TEXAS HEALTH AND HUMAN SERVICES COMMISSION

OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Amerigroup Texas, Inc.

November 30, 2018
OIG Report No. AUD-19-006

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

November 30, 2018

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Amerigroup Texas, Inc.

WHY THE OIG CONDUCTED THIS AUDIT

Amerigroup 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. As an MCO for Medicaid and CHIP program recipients, Amerigroup processes and pays medical provider claims, which contain protected health information and other confidential information. Amerigroup is required to protect and secure confidential Health Human Services (HHS) System information in accordance with criteria established in the Uniform Managed Care Contract (UMCC).

The OIG conducted this audit to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by Amerigroup.

WHAT THE OIG RECOMMENDS

Medicaid and CHIP Services (MCS) should consider tailored contractual remedies to address Amerigroup's delay in complying with the OIG Audit Division's request for information.

In addition, MCS should require Amerigroup to effectively review physical access logs on a monthly basis and update related internal policies in accordance with the HHS Information Security Standards and Guidelines.

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

WHAT THE OIG FOUND

Amerigroup designed and implemented effective security controls in all evaluated areas except for the frequency it reviewed access logs to its data center. Amerigroup, consistent with its internal policy, conducted quarterly reviews of data center access. Information Security Standards and Guidelines, however, requires monthly reviews of access logs.

Evidence Amerigroup initially provided for many of the security controls tested during this audit was limited, redacted, or not provided at all, preventing the OIG Audit Division from concluding on the effectiveness of those controls.

UMCC requires Amerigroup to provide the OIG Audit Division with access to (a) service locations, facilities, and installations, (b) records, and (c) software and equipment. Evidence obtained during a site visit at Amerigroup's headquarters in January 2018 and follow up WebEx sessions in February 2018, the scheduled period for audit fieldwork, enabled the OIG Audit Division to conclude on only 27 of 53 selected security controls. To achieve the audit objective and avoid reporting a scope limitation, the OIG Audit Division continued to coordinate with MCS and Amerigroup to obtain evidence on the remaining 26 controls.

In June 2018, Amerigroup provided information needed to conclude on the 26 controls. However, the OIG Audit Division cannot conclude whether the information provided in June 2018 represented Amerigroup's information security position at the time of the audit site visit in January 2018.

MCS agreed with the audit recommendations and detailed the actions it has planned to implement them. Amerigroup, in a comment letter included in Appendix D of the report, did not agree that it failed to respond timely to information requests and indicated it considered OIG Audit Division information requests to be excessive and unnecessary. Auditor comments follow the Amerigroup comment letter.

LESSONS LEARNED

HHSC and MCOs must collaborate to ensure the security of confidential HHS System information processed and stored by an MCO is sufficient to meet information technology (IT) security standards required by state and federal regulations. Weaknesses in the design or implementation of IT security controls for MCO systems that contain confidential HHS System information create a risk that IT security controls do not provide sufficient safeguards to protect confidential HHS System information from accidental or unauthorized access, loss, or disclosure.

TABLE OF CONTENTS

INTRODUCTION

The Texas Health and Human Services Commission (HHSC) Office of Inspector General (OIG) Audit Division conducted an audit of security controls over confidential Health and Human Services (HHS) System information at Amerigroup Texas, Inc. (Amerigroup). Amerigroup 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. Amerigroup processes and pays Medicaid and CHIP managed care provider claims, which contain confidential data, including protected health information. Amerigroup 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 Amerigroup was protected from unauthorized access, loss, or disclosure.

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

Objective and Scope

The audit objective was to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by Amerigroup.

The audit scope included the design and operating effectiveness of Amerigroup's information technology (IT) controls from September 2016 through November 2017, including:

- Selected logical security controls implemented to protect access to data in the Facets application database, data warehouses, and servers in the production environment.
- Physical security over IT infrastructure.
- General controls supporting backup and recovery activities.
- Controls for user account management, information system monitoring, and physical access to the data center.

Background

Amerigroup coordinates health services for members in the Medicaid State of Texas Access Reform (STAR) and CHIP programs, and supports Medicaid and CHIP (a) provider claims processing and (b) provider and member benefits administration. The Facets application adjudicates, pays, and stores provider claims information. The Facets application also provides explanations of benefits to Amerigroup providers and members.

Claims information is stored on an Oracle database and replicated daily to Amerigroup's data warehouses,[1] where it is accessed by Amerigroup'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 off site.

