Audit Report

Security Controls Over Confidential HHS System Information

El Paso Health

April 24, 2020
OIG Report No. AUD-20-009

Inspector General

Texas Health
and Human Services

HHS OIG
TEXAS HEALTH AND HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

April 24, 2020 Audit Report

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

El Paso Health

WHY OIG CONDUCTED THIS AUDIT

The OIG Audit Division conducted this audit to assess the design and effectiveness of (a) selected security controls over confidential HHS System information stored and processed by El Paso Health and (b) business continuity and disaster recovery planning for selected activities related to the delivery of managed care services to Medicaid and CHIP members.

Having secure information systems is important because El Paso Health stores and processes protected health information for its members. In 2019, El Paso Health served 74,495 members and received $158.9 million in capitation payments.

WHAT OIG RECOMMENDS

El Paso Health should:

- Consistently ensure that user accounts are disabled after a 90-day period of inactivity and access to all information systems is disabled when employees terminate.
- Establish and document baseline security configurations for servers and any other network devices that store and process confidential HHS System information.
- Document procedures for the sanitization of media and the destruction of confidential HHS information.

MANAGEMENT RESPONSE

In its management responses, El Paso Health indicated agreement with the audit results and will take appropriate actions by July 2020 to address issues identified in this report.

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

WHAT OIG FOUND

El Paso Health implemented controls to safeguard confidential Health and Human Services (HHS) System information and developed procedures to ensure the continuation of the operations necessary to deliver services to members in the event of an emergency or disaster. However, El Paso Health should further strengthen controls related to user access, configuration management, and media protection.

El Paso Health complied with HHS Information Security Controls (IS-Controls) requirements related to information security oversight, information system monitoring, risk management, and workforce training. These controls help to strengthen the security of information technology systems and confidential HHS System data transmitted and stored by El Paso Health.

El Paso Health 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.

El Paso Health did not always comply with IS-Control requirements for user account management, configuration management, and media protection. Specifically, El Paso Health did not:

- Consistently manage user access to information systems that contained confidential HHS System information by timely disabling user accounts after 90 days for non-privileged accounts and timely deactivating user accounts during the termination process to protect confidential HHS System information from unauthorized access, loss, or disclosure.
- Establish and maintain documented baseline security configurations for information systems that process and store confidential HHS System information. Documented configurations mitigate security weaknesses by ensuring that server implementation and change management processes are standardized and repeatable.
- Maintain documented procedures to guide destruction and sanitization of media housing confidential HHS System information to ensure all data is properly removed.

BACKGROUND

El Paso Health contracted with Health and Human Services Commission to provide Medicaid managed care to its members through the State of Texas Access Reform (STAR) program and Children’s Health Insurance Program (CHIP). It is required to protect confidential information, including protected health information, of members and ensure managed care services are restored timely in the event of a disruption such as during an emergency or disaster.

El Paso Health is required to protect and secure confidential HHS System information, such as claims data, in accordance with requirements established in IS-Controls starting September 1, 2018.

TABLE OF CONTENTS

INTRODUCTION

The Texas Health and Human Services (HHS) Office of Inspector General (OIG) Audit Division conducted an audit of security controls over confidential HHS System information at El Paso Health. El Paso Health provides Medicaid managed care to its members through the State of Texas Access Reform (STAR) program and the Children's Health Insurance Program (CHIP).

The OIG Audit Division conducted the audit to determine whether (a) confidential HHS System information in the custody of El Paso Health and its subcontractors was protected from unauthorized access, loss, or disclosure; and (b) plans were developed and tested, and El Paso Health's workforce was trained to provide availability and continuity of business operations and services to members in the event of information technology (IT) outages or disasters.

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 El Paso Health.

- The business continuity and disaster recovery planning for selected activities related to the delivery of managed services to Medicaid and CHIP members enrolled with El Paso Health.

The audit scope covered, for 2019:

- IT controls for logical security implemented to protect access to the El Paso Health network, claims processing, care coordination application, and related application and reporting databases.

- System security, risk management, and business continuity and disaster recovery plans.

- Security of data in transit and stored.

- Incident response, information system monitoring, and security training.

- Physical security of IT infrastructure.
- General controls supporting systems backup, contingency planning, and recovery activities.

