OFFICE OF INSPECTOR GENERAL

TEXAS HEALTH AND HUMAN SERVICES COMMISSION

AUDIT OF DADS CLAIMS MANAGEMENT SYSTEM

Information Technology Interface Processing Controls

February 28, 2017
IG Report No. IG-16-120

HHSC IG
TEXAS HEALTH AND HUMAN SERVICES COMMISSION
INSPECTOR GENERAL

AUDIT OF DADS CLAIMS MANAGEMENT SYSTEM

Information Technology Interface Processing Controls

WHY THE IG CONDUCTED THIS AUDIT

The Department of Aging and Disability Services (DADS) Claims Management System was developed to adjudicate Medicaid fee-for-service claims for the aging and disabled Medicaid recipients of Texas served by DADS long-term care program areas. Through the DADS Claims Management System, fee-for-service Medicaid providers bill for services delivered to Medicaid recipients.

The DADS Claims Management System consists of multiple adjudication systems that gather information from, and share information with, each other and other sources, then forward information to other systems for payment, all through the use of data interfaces. For claims to be adjudicated and paid correctly, interfaces must transmit data accurately and completely, and data must be protected from unauthorized access, modification, and deletion.

The objective of the audit was to evaluate the adequacy of IT interface processing controls designed to (a) ensure systems transmit information accurately and completely and (b) protect data from unauthorized access, modification, and deletion.

WHAT THE IG RECOMMENDS

HHSC IT and HHSC Contracted Community Services should continue to automate the transmittal of batch files, and improve controls that (a) ensure only contracted providers receive Medicaid payments and (b) prevent unauthorized access or modification to provider payment files.

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

WHAT THE IG FOUND

Claims payment files in the two largest claims adjudication systems within the DADS Claims Management System transmitted across interfaces with no errors, and controls were in place to omit duplicate claims and prevent duplicate payments.

The Intellectual Disability Client Assignment and Registration System (ID CARE) and the Texas and Medicaid Healthcare Partnership (TMHP) process about 97 percent of the claims in the DADS Claims Management System. These two systems collectively processed approximately $3.3 billion in medical claims payments in 2016.

Claims Management System	Claims Payments
Claims adjudicated through ID CARE	$ 1,179,291,403
Claims adjudicated through TMHP	2,116,610,806
All other claims adjudicated through other interfaces	101,503,454
Total	$ 3,397,405,663

Opportunities for improvement exist related to the completeness and accuracy of transmitted data and the security of data in motion.

Completeness and Accuracy of Transmitted Data

HHSC IT manually released job schedules, rather than allowing processing of batch files to be automatically released through the DADS Provider Payment System, a practice which could result in unnecessary delays or errors in processing. HHSC IT management resolved this issue before the completion of the audit by implementing automated release of job schedules for the transfer of files for the system the system.

Active and terminated contract information contained in the DADS Long-Term Care Provider System and in the TMHP system did not agree. Although no inappropriate payments occurred for the months tested, weaknesses in the control structure designed to ensure that only providers with current DADS contracts are paid for Medicaid claims could result in inappropriate provider payments.

Security of Data in Motion and at Rest

A machine account name and the associated account password were inappropriately published in system processing logs. The account had administrator access, making unauthorized access or modification to provider payment files possible. No evidence was found to indicate files were modified. The database administrator changed the password immediately after the audit team identified the issue.

Responsible management at HHSC acknowledged the findings of the report and agreed to implement corrective actions to continue to utilize the automated job scheduler, correct and monitor contracts in the Long-Term Care Provider system, ensure changes to scripts are monitored, and ensure that password requirements adhere to HHS IT policies.

LESSONS LEARNED

IT interfaces for adjudicating fee-for-service claims should maintain sufficient controls to protect data security and integrity. Managers of IT claims processing systems should routinely review workflows for inefficiencies and vulnerabilities. Routine reviews may guide prospective system improvements.

TABLE OF CONTENTS

INTRODUCTION 1

Background *1*

RESULTS, ISSUES, AND RECOMMENDATIONS 5

Completeness and Accuracy of Transmitted Data

Issue 1: **Automated Release of Batch Files For Processing Was Not Always Enabled** **5**

Recommendation 1 ..... *5*

HHSC Management Response *6*

Issue 2: **Control Weaknesses in the DADS Long-Term Care Provider System and in the TMHP System Could Allow Improper Provider Payments** **6**

Recommendations 2.1 - 2.3 ..... *8*

HHSC Management Response *8*

Security of Data in Motion and at Rest

Issue 3: **A DADS Provider Payment System Machine Account Name and Password Were Published in System Processing Logs** **9**