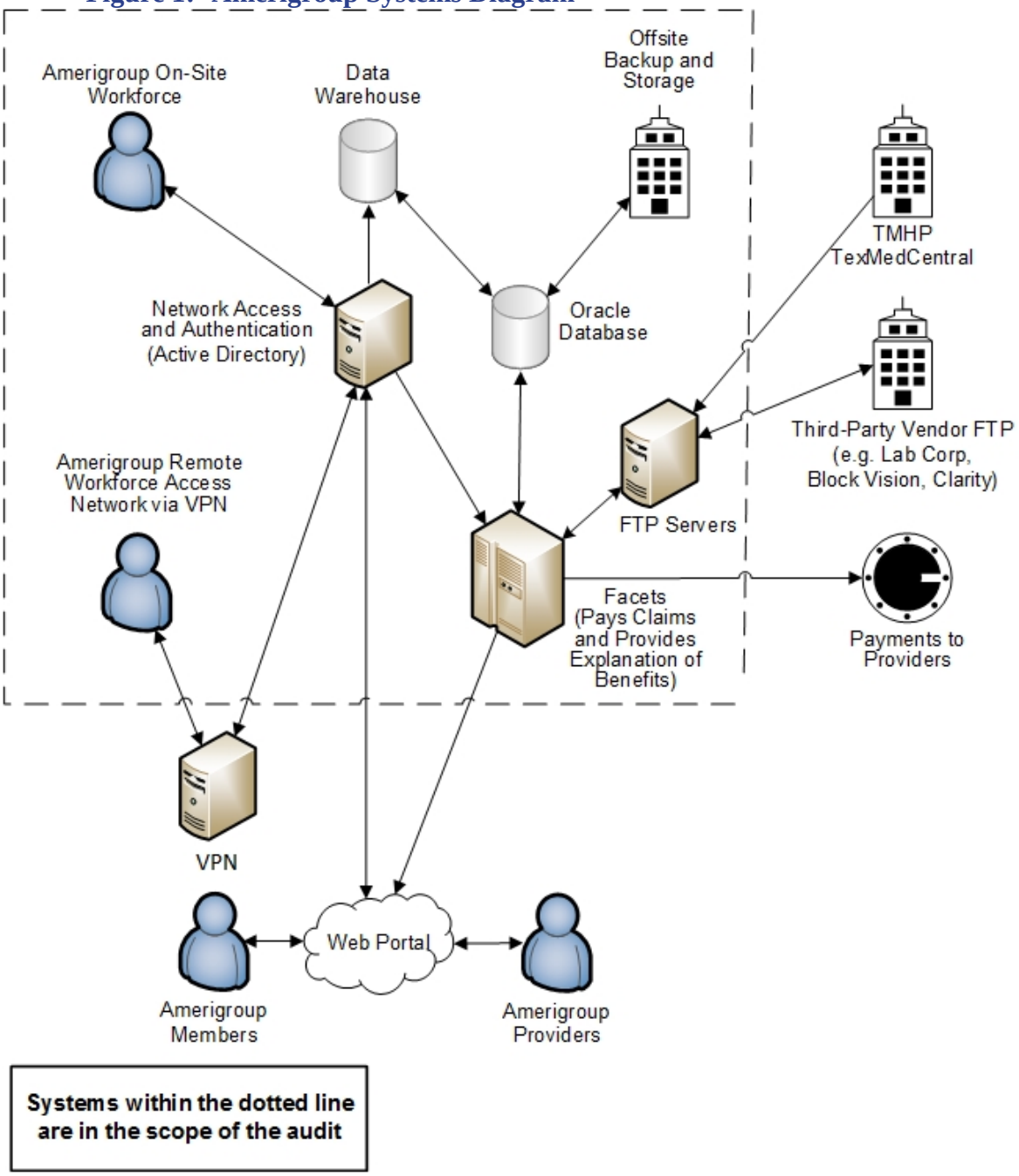
To access the Facets application, Amerigroup's workforce authenticate through Active Directory[2] to an internal company network. When working remotely, the workforce will first authenticate to the network via a Virtual Private Network (VPN) and then authenticate through Active Directory. To access the Facets application, all workforce authenticate using separate credentials. Amerigroup receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) and other third parties through secure file transfers using TexMedCentral.

A diagram of these systems is illustrated in Figure 1.

