit only cryptographically protected passwords.
- Enforce password lifetime restrictions of a minimum of one day for all accounts and a maximum of 60 days for privileged accounts; 90 days for non-privileged accounts, and 180 days for system accounts.
- Prohibit password reuse for six generations for moderate systems.
- Allow the use of a temporary password for system logons with an immediate change to a permanent password.

TCHP password configurations that were in effect during the audit period, although not in compliance with ISSG, were in compliance with IS-Controls. Consequently, this issue does not have a recommendation.

RISK MANAGEMENT

Risk management is a process for identifying and controlling threats to IT. A key component of risk management is risk assessment. Risk assessments systematically identify, estimate, and prioritize risk to organizational operations, assets, individuals, and other organizations resulting from the operation and use of information systems. The purpose of risk assessments is to inform decision makers and support risk responses by identifying (a) relevant threats to organizations, (b) vulnerabilities both internal and external to the organization, (c) impact to the organization that occur given the potential for threats exploiting vulnerabilities, and (d) likelihood that harm will occur. The result of this process is a determination of risk. Vulnerability scans are an integral part of the risk assessment process.

¹⁹ HHS Information Security Controls, Appendix B, IA-05(01), v. 1.0 (Feb. 9, 2018).

Vulnerability Scans

ISSG requires scans for vulnerabilities in the information system and hosted application at minimum annually and when new vulnerabilities potentially affecting the components are identified and reported. Vulnerabilities must be remediated based on risk prioritization in accordance with assessment of risk.²⁰

Issue 3: TCHP Did Not Conduct Vulnerability Scans Until April 2018 and Did Not Remediate Identified Vulnerabilities

TCHP did not perform annual vulnerability scans during the 18-month period from September 2016 through March 2018.

TCHP conducted a scan on April 9, 2018, that identified critical (24 confirmed and 24 potential) and severe (141 confirmed and 193 potential) vulnerabilities. In February 2019, TCHP indicated it was in the process of addressing the identified vulnerabilities with the assistance of a consulting firm, and had not yet remediated any of the identified vulnerabilities.

Failure to perform vulnerability scans and remediate identified vulnerabilities exposes the information system to risk of corruption, breaches, or weaknesses, which may be used to allow unauthorized access, loss, or disclosure of confidential HHS System information.

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires scans for vulnerabilities in the information system and hosted application at minimum monthly and when new vulnerabilities potentially affecting the components are identified and reported.²¹

Recommendation 3a

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should require TCHP to implement a process to conduct required vulnerability scans of its IT system.

²⁰ HHS Information Security Standards and Guidelines Controls Catalog, § 7.15, RA(5), v. 6 (Sept. 21, 2015).

²¹ HHS Information Security Controls, Appendix B, RA-05, 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 TCHP implement a process to conduct required vulnerability scans of its IT system.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

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

Target Implementation Date

January 2020

Beginning on September 1, 2018, TCHP was required to follow IS-Controls. IS-Controls requires vulnerabilities to be remediated based on risk prioritization in accordance with assessment of risk.²²

Recommendation 3b

MCS, through its contract oversight responsibilities, including the use of tailored contractual remedies as appropriate, should require TCHP to implement processes that ensure the timely remediation of identified vulnerabilities in accordance with an organizational assessment of risk.

Management Response

Action Plan

MCS agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to require TCHP implement processes that ensure the timely remediation of identified vulnerabilities in accordance with an organizational assessment of risk.

MCS expects TCHP to take immediate corrective action under a Corrective Action Plan (CAP). MCS will allow 180 days to implement all actions within the CAP.

²² HHS Information Security Controls, Appendix B, RA-05, 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 currently reviews the submitted system security plans and checklists prepared by the Managed Care Organizations (MCOs).

Responsible Managers

Director, Managed Care Compliance and Operations

Director, IT Medicaid and CHIP Systems

Target Implementation Date

January 2020

CONCLUSION

TCHP complied with ISSG requirements related to workforce training, information security oversight, configuration management, and information systems monitoring. TCHP also complied with ISSG requirements related to business continuity and disaster recovery planning.

There were exceptions related to ISSG requirements related to user account management and risk management. Specifically, TCHP did not:

- Perform annual reviews of user accounts and associated roles and permissions to ensure access to applications was appropriate and justified.
- Disable inactive accounts after 60 days of inactivity for privileged accounts and after 90 days for non-privileged accounts.
- Immediately disable user accounts for some terminated individuals.
- Enforce requirements for locking accounts when unsuccessful logon attempts occurred.
- Perform annual vulnerability scans during the 18-month period from September 2016 through March 2018.