Background

El Paso Health coordinates health services for members[1] in the Medicaid STAR and CHIP programs and supports Medicaid and CHIP (a) provider claims processing and (b) provider and member benefits administration. El Paso Health supports its Medicaid and CHIP operations through its IT infrastructure, including networks, applications, databases, web portals, and call centers supporting members and providers.

When working remotely, El Paso Health's workforce accesses the network via a virtual private network (VPN) connection that authenticates the users through a directory service. Once authenticated on the network, authorized users can access the claims and client management applications. El Paso Health utilizes a single sign-on[2] solution for accessing network applications.

El Paso Health maintains both a primary data center and a secondary data center designed to sustain operations in the event of a disruption to the primary data center. Claims data is backed-up daily for storage at an off-site facility.

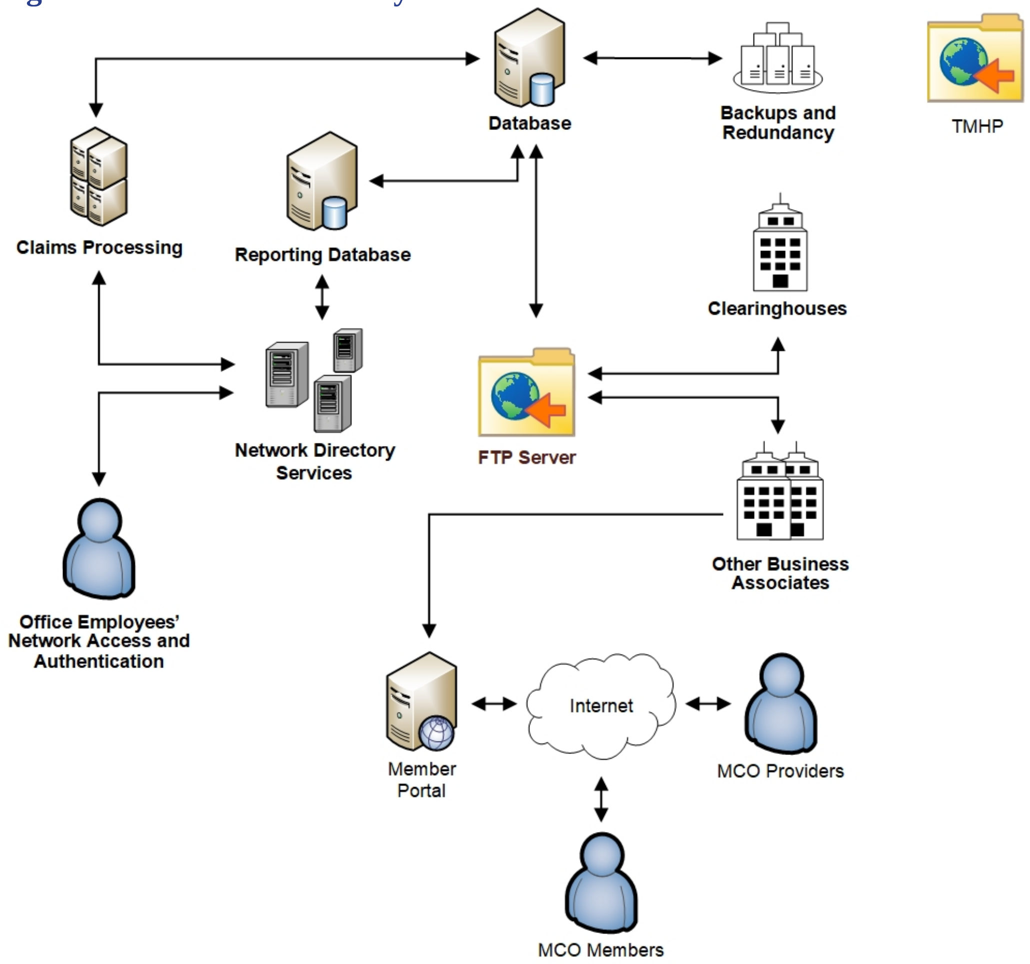
El Paso Health receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) through clearinghouses, an explanation of benefits portal, and other third-parties using secure file transfers.

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

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

Figure A is an illustration of El Paso Health's systems and processes. The information systems in bold designate the applications and processes in the scope of the audit, including (a) access to El Paso Health's network, claims application, and associated databases, (b) sharing of data with external business associates, and (c) storage and backup activities.