[1] A "data warehouse" is a type of database that contains copies of transaction data from one or more systems.

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

Figure 1: Amerigroup Systems Diagram



Source: OIG Audit Division

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

Amerigroup's data center provides the facility and IT infrastructure for the Facets application. The OIG Audit Division performed a physical security review at this

location. Amerigroup's data backup activities were also included in the scope of this audit.

Medicaid and CHIP Services (MCS), HHSC IT, and Amerigroup share accountability for safeguarding confidential HHS System information from accidental or unauthorized access, loss, or disclosure. The Uniform Managed Care Contract (UMCC) requires MCOs to submit a system security plan annually for HHSC's review and approval.[3] A well-designed system security plan contains detailed management, operational, and technical information about a system, its security requirements, and the controls implemented to provide protection against risks and vulnerabilities. Additionally, UMCC requires MCOs to comply with applicable laws, rules, and regulations regarding information security,[4] including but not limited to:

- Health and Human Services Information Security Standards and Guidelines (ISSG),[5] which includes the Security Controls Catalog
- Title 1, Sections 202.1 and 202.3 and Subchapter B, Texas Administrative Code (TAC)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[6]

Security controls must follow guidance provided in the ISSG catalog of security controls, which is based on the National Institute of Standards and Technology (NIST) security standards. The OIG Audit Division applied criteria, represented by the ISSG guidelines and Amerigroup's Workforce Information Security Program. Audit work included (a) a detailed review of policies and procedures to gain an understanding of the design of controls, (b) an on-site visit to observe security controls and the physical dispensation of assets and inventory, and (c) tests of key controls and related activities stored and processed by Amerigroup's Facets 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 the ISSG-defined groupings of security controls. Each control group contains multiple controls,

[3] Uniform Managed Care Contract, Attachment A, § 8.1.18.2, v. 2.19 (Sept. 1, 2016) through v. 2.24 (Sept. 1, 2017).

[4] Uniform Managed Care Contract, Attachment A, § 11.08, v. 2.19 (Sept. 1, 2016) through v. 2.24 (Sept. 1, 2017).

[5] In February 2018, the title of this document was changed to Information Security Controls.

[6] Regulations implementing HIPAA are found at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C (2013).

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 Control Groups
Information Security Oversight and Risk Management	Planning Risk Assessment
Information Integrity	System and Information Integrity System and Communications Protection
User Account Management	Access Control Identification and Authentication
Configuration Management	Configuration Management
Contingency Planning	Contingency Planning
Incident Response	Incident Response
IT Security Policies and Procedures	All
Vulnerability Assessment and Remediation	Security Assessment and Authorization
Personnel Security	Personnel Security
Physical Security	Physical and Environmental Protection

Source: Prepared by the OIG Audit Division based on ISSG

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

The OIG Audit Division examined the IT security controls and relevant activities supporting data security at Amerigroup. Audit work included (a) detailed tests of activities, supporting technologies, and data and (b) a site visit to the location where key activities were performed and data was stored. Third-party subcontractors such as Block Vision, the vision benefits management vendor for Amerigroup, were not included in the scope of this audit.

The OIG Audit Division presented audit results, issues, and recommendations to MCS and to Amerigroup in a draft report dated October 10, 2018. Each was provided with the opportunity to study and comment on the report. MCS management responses are included in the report following each recommendation.

MCS agreed with the audit recommendations and detailed the actions it has planned to implement them.

Amerigroup, in a comment letter included in Appendix D of the report, did not agree that it failed to respond timely to information requests and indicated it considered OIG Audit Division information requests to be excessive and unnecessary. Auditor comments follow the Amerigroup comment letter.

AUDIT RESULTS

The OIG Audit Division obtained and evaluated information provided by Amerigroup related to access controls, physical security, data backup, and risk assessment during the scheduled fieldwork period. However, Amerigroup initially provided limited, redacted, or no information at all in response to the majority of requests for evidence of activities and controls in place to protect confidential HHS System information. Amerigroup did not provide the outstanding information until June 2018, six months after the OIG Audit Division initially requested the information. A timeline of events is included in Table 2.

Amerigroup designed and implemented effective security controls in all evaluated areas except for the frequency it reviewed access logs to its data center.