Recommendations 3.1 - 3.4 ..... *10*

HHSC Management Response *10*

CONCLUSION 12

APPENDICES 14

A: Objective, Scope, and Methodology *14*

B: Sampling Methodology *16*

C: Report Team and Report Distribution *18*

D: IG Mission and Contact Information *19*

INTRODUCTION

The Texas Health and Human Services Commission (HHSC) Inspector General (IG) Audit Division has completed an audit of Texas Department of Aging and Disability Services (DADS) Claims Management System Information Technology (IT) interfaces. The objective of the audit was to evaluate the adequacy of IT interface processing controls designed to (a) ensure systems transmit information accurately and completely and (b) protect data from unauthorized access, modification, and deletion. The audit did not include verification of the correctness and accuracy of the adjudication[1] and payment of each individual claim processed.

Background

Effective September 1, 2016, the section of DADS responsible for DADS Claims Management System IT interfaces was transferred to HHSC by legislative mandate. This action was part of a larger Health and Human Services (HHS) System transformation. As a result, issues and recommendations resulting from this audit will be directed to management at HHSC.

The DADS Claims Management System was developed to adjudicate Medicaid fee-for-service[2] claims for aging and disabled Medicaid recipients in Texas served by DADS long-term care program areas. Certain long-term care programs, referred to as long-term service and supports (LTSS) programs, provided through DADS have not yet transitioned to the managed care model.[3] Programs that are not provided through managed care are considered to be fee-for-service programs. Medicaid LTSS providers bill for services delivered to Medicaid recipients in fee-for-service programs through the DADS Claims Management System. Table 1 provides a summary of LTSS claims payments adjudicated through (a) the Intellectual Disability Client Assignment and Registration System (ID CARE), (b) the Texas and Medicaid Healthcare Partnership (TMHP), and (c) other fee-for-services claims interfaces within the DADS Claims Management System, in 2016.

[1] Adjudication is a process designed to determine whether claims should be paid or not.

[2] Medicaid fee-for-service was the original service delivery model for Texas Medicaid introduced in 1967. In this model, enrolled Medicaid providers are reimbursed retrospectively for a Medicaid eligible health care service or services provided to a Medicaid eligible patient.

[3] Managed care refers to a system of health care in which patients agree to visit only certain doctors and hospitals, and in which the cost of treatment is monitored by a managing company with the outcome focused on quality of care.

Table 1: Fee-For-Service Long-Term Care Claims Payments Adjudicated Through the DADS Claims Management System in 2016

Claims Management System	Claims Payments
Claims adjudicated through ID CARE	$ 1,179,291,403
Claims adjudicated through TMHP	2,116,610,806
All other claims adjudicated through other interfaces	101,503,454
Total	$ 3,397,405,663

Source: DADS Claims Management System

The IG Audit Division evaluated IT interfaces between systems used to process, adjudicate, and pay claims within ID CARE and TMHP. ID CARE interfaces support claims processing for certain Home and Community-based Services (HCBS) programs.[4] TMHP IT interfaces support claims processing for other long-term care programs. These systems collectively represent approximately $3.3 billion in Medicaid claims during 2016, accounting for approximately 97 percent of total DADS fee-for-service claims payments. The IG Audit Division examined interface processing controls over claims submitted during March and June 2016, totaling approximately $553 million.

DADS initiated an IT development project in 2010 to design and build a system that would transition the adjudication of claims for certain DADS HCBS[5] programs from the ID CARE system to TMHP. According to a State Auditor's Office report, the project halted in 2013 because of poorly identified business requirements, incompatible technologies, and underestimated complexity of the project.[6] Most of DADS claims processing for long-term care services had already transitioned to TMHP, which also manages Medicaid claims processing for several other HHS programs. Certain DADS HCBS programs remain reliant on ID CARE for claims processing, which uses a mainframe that remained under the operation of the DADS IT Division.

The frequency of claims payment processing differs between ID CARE and TMHP. ID CARE adjudicates claims on a weekly basis, while TMHP adjudicates claims daily. Both systems receive Medicaid eligibility information from the Texas Integrated Eligibility Redesign System (TIERS), and both systems process transactions through the Health and Human Services Accounting System (HHSAS) for payment by the Comptroller of Public Accounts