Figure A: El Paso Health's Systems



Source: OIG Audit Division

The OIG Audit Division examined the claims application and associated (a) infrastructure, (b) operating system, and (c) database that process and store claims information.

El Paso Health's data centers provide the facility and IT infrastructure for the claims 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 planning activities in the event of (a) a disaster declared by the Federal Emergency Management Agency (FEMA) or the Texas governor, or (b) other operational disruptions.

Health and Human Services Commission (HHSC) Medicaid and CHIP Services (MCS), HHSC IT, and El Paso Health share accountability for safeguarding confidential HHS System information from accidental or unauthorized access, loss, or disclosure. The Uniform Managed Care Contract (UMCC) sets forth the terms and conditions to which each managed care organization (MCO) must adhere when conducting business in the State.[3] Security control baselines must follow guidance provided in HHS Information Security Controls (IS-Controls),[4] which is based on the National Institute of Standards and Technology security standards.

The OIG Audit Division applied criteria from IS-Controls and El Paso Health's security policies, 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 El Paso Health.

Methodology

The OIG Audit Division reviewed key security controls protecting confidential HHS System information in the custody of El Paso Health, primarily the claims application. 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.

Appendix A presents an overview of all control groups and baselines tested in this audit.

The OIG Audit Division examined the IT security controls and relevant activities supporting data security at El Paso Health by (a) reviewing policies and procedures in detail to gain an understanding of the design of controls, (b) visiting El Paso Health 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 El Paso Health.

The OIG Audit Division presented audit results, issues, and recommendations to El Paso Health in a draft report dated March 18, 2020. El Paso Health was provided with the opportunity to study and comment on the report. The El Paso Health management responses to the audit recommendations contained in the report are included in the report following each recommendation.

[3] Uniform Managed Care Contract, v. 2.26 (Sept. 1, 2018).

[4] HHS Information Security Controls, v. 1.0 (Feb. 9, 2018).

In its management responses, El Paso Health indicated agreement with the audit results and will take appropriate actions by July 2020 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, § 202.3 and Subchapter B (2015) and (2016)
- Uniform Managed Care Contract, v. 2.26 (2018) through v. 2.26 (2019)
- HHS Information Security Controls (IS-Controls), v. 1.0 (2018)[5]

Auditing Standards

Generally Accepted Government Auditing Standards

The OIG Audit Division conducted this audit in accordance with generally accepted government auditing standards (GAGAS) 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 (formerly known as the Information Systems Audit and Control Association)

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.

[5] The HHS Information Security Controls was formerly known as Enterprise Information Security Standards and Guidelines (EISSG and ISSG).

AUDIT RESULTS

El Paso Health complied with IS-Control requirements related to information security oversight, information systems monitoring, risk management, workforce training, and business continuity.

Information Security Oversight

El Paso Health established an information security and privacy program, which maintained information security, privacy, and policy standards that were reviewed and updated annually. El Paso Health is in communication with HHS to coordinate enhancements and modifications to the security plan with regards to anticipated changes to the HHS IS-RAMP and annual deliverables.

Information Systems Monitoring

El Paso Health ensured the integrity, availability, and confidentiality of HHS System information by implementing technical, administrative, and physical safeguards. El Paso Health also (a) employed tools and processes to monitor and protect the information system from unauthorized access, irregularities, incidents, and other issues and (b) performed appropriate response activities to resolve noted incidents. El Paso Health conducted periodic vulnerability scans to heighten awareness and improve security.

Risk Management

El Paso Health conducted annual assessments of its information technology systems and implemented strategies to manage identified risks, including those associated with confidential HHS System information.

Workforce Training

El Paso Health provided its workforce with security and privacy training, conducted appropriate background checks, ensured individual accountability, and implemented appropriate sanctions for non-compliance.

Business Continuity

El Paso Health complied with IS-Control requirements related to business continuity and disaster recovery planning. 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 the continuity of operations in the event of an emergency or other business disruption. Additionally, the UMCC requires MCOs to have plans in place to provide member services and process claims should disasters interrupt normal business.[6] El Paso Health's business continuity and disaster recovery planning and related activities specific to claims processing, member services, and supporting functions, are summarized below.

Policies—El Paso Health maintained, reviewed, and updated the contingency planning policies and procedures that ensure the continuation of business practices and maintain services to members in the event of an emergency or disaster.