ACCESS TO INFORMATION

Issue 1: Amerigroup Limited and Delayed Access to Information

UMCC requires Amerigroup to provide the OIG Audit Division with access to (a) service locations, facilities, and installations, (b) records, and (c) software and equipment. In addition, Amerigroup must provide any assistance that the OIG Audit Division reasonably requires to complete its audit.[7] UMCC provides that an MCO's failure to respond to an OIG request for information in the manner and format requested may result in an assessment of liquidated damages up to $1,000 per day, per MCO program, for each day of noncompliance.[8]

The OIG Audit Division requested information from Amerigroup needed to evaluate the design and effectiveness of security controls over the confidential HHS System information processed and stored in the Amerigroup data center as outlined in Table 2.

[7] Uniform Managed Care Contract, Attachment A, § 9.03, v. 2.24 (Sept. 1, 2017) through v. 2.25 (Mar. 1, 2018).

[8] Uniform Managed Care Contract, § 8.1.19.2 and Attachment B-3 § 24, v. 2.24 (Sept. 1, 2017) through v. 2.25 (Mar. 1, 2018).

Table 2: Summary of OIG Audit Division Activities

November 2017
• Audit Notification informing Amerigroup of the IT security audit. • Entrance Conference with Amerigroup, which included discussion of the audit objective, scope, methodology, and evidence that will be requested.
December 2017
• Initial Information Request submitted to Amerigroup specifying types of evidence needed to meet professional auditing standards. • Enagagment Letter informing Amerigroup of the final audit scope, objective, and methodology, and confirming the January site visit to test processes and controls and obtain audit evidence.
January 2018
• On-site testing and observation of controls at Amerigroup out-of-state headquarters location. • Amerigroup informed the OIG Audit Division for the first time that certain requested information would not be provided. • Ongoing discussions related to information not yet provided by Amerigroup.
February 2018
• WebEx session held to test controls and obtain additional audit evidence. Key information requests remain outstanding.
Februrary through June 2018
• Ongoing discussions related to information not yet provided by Amerigroup.
June 2018
• Amerigroup held WebEx session to demonstrate controls and provided remaining information and evidence needed to complete audit.

Source: OIG Audit Division

The OIG Audit Division requested information supporting the policies and procedures Amerigroup set forth to protect confidential HHS System information including access control documentation, system configuration settings, user logs, and other information relating to the security controls under review. The OIG Audit Division conducted a site visit in January 2018 at Amerigroup headquarters and held a WebEx session in February 2018 to observe key processes and controls. Based on evidence obtained during the site visit and WebEx session, the OIG Audit Division determined that 27 of the 53 selected security controls were designed appropriately. However, evidence provided by Amerigroup for the remaining 26 security controls was limited, redacted, or not provided at all, preventing the OIG Audit Division from concluding on the effectiveness of those controls.

Table 3 indicates the controls for which the OIG Audit Division was unable to make a determination of the effectiveness of the control based on the information initially provided.

Table 3: Security Controls for Which Amerigroup Initially Did Not Provide or Only Partially Provided Information

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)
AC-1	Policy and Procedures	CE
AC-2	Account Management	CE
AC-5	Separation of Duties	CE
AC-6	Least Privilege	CE
AC-7	Unsuccessful Logon Attempts	CE
AC-11	Session Lock	CE
AC-12	Session Termination	CE
CA-2	Security Assessments	CE
CM-1	Configuration Management Policy and Procedures	CE
CM-2	Baseline Configuration	CE
CM-4	Security Impact Analysis	CE
CM-5	Access Restrictions for Change	CE
CM-6	Configuration Settings	CE
CM-7	Least Functionality Priority/Baseline	CE
CM-8	Information System Component Inventory	CE
CP-3	Contingency Training	CE
IA-5(1)	Authenticator Management (Password-based Authentication)	CE
IR-4	Incident Handling	CE
IR-5	Incident Monitoring	CE
IR-6	Incident Reporting	CE
PE-3	Physical Access Control	CD,CE
PE-6	Monitoring Physical Access	CD,CE
SC-4	Information in Shared Resources	CE
SC-8	Transmission Confidentiality and Integrity	CE
SC-10	Network Disconnect	CE
SC-13	Cryptographic Protection	CE

Source: OIG Audit Division

The OIG Audit Division and Amerigroup held a WebEx session in June 2018, where Amerigroup provided screen shots and demonstrations of most of the data that was outstanding. The remaining data was then provided via secure file transfer later that month. The OIG Audit Division accepted, evaluated, and concluded on the additional information provided. However, the OIG Audit Division cannot conclude whether the information provided in June 2018 represented Amerigroup's information security position at the time of the audit site visit in January 2018.