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

- Performing reviews to determine whether access, roles, and privileges granted to users are appropriate and making adjustments as needed.
- Automatically disabling accounts that have been inactive for more than 90 days for all systems and applications that create, process, transfer, or store confidential HHS System information.
- Immediately disabling user accounts for terminated employees and contractors.
- Strengthening its account lockout policy and configurations.
- Conducting required vulnerability scans of its IT system and timely remediating identified vulnerabilities.

The OIG Audit Division thanks the management and staff of MCS, HHSC IT Health Services Systems, HHS Information Systems Security, and TCHP 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-1	Access Control Policy and Procedures		N/A
AC-2	Account Management	CD, CE	1.1 and 1.2
AC-2(1)	Automated System Account Management	CE	1.1 and 1.2
AC-5	Separation of Duties		N/A
AC-6	Least Privilege		N/A
AC-6(1)	Authorize Access to Security Functions		N/A
AC-6(5)	Privileged Accounts		N/A
AC-7	Unsuccessful Logon Attempts	CD	1.4
AC-17	Remote Access		N/A
Identification and Authentication (IA)			
IA-1	Identification and Authentication Policy and Procedures		N/A
IA-2	Identification and Authentication [Organizational Users]	CD,CE	2
IA-3	Device Identification and Authentication		N/A
IA-5	Authenticator Management	CD,CE	2
IA-8	Identification and Authentication [Non-organizational Users]		N/A
Personnel Security Controls (PS)			
PS-4	Personnel Termination	CE	1.3
Awareness and Training (AT)			
AT-1	Security Awareness and Training Policy and Procedures		N/A
AT-2	Security Awareness Training		N/A
Security Assessment and Authorization (CA)			
CA-1	Security Assessment and Authorization Policy and Procedures		N/A
CA-2	Security Assessments		N/A
CA-5	Plan of Action and Milestones		N/A
CA-6	Security Authorization		N/A
Planning (PL)			
PL-1	Security Planning Policy and Procedures		N/A
PL-2	System Security Plan		N/A
Configuration Management (CM)			
CM-1	Configuration Management Policy and Procedures		N/A

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
CM-2	Baseline Configuration		N/A
CM-3	Configuration Change Control		N/A
CM-4	Security Impact Analysis		N/A
CM-5	Access Restrictions for Change		N/A
CM-6	Configuration Settings		N/A
CM-7	Least Functionality		N/A
CM-8	Information System Component Inventory		N/A
CM-9	Configuration Management Plan		N/A
Systems and Communications Protection (SC)			
SC-13	Cryptographic Protection		N/A
Maintenance (MA)			
MA-1	System Maintenance Policy and Procedures		N/A
MA-2	Controlled Maintenance		N/A
Contingency Planning (CP)			
CP-1	Contingency Planning Policy and Procedures		N/A
CP-2	Contingency Plan		N/A
CP-3	Contingency Training		N/A
CP-4	Contingency Plan Testing		N/A
CP-7	Alternate Processing Site		N/A
CP-9	Information System Backup		N/A
CP-10	Information System Recovery and Reconstitution		N/A
Incident Response (IR)			
IR-1	Incident Response Policy and Procedures		N/A
IR-3	Incident Response Testing		N/A
IR-4	Incident Handling		N/A
IR-5	Incident Monitoring		N/A
IR-6	Incident Reporting		N/A
IR-8	Incident Response Plan		N/A
Risk Assessment (RA)			
RA-1	Risk Assessment Policy and Procedures		N/A
RA-2	Security Categorization		N/A
RA-3	Risk Assessment		N/A
RA-5	Vulnerability Scanning	CD,CE	3

Appendix B: Texas Children's Health Plan Comment Letter



July 24, 2019

Sent via Electronic Mail (Steve.Sizemore2@hhsc.state.tx.us)

Mr. Steve Sizemore, CIA, CISA, CGAP
Performance Audit Director
Texas Health and Human Services Commission
Inspector General

Re: Audit Report of Texas Children's Health Plan: Security Controls Over Confidential HHS System Information and Business Continuity and Disaster Recovery Plans

Mr. Sizemore,

I am writing to respond formally to the above-mentioned audit report. Texas Children's Health Plan ("TCHP") appreciates the engagement from the Office of Inspector General ("OIG") with respect to this audit. However, TCHP disagrees with a number of the findings. Please find aspects of the report with which TCHP disagrees below as well as TCHP's management response. For convenience, TCHP has quoted the issues from the report in bold.

Issue 1.1: TCHP Did Not Review User Accounts for Appropriateness

TCHP Disagreement with the Findings

TCHP disagrees that it did not perform annual reviews of user access to HealthTrio. TCHP performs an annual review of user access to HealthTrio on an annual basis and started in 2018 due to new requirements from Annual Financial Reporting Model Regulation ("AFRMR").