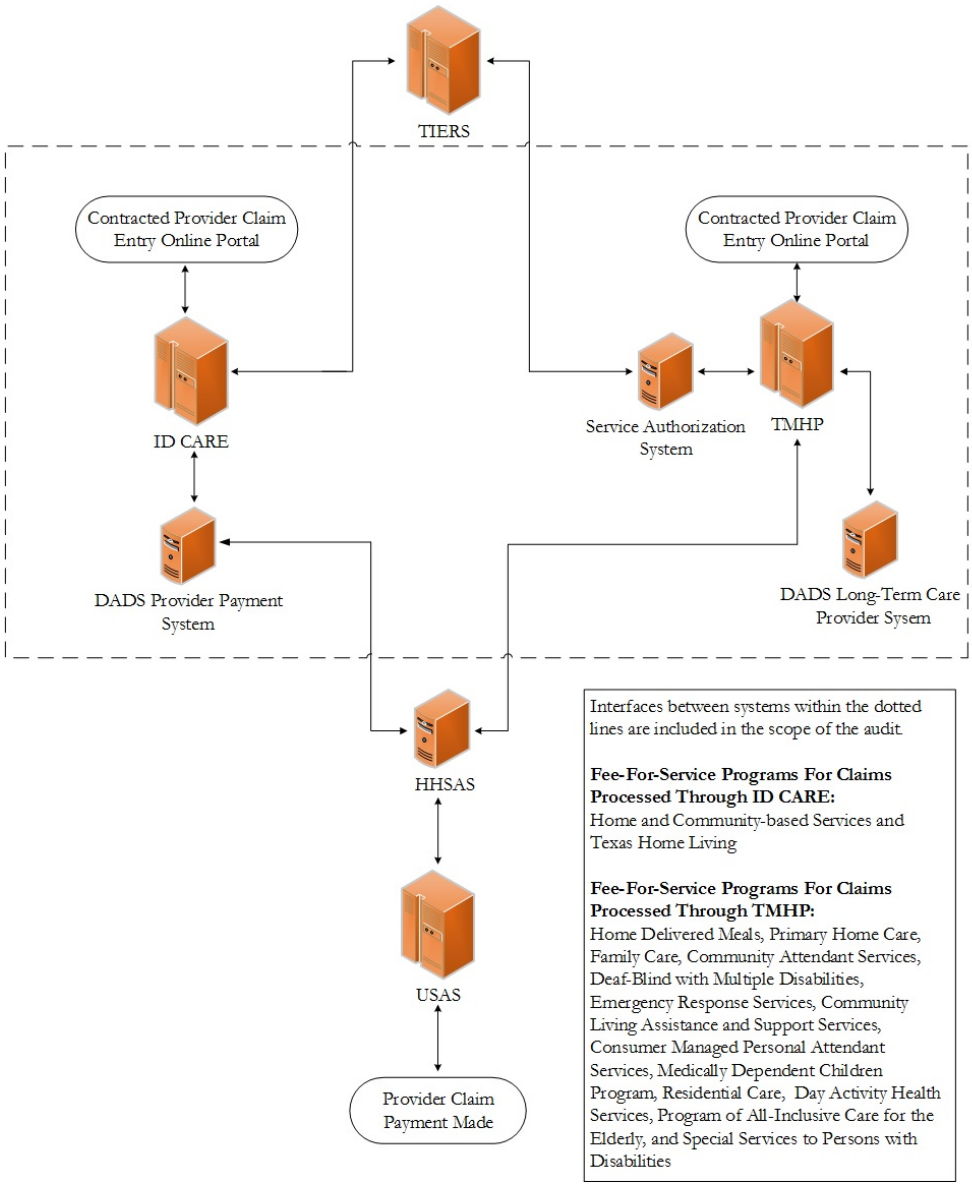
[4] Home and Community-based Services are programs that provide individualized services and supports to people with intellectual disabilities who are living with their families, in their own homes or, in other community settings as opposed to institutionalized settings.

[5] DADS HCBS programs relying on ID CARE include the Home and Community-based Services Medicaid waiver program, known as HCS, and the Texas Home Living Medicaid waiver program.

[6] State Auditor's Office Report on Analysis of Quality Assurance Team Projects, Report No. 14-020 (February 2014).

Uniform Statewide Accounting System (USAS). The audit work performed included an examination of ID CARE and TMHP interface controls. Figure 1 below outlines the process flows for the submission and adjudication of claims through the ID CARE and TMHP systems that result in provider payments.

Figure 1: DADS Claims Management System



Source: IG Audit Division

In the Medicaid fee-for-service delivery model, healthcare provider claims for services rendered are paid through an adjudication process. The adjudication process moves through a variety of applications that interface to ensure claims are associated with eligible clients, providers, approved services, approved quantities of service units, and within authorized timeframes.

Claims are entered by providers into secured online portals, which consist of two distinct electronic gateways that allow providers to connect to the DADS Claims Management System, which includes