After the additional non-redacted items were provided in June 2018, all outstanding controls were reviewed and the evidence provided was considered sufficient and appropriate to conclude on the effectiveness of the controls, with the exception of physical security controls, which is covered in Issue 2.

UMCC states that Amerigroup "must respond to Office of Inspector General request for information in the manner and format requested." HHSC may assess up to $1,000 per day that the information is not submitted, is late, inaccurate, or incomplete.[9]

Recommendation 1

MCS, through its contract oversight responsibility, should consider tailored contractual remedies to address Amerigroup's delay in complying with the OIG Audit Division's request for information.

Management Response

Action Plan
MCS agrees with the recommendation and will consider contractual remedies to address Amerigroup's five and one-half-month delay in complying with the OIG Audit Division's request for information.

Responsible Manager
Director, Managed Care Compliance and Operations

Target Implementation Date
August 31, 2019

PHYSICAL SECURITY

Issue 2: Physical Access Logs Were Not Reviewed Monthly

ISSG requires Amerigroup to review data center physical access logs once a month.[10] While on site in January 2018, the OIG Audit Division reviewed Amerigroup policy and logs to determine whether this requirement was met. Audit results indicated that Amerigroup performed quarterly, instead of monthly, reviews of physical access logs.

[9] Uniform Managed Care Contract, Attachment B-1, § 8.1.19.2 and Attachment B-3, § 24, v. 2.19 (Sept. 1, 2016) through v. 2.24 (Sept. 1, 2017).

[10] HHS Information Security Standards and Guidelines Controls Catalog, § 7.11, PE-6(b), v. 6 (Sept. 21, 2015).

Amerigroup Did Not Review Physical Access Logs Monthly

Amerigroup's Workforce Information Security Program requires that data center physical access logs be reviewed on a quarterly basis. This policy is not consistent with ISSG, which requires monthly review of physical access logs.[11]

By conducting quarterly rather than monthly reviews of physical access logs, Amerigroup may not timely detect unauthorized access to its data center leaving confidential HHS System information at risk of unauthorized access, loss, and disclosure.

Recommendation 2

MCS, through its contract oversight responsibilities, should require Amerigroup to effectively review physical access logs on a monthly basis and update internal policies in accordance with ISSG.

MCS should consider tailored contractual remedies to compel Amerigroup to comply with monthly physical access log review requirements.

Management Response

Action Plan
MCS agrees with the recommendation. MCS will allow Amerigroup 20 business days from receipt of the final audit report to submit a corrective action plan (CAP). MCS will require Amerigroup to effectively review physical access logs on a monthly basis and provide update internal policies in accordance with Health and Human Services IS- Controls (formerly the Information Security Standards and Guidelines (ISSG)).

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

Target Implementation Date
March 2019

[11] HHS Information Security Standards and Guidelines Controls Catalog, § 7.11, PE-6(b), v. 6 (Sept. 21, 2015).

CONCLUSION

The OIG Audit Division completed an audit of selected security controls over confidential HHS System information in the custody of Amerigroup. The audit included an evaluation of IT security controls over the Facets application and its operating environment. The OIG Audit Division conducted a site visit at Amerigroup in January 2018 and held WebEx sessions in February and June 2018.

The OIG Audit Division concluded:

- Overall, security controls designed to protect confidential HHS System information from unauthorized access, loss, and disclosure were sufficient.

- Amerigroup did not provide requested information and evidence needed to achieve the audit objective, as required by contract, until after the on-site field visit was conducted. Although the OIG Audit Division accepted, evaluated, and concluded on the information provided in June 2018, the information does not represent Amerigroup's information security position at the time of the audit in January 2018.

- Amerigroup conducted quarterly, rather than monthly, reviews of data center access logs.

The OIG Audit Division offered recommendations which, if implemented, will result in stronger Physical Protection Controls to Amerigroup's data center to protect confidential HHS System information from unauthorized access, loss, and disclosure.

The OIG Audit Division thanks the management and staff of MCS, HHSC IT, and Amerigroup for their cooperation and assistance during this audit.

Appendix A: Objective, Scope, Methodology, Criteria, and Auditing Standards

Objective

The objective of this audit was to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by Amerigroup.