Issue 1.2: TCHP Did Not Timely Disable Inactive Accounts

TCHP Disagreement with the Findings

TCHP disagrees with this audit finding for HealthTrio accounts. TCHP has effective controls in place to automatically lock accounts that have been inactive for more than 90 days. Although the account is not disabled or deleted, the account is effectively locked and no longer accessible. Once the account is locked after the 90th day of inactivity, end-users have to follow a formal request process to re-gain access to HealthTrio. The end-user cannot re-enable access independently via a self-service model.

Issue 1.3: TCHP Did Not Disable the User Accounts of Some Terminated Employees and Contractors

Management Response

TCHP agrees with the audit finding, however, terminated AD users are not able to access QXNT which significantly reduces the risk inappropriate access to QXNT by a terminated user.

Issue 1.4: TCHP Did Not Lock User Accounts After Multiple Unsuccessful Logon Attempts

6330 West Loop South, WLS 8300 Bellaire, TX 77401

TCHP Disagreement with the Findings

TCHP provided a response to OIG ensuring TCHP adheres to security best practices for the unsuccessful logon attempts setting on March 4, 2019 in a formal statement on TCHP letterhead. Please see Exhibit A.

Issue 2: TCHP Did Not Enforce Password RequirementsManagement Response

As noted in the audit, TCHP was and is in compliance with OIG IS-Controls, and no action is needed. Because TCHP was in compliance with pertinent requirements, TCHP requests OIG remove this audit finding from the OIG Final Audit report.

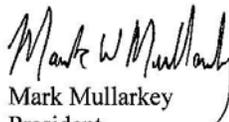
Issue 3: TCHP Did Not Conduct Vulnerability Scans Until April 2018 and Did Not Remediate Identified VulnerabilitiesTCHP Disagreement with the Findings

TCHP disagrees with this audit finding as TCHP did meet ISSG requirement of annually scanning for vulnerabilities, at a minimum, starting in 2018.

Management Response

Texas Children's patch policy requires patching security vulnerabilities on a set schedule. Effective April 2018, vulnerability scans are ran after each patch deployment for compliance confirmation. Out-of-band critical security patches are risk assessed to determine if an accelerated mitigation plan is required based on existing mitigating controls.

Sincerely,



Mark Mullarkey
President
Texas Children's Health Plan

Auditor Comments

The OIG Audit Division appreciates the feedback provided by TCHP in its comment letter and respects the TCHP position on reported issues. The OIG Audit Division offers the following comments in response to the TCHP comment letter:

- Issues 1.1, 1.4, and 3
The actions taken by TCHP to address security issues, though commendable, occurred during or after the audit period.
- Issues 1.2, 1.3, and 2
The controls as described by TCHP were not supported by the evidence provided to the OIG Audit Division.

During this audit, as potential issues were identified, the OIG Audit Division shared detailed evidence supporting the issues with TCHP, presenting an opportunity to research the issues and provide additional or replacement evidence. When received from TCHP, the OIG Audit Division considered the additional or replacement evidence and, when appropriate, adjusted audit results and conclusions accordingly. These collaborative efforts continued through July 2019.

The OIG Audit Division stands by its methodology for conducting this audit, its approach for obtaining sufficient and appropriate evidence to achieve the audit objectives, and the issues, conclusions, and recommendations presented in this report. The OIG Audit Division conducts audits in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States, which require auditors to obtain sufficient and appropriate evidence to provide a reasonable basis for findings and conclusions.

Appendix C: Report Team and Distribution

Report Team

OIG staff members who contributed to this audit report include:

- David Griffith, CPA, CIA, CGFM, Deputy IG for Audit
- Marios Parpounas, CIA, CISA, CGFM, CFE, Assistant Deputy IG for Audit
- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Anton Dutchover, CPA, Audit Manager
- Melissa Larson, CIA, CISA, CFE, IT Audit Manager
- Daniel Graf, CISA, IT Project Manager
- Brian Baker, Staff Auditor
- JoNell Abrams, Staff Auditor
- Kathryn Messina, 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 and Compliance and Operations, Medicaid and CHIP Services
- Steve Buche, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Ivan Hovey, Director, HHSC IT Applications
- Thuy Cao, HHS Chief Information Security Officer

Texas Children's Health Plan

- Mark Mullarkey, President
- Sharon McWhorter, Director, Controls and Compliance
- John Turner, Director IS Health Plan Enterprise Systems
- Mariana Pope, Director, Compliance and Privacy
- Theresa Tonthat, Director, Information Security
- Donald Walker, Director, Senior Legal Counsel

Appendix D: 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
- Olga Rodriguez, Chief of Strategy and Audit
- Quinton Arnold, Chief of Inspections and Investigations
- Steve Johnson, Interim 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