Plans—El Paso Health maintained, and periodically reviewed and updated, business continuity and disaster recovery plans. Additionally, El Paso Health's plans for emergency and disaster events included processes to (a) ensure members have access to managed care services, (b) process prior authorizations, and (c) allow claims processing exceptions by specific locations.

Training—El Paso Health trained personnel annually on their responsibilities during a disaster.

Testing—El Paso Health tested its business continuity and disaster recovery plans annually and updated its plans based on the results.

Off-site Storage—El Paso Health stored backup tapes at a third-party subcontractor location.

Alternate Processing Site—El Paso Health had an off-site data center with capability to resume claims processing and other operations in the event of a disruption at its primary data center.

Alternate Telecommunications Site—A secondary call center provides El Paso Health with the capability to maintain member services and provider support in the event the primary call center is unable to operate.

Information System Backup—El Paso Health conducted backups of key systems and data daily, weekly, and monthly. Backup tapes were transferred to a third-party subcontractor for storage and were tested periodically. Backup tapes were available to support restoration of claims processing in the event of loss, disruption, or other incident.

[6] Uniform Managed Care Contract, Attachment B-1, Chapter 7.2.6, v. 2.26 (Sep. 1, 2018) through v. 2.28 (Mar. 1, 2019).

Although El Paso Health was compliant in the areas noted, there were exceptions to IS-Controls requirements for:

- User Account Management
- Configuration Management
- Media Protection

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, a key feature of user account management, 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. User account management includes (a) access controls related to approving and terminating user account roles and privileges, (b) periodic user account reviews, (c) disabling inactive accounts, (d) disabling accounts for terminated users, and (e) locking user accounts for excessive unsuccessful log on attempts.

Disabling Inactive and Terminated User Accounts, and User Account Provisioning

Inactive accounts are accounts that have not been accessed for a specified period of time, which indicates a user's access to an application may not be needed. Account provisioning processes are control standards used 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.

Issue 1: El Paso Health Should Consistently Disable Inactive and Terminated User Accounts

El Paso Health did not disable one inactive network account as required and did not disable user access to the claims system within required timeframes for four terminated employees. El Paso Health disabled two of the four accounts prior to audit fieldwork and disabled the other two when identified by the OIG Audit Division. El Paso Health did conduct annual reviews of access to its network and claims application.

IS-Controls requires the information system to automatically disable inactive accounts within 90 days[7] and the organization to revoke and disable information system access prior to or during the employee termination process.[8] Further, El Paso Health's policy requires the Information Service Department to process the employee technology access form, which is used to request granting, modification, or termination of employee access, within 24 hours of receipt.[9]

Disabling inactive accounts and accounts associated with terminated employees timely reduces the risk that a terminated individual could continue to access IT systems including the claims application. While disabled network accounts reduce the risk that a terminated individual could continue to access the claims application, the risk that an internal user could exploit unused active accounts remains. Failure to consistently disable inactive and terminated user accounts within the claims application and the network places confidential HHS System information at risk of unauthorized access, modification, or destruction.

Recommendation 1

El Paso Health should take appropriate action to address the inactive account and ensure access for terminated employees is disabled in accordance with IS-Controls requirements.

Management Response

Action Plan

El Paso Health will ensure that inactive network accounts are disabled. To enhance this process, El Paso Health will create an automation script to deactivate the accounts automatically. This process will further ensure that accounts with no activity within 90 days are expeditiously inactivated from within our network.

El Paso Health will ensure that access is simultaneously terminated within the claims management information system at the same time we terminate the users' active directory account from within our network. El Paso Health attests that they have adjusted their processes to ensure that this requirement is currently met.

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

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

[9] El Paso Health policy and procedure, MIS 1.4, Changes in User Access or Rights (Aug. 22, 2017).

Responsible Managers

- *Chief Information Officer*
- *Director of Systems and Network*

Target Implementation Date

June 2020

Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of IT 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 system components, network topology, and the local placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Issue 2: El Paso Health Should Develop Baseline Configurations

El Paso Health did not maintain documented baseline configurations for its servers containing confidential HHS information. IS-Controls requires the organization to develop, document, and maintain a current baseline of the information system's configuration controls.[10] 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.

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

El Paso Health 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, El Paso Health 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 2

El Paso Health should establish and document baseline configurations for servers as well and any other network devices that store and process confidential HHS System information.