Scope

The scope of this audit included the design and operating effectiveness of Amerigroup's IT controls from September 2016 through November 2017, including:

- Selected logical security controls implemented to protect access to data in the Facets application database, data warehouses, and servers in the production environment.
- Physical security over IT infrastructure.
- General controls supporting backup activities.
- Controls for user account management, information system monitoring, and physical access to the data center.

Methodology

To accomplish its objectives, the OIG Audit Division collected information through discussions and interviews with responsible staff at HHSC and Amerigroup, and reviewed the following documentation:

- IT security policy and procedures
- System security plans
- Service organization control reports
- Network penetration reports

The OIG Audit Division issued an engagement letter to Amerigroup on December 27, 2017, providing information about the upcoming audit, conducted fieldwork at Amerigroup's facility in Virginia Beach, Virginia, on January 8, 2018, through January 10, 2018. While on site, the OIG Audit Division interviewed responsible personnel, tested logical security controls, conducted a physical security inspection of the data center, and reviewed relevant documentation. On February 9, 2018, and June 14, 2018, the OIG Audit Division held WebEx sessions

with Amerigroup to observe security controls. In the February 2018 session, Amerigroup provided limited documentation, reports, and scans. In June 2018, Amerigroup provided additional supporting documentation.

Criteria

The OIG Audit Division used the following criteria 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. 2.19 (2016) through v. 2.25 (2018)
- HHS Information Security Standards and Guidelines Controls Catalog, v. 6 (2015)

Auditing Standards

Generally Accepted Government Auditing Standards

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

ISACA

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

Appendix B: Testing Methodology

The OIG Audit Division examined Amerigroup IT security controls that were in effect during the period from September 2016 through November 2017. After performing a risk and controls assessment of Amerigroup's documented IT security control structure, the OIG Audit Division performed testing of selected security controls over Amerigroup's production environment and supporting infrastructure.

Information Security Oversight and Risk Management

The OIG Audit Division reviewed Amerigroup's information security oversight review and approval process of system security controls and risk management. Additionally, the OIG Audit Division reviewed the risk management plan and associated risk assessment for Amerigroup to verify the information system environment.

Information Integrity

The OIG Audit Division reviewed data transfer protocols intended to protect the integrity and reliability of confidential HHS System information exchanged with third parties.

User Account Management

The OIG Audit Division reviewed controls over user access to determine whether controls were in place, adequately designed, and operating effectively, and whether privileged access to information systems was appropriate.

Configuration Management

The OIG Audit Division interviewed Amerigroup personnel and examined applicable IT policies and system configurations.

Contingency Planning

The OIG Audit Division reviewed Amerigroup's activities related to physical security of backup tapes and interviewed responsible personnel to determine the effectiveness of the back-up activities.

Incident Response

The OIG Audit Division interviewed Amerigroup personnel and examined supporting documentation to (a) determine whether virus management and network analytic tools were implemented and monitored to review the movement of data

and use of the network by its workforce and (b) identify processes for monitoring and responding to security events on the Amerigroup network.

The OIG Audit Division requested Amerigroup's incident response plan and interviewed responsible personnel to determine the effectiveness of procedures for incident monitoring and responding, including incident response testing.

IT Security Policies and Procedures

The OIG Audit Division reviewed Amerigroup's Workforce Information Security Program and associated policies to determine if the policies were updated to reflect current processes and implemented as stated.

Vulnerability Assessment and Remediation

The OIG Audit Division reviewed the logs of the most recent vulnerability and risk assessments conducted by Amerigroup to determine whether the remediation process associated with those assessments appeared designed to address identified risks.

Personnel Security

The OIG Audit Division performed a review of data center access logs and human resources employment reports to determine whether access was disabled upon termination of employment.

Physical Security

The OIG Audit Division performed a physical security inspection of the Amerigroup data center and evaluated physical access logs determine whether access was limited to authorized workforce and visitors.

Appendix C: Controls Tested

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
Access (AC) Controls			
AC-1	Policy and Procedures		
AC-2	Account Management		
AC-2(3)	Disable Inactive Accounts		
AC-5	Separation of Duties		
AC-6	Least Privilege		
AC-6(1)	Authorize Access to Security Functions		
AC-6(5)	Privileged Accounts		
AC-7	Unsuccessful Logon Attempts		
AC-11	Session Lock		
AC-12	Session Termination		
AC-17	Remote Access		
Security Assessment and Authorization (CA) Controls			
CA-1	Security Assessment and Authorization Policy and Procedures		
CA-2	Security Assessments		
CA-5	Plan of Action and Milestones		
CA-6	Security Authorization		
CA-7	Continuous Monitoring		
Configuration Management (CM) Controls			
CM-1	Configuration Management Policy and Procedures		
CM-2	Baseline Configuration		
CM-3	Configuration Change Control		
CM-4	Security Impact Analysis		
CM-5	Access Restrictions for Change		
CM-6	Configuration Settings		
CM-7	Least Functionality Priority/Baseline		
CM-8	Information System Component Inventory		
CM-9	Configuration Management Plan		
Contingency Planning (CP)			
CP-9	Information System Backup		
Identification and Authentication (IA) Controls			
IA-1	Identification and Authentication Policy and Procedures		
IA-2	Identification and Authentication [Organization Users]		
IA-3	Device Identification and Authentication		

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
IA-5(1)	Authenticator Management (Password-based Authentication)		
IA-8	Identification and Authentication [Non-organizational Users]		
Incident Response (IR) Controls			
IR-1	Incident Response Policy and Procedures		
IR-3	Incident Response Testing		
IR-4	Incident Handling		
IR-5	Incident Monitoring		
IR-6	Incident Reporting		
IR-8	Incident Response Plan		
Physical and Environmental Protection (PE) Controls			
PE-3	Physical Access Controls		
PE-6	Monitoring Physical Access	CD,CE	2
PE-6(1)	Intrusion Alarms/Surveillance Equipment		
PE-8	Visitor Access Records		
Planning (PL) Controls			
PL-1	Security Planning Policy and Procedures		
PL-2	System Security Plan		
Personnel Security (PS) Controls			
PS-1	Personnel Security Policy and Procedures		
PS-4	Personnel Termination		
Risk Assessment (RA) Controls			
RA-1	Risk Assessment Policy and Procedures		
RA-2	Security Categorization		
RA-3	Risk Assessment		
RA-5	Vulnerability Scanning		
System and Communications Protection (SC) Controls			
SC-4	Information in Shared Resources		
SC-8	Transmission Confidentiality and Integrity		
SC-10	Network Disconnect		
SC-13	Cryptographic Protection		

Appendix D: Amerigroup Comment Letter

Amerigroup
An Anthem Company

November 28, 2018
Steve Sizemore, Performance Audit Director
Office of the Inspector General
Texas Health and Human Services Commission
11501 Burnet Rd., Bldg. 902
Austin, TX 78758

Re: Response to Draft Office of Inspector General (OIG) Report Dated October 10, 2018

Dear Mr. Sizemore,

Amerigroup is committed to collaborating fully with the Texas Health and Human Services Commission to protect and secure confidential Health and Human Services (HHS) information, including protected health information and other confidential information. Amerigroup values its partnership with HHS greatly but must respectfully disagree with the content contained in the draft OIG report dated October 10, 2018. We greatly appreciate the opportunity to summarize Amerigroup's perspective on the audit report and anticipate that OIG will have an opportunity to evaluate the facts contained within and update the draft OIG report accordingly.

Consistent with company and industry practices, Amerigroup responded by quickly assessing the documentation requested by the OIG reviewers, identifying which items could be provided directly and which items were best addressed through alternative means including partially redacted records, onsite review and online meeting review (Webex) given the confidential nature of such information. However, the level of required documentation exceeded any prior review request within our organization (of which our organization responds to over 20,000 annually). We firmly believe the OIG reviewers could have documented their review of items and determination of their adequacy without separately seeking actual copies of the materials.

Recognizing the cybersecurity risks that exist in the world today, Amerigroup appreciates OIG's goal of verifying the security of the information. One of the ways that Amerigroup works to address these interests is by maintaining HITRUST certification, which is obtained through the HITRUST CSF Assurance Program, the most widely-used information security framework used by United States health care organizations. Amerigroup's HITRUST assessment is performed by an independent, nationally recognized auditing firm and includes a total of 314 unique Baseline Security Control Statements that are assessed. Amerigroup's HITRUST assessment includes an

823 Congress Ave, Suite 1100
Austin, TX 78701
512.382.4970

www.amerigroup.com

Amerigroup
An Anthem Company

independent third party review of specific documentation, interviews with process and control owners, and substantive testing of controls based on certification assessment requirements. Amerigroup provided evidence of HITRUST certification to the TX OIG auditors for purpose of supporting the exam, however, the auditors declined to accept this evidence.