Management Response

Action Plan

El Paso Health will create baseline configurations for our servers. The baseline configurations for servers will be added to Section 11 Data Repositories Inventory, Risk, and Priority section of the Disaster Recovery Plan. A new sub-section will be added named 11.2 Server Baseline Configurations.

Responsible Managers

- *Chief Information Officer*
- *Director of Systems and Network*

Target Implementation Date

July 2020

Media Protection

Sanitization prior to the disposal of media devices, including but not limited to backup tapes, external or removable hard disk drives, flash drives, and digital video media, is a key control in preventing the retrieval of residual data on media that is at the end of its life cycle. Consequently, the application of effective sanitization techniques is a critical aspect of ensuring that sensitive data is effectively protected by an organization against unauthorized disclosure.

In order for an organization to appropriately safeguard information, it must ensure proper disposal of assets and used media. Documented policies and procedures (a) facilitate the implementation of approved methods for sanitization and protection of media and confidential information and (b) are necessary to ensure information is properly secured and then disposed when no longer needed.

Issue 3: El Paso Health Did Not Document Procedures for Media Sanitization and Protection

El Paso Health did not maintain documented procedures for sanitizing media in accordance with applicable federal, state, and organizational policies prior to disposal or reuse outside of organizational control.

IS-Controls requires the organization to develop, document, and disseminate procedures to applicable personnel to facilitate the implementation of the media protection policy and associated media protection controls.[11] The organization is required to sanitize digital media prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal, state, and organizational standards and policies.[12]

El Paso Health had policies in place requiring appropriate disposal and sanitization of equipment but had not documented the specific procedures employed to ensure the effective and authorized methods for sanitization of equipment were followed. Because El Paso Health did not have documented procedures, it could not ensure IT staff sanitized and destroyed media in a consistent and reliable manner to confirm that confidential information was appropriately safeguarded from unauthorized exposure.

Recommendation 3

El Paso Health should document procedures for the sanitization of media and the destruction of confidential HHS information.

Management Response

Action Plan

El Paso Health will create a standard operating procedure (SOP) listing the step-by-step procedures used to sanitize media according to our MIS 4.9 Physical Safeguards Device and Media Controls policy.

[11] HHS Information Security Controls, Appendix B, MP-01, v. 1.0 (Feb. 9, 2018).

[12] HHS Information Security Controls, Appendix B, MP-06, v. 1.0 (Feb. 9, 2018).

Responsible Managers

- *Chief Information Officer*
- *Director of Systems and Network*

Target Implementation Date

July 2020

CONCLUSION

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

The OIG Audit Division concluded that El Paso Health:

- Complied with IS-Control requirements related to information security oversight, systems monitoring, risk management, and workforce training.
- Maintained business continuity and disaster recovery plans and policies to enable business processes to continue in case of an emergency, including training personnel, testing of the disaster recovery plan, and storing backup tapes off-site.
- Did not consistently manage user access to information systems that contained confidential HHS System information by timely disabling user accounts after 90 days for non-privileged accounts and timely deactivating user accounts during the termination process.
- Did not maintain baseline configurations of information systems, which are used to process, transmit, and house confidential HHS System information.
- Did not maintain documented procedures to guide destruction and sanitization of media housing confidential HHS System information.

The OIG Audit Division offered recommendations which, when implemented, will result in El Paso Health having:

- Timely termination of user access.
- Stronger controls over user accounts with access to confidential HHS System information.
- Established baseline server configurations that are implemented for systems that store and process confidential HHS System information.
- Consistent, documented processes ensuring the effective sanitization and destruction of media and confidential HHS System information.

For instances of noncompliance identified in this audit report, MCS may consider tailored contractual remedies to compel El Paso Health to meet contractual requirements related to protecting confidential HHS System information. In addition, audit findings in this report may be subject to OIG administrative enforcement measures, including administrative penalties. [13, 14]

The OIG Audit Division thanks the management and staff of MCS, HHSC IT Health Services Systems, HHS Information Systems Security, and El Paso Health for their cooperation and assistance during this audit.

[13] 1 Tex. Admin. Code § 371.1603 (May 1, 2016).

[14] Tex. Hum. Res. Code § 32.039 (Apr. 2, 2015).