While it is true that Amerigroup continued to provide information over a period of multiple months, throughout the entire process, Amerigroup remained responsive to the OIG auditors, continuing dialog and always verifying that timeframes for response met auditor expectations. Key to the length of the timeframe are factors outside of Amerigroup's control which must be considered:

- On February 9th, a WebEx was held to review outstanding items. At the conclusion of the WebEx, a limited number of items were requested for follow-up. These requests were satisfied on February 15th. From February 15th through May 17th, OIG did not communicate that the follow up materials provided were insufficient.
- Throughout the process, Amerigroup continued to receive new requests, which had not been part of the original, or previous requests. This included the items sought in the May 17th Final Request.
- During the audit process, OIG audit staff leading/working the audit changed. Discussions and understanding reached with one auditor were not carried through the entire engagement which created a need to revisit prior discussions and evidence produced.
- For most requests, specific response timeframes were not provided. For each request that Amerigroup received, an agreed-upon timeframe was established between Amerigroup and the OIG auditors. Amerigroup is unaware of instances where these agreed upon due dates were missed.

Amerigroup has separately provided a summary timeline to the OIG which details the collaborative engagement which took place during the time period in question.

Overall, the report as written mischaracterizes Amerigroup's level of engagement in this review by implying that we failed to respond in a timely manner. Amerigroup appreciates that its efforts to coordinate the form and format of document review was challenging in light of OIG's desire to maintain copies of all documents. However, fundamentally both entities were focused on the same goal – confirming the development and consistent application of adequate security provisions to protect program information.

Amerigroup
An Anthem Company

Thank you again for the opportunity to respond to the draft audit report. We are available at your convenience to discuss these interests further and looking forward to our continued partnership and collaboration in support of the Texas Medicaid program.

Sincerely,

Tisch A. Scott

Auditor Comments

The OIG Audit Division appreciates and values the feedback provided by Amerigroup in its comment letter. The OIG Audit Division respectfully disagrees with Amerigroup's position that (a) information requests were excessive and unnecessary and (b) it responded timely to OIG Audit Division information requests, and offers the following comments in response to the Amerigroup letter.

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.

The OIG Audit Division understands and recognizes the sensitivity of security-related information, and worked extensively with Amerigroup to reach agreement on the type and extent of evidence that would be needed to achieve the audit's objectives while complying with professional auditing standards. These efforts began upon the audit's initiation in November 2017 and continued throughout the (a) information requests and other planning phase activities in December 2017, (b) fieldwork site visit in January 2018 where audit evidence was to be obtained and related follow up activities, and (c) WebEx session in June 2018 and subsequent Amerigroup submittal of audit evidence originally requested in December 2017.

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 and conclusions presented in this report.

Appendix E: Report Team and Distribution

Report Team

The OIG staff members who contributed to this audit report include:

- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Anton Dutchover, CPA, Audit Manager
- James A. Hicks, CISA, IT Audit Project Manager
- Daniel Graf, CISA, IT Audit Project Manager
- Brian Baker, 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
- Enrique Marquez, Chief Program and Services Officer, Medical and Social Services Division
- Karen Ray, Chief Counsel
- Karin Hill, Director of Internal Audit
- Stephanie Muth, State Medicaid Director, Medicaid and CHIP Services
- Grace Windbigler, Director, Managed Care Compliance and Operations, Medicaid and CHIP Services
- Steve Buche, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Shirley Erp, HHS Chief Information Security Officer

Amerigroup Texas

- Tisch Scott, President
- Bobbie Jo Jonas, Director, Regulatory Services

Appendix F: OIG Mission and Contact Information

The mission of the 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
- Anita D'Souza, Chief of Staff and Chief Counsel
- Olga Rodriguez, Chief Strategy Officer
- Christine Maldonado, Chief of Operations and Workforce Leadership
- Brian Klozik, Deputy IG for Medicaid Program Integrity
- Lizet Hinojosa, Deputy IG for Benefits Program Integrity
- David Griffith, Deputy IG for Audit
- Quinton Arnold, Deputy IG for Inspections and Investigations
- Alan Scantlen, Deputy IG for Data and Technology
- Judy Hoffman-Knobloch, Assistant Deputy IG for Medical Services

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 the 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