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		
AC-02	Account Management	CE	1
AC-03	Access Enforcement		
AC-04	Information Flow Enforcement		
AC-06	Least Privilege		
Awareness and Training (AT)			
AT-01	Security Awareness and Training Policy and Procedures		
AT-02	Security Awareness Training		
Security Assessment and Authorization Control (CA)			
CA-01	Security Assessment and Authorization Policy and Procedures		
CA-02	Security Assessments		
Configuration Management (CM)			
CM-01	Configuration Management Policy and Procedures		
CM-02	Baseline Configuration	CD, CE	2
CM-03	Configuration Change Control		
Contingency Planning (CP)			
CP-01	Contingency Planning Policy and Procedures		
CP-02	Contingency Plan		
CP-03	Contingency Training		
CP-04	Contingency Plan Testing		
CP-06	Alternate Storage Site		
CP-07	Alternate Processing Site		
CP-08	Telecommunications Services		
CP-09	Information System Backup		
Identification and Authentication (IA)			
IA-01	Identification and Authentication Policy and Procedures		
IA-02	Identification and Authentication [Organization Users]		
IA-05	Authenticator Management		
IA-08	Identification and Authentication [Non-organizational Users]		
Incident Response (IR)			
IR-01	Incident Response Policy and Procedures		

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
IR-03	Incident Response Testing		
IR-04	Incident Handling		
IR-08	Incident Response Plan		
Maintenance (MA)			
MA-01	System Maintenance Policy and Procedures		
Media Protection (MP)			
MP-01	Media Protection Policy and Procedures	CE	3
MP-06	Media Sanitization	CE	3
Physical and Environmental Protection Controls (PE)			
PE-01	Physical and Environmental Protection Policy and Procedure		
PE-02	Physical Access Authorization		
PE-03	Physical Access Control		
Planning Controls (PL)			
PL-01	Security Planning Policy and Procedures		
PL-02	System Security Plan		
Information Security Program Plan (PM)			
PM-02	Senior Information Security Officer		
Personnel Security (PS)			
PS-01	Personnel Security Policy and Procedures		
PS-03	Personnel Screening		
PS-04	Personnel Termination	CE	1
PS-05	Personnel Transfer		
PS-07	Third-Party Personnel Screening		
PS-08	Personnel Sanctions		
Risk Assessment Control (RA)			
RA-01	Risk Assessment Policy and Procedures		
RA-02	Security Categorization		
RA-03	Risk Assessment		
RA-05	Vulnerability Scanning		
Systems and Communications Protection (SC)			
SC-01	System and Communications Protection Policy and Procedures		
SC-08	Transmission Confidentiality and Integrity		
SC-28	Protection of Information at Rest		
System and Information Integrity (SI)			
SI-01	System and Information Integrity Policy and Procedures		
SI-04	Information System Monitoring		

Appendix B: Report Team and Distribution

Report Team

OIG staff members who contributed to this audit report include:

- Audrey O'Neill, CIA, CFE, CGAP, Chief of Audit
- Kacy J. VerColen, CPA, Assistant Deputy Inspector General 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
- Ashley Rains, CFE, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Phil Wilson, Acting Executive Commissioner
- Victoria Ford, Acting Chief Operating Officer and Chief Policy and Regulatory Officer
- Karen Ray, Chief Counsel
- Michelle Alletto, Chief Program and Services Officer
- Nicole Guerrero, Director of Internal Audit
- Stephanie Muth, State Medicaid Director, Medicaid and CHIP Services
- Camisha Banks, Interim Director, Managed Care and Compliance and Operations, Medicaid and CHIP Services
- Ricardo Blanco, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Leatha Marr, Director, HHSC IT Application Services
- Thuy Cao, HHS Chief Information Security Officer

El Paso Health

- Frank Dominguez, President and Chief Executive Officer
- Janel Lujan, Chief Operating Officer
- Rocio Chavez, Chief Compliance Officer
- Sharon Perkins, Chief Information Officer and HIPAA Security Officer
- Jesus Martinez, Director of Systems and Network

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
- Juliet Charron, Chief of Strategy
- Quinton Arnold, Chief of Inspections and Investigations
- Steve Johnson, Chief of Medicaid Program Integrity

To Obtain Copies of OIG Reports

- OIG website: ReportTexasFraud.com

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
  Office of Inspector General
  P.O. Box 85200
  Austin, Texas 78708-5200
- Phone: 512-491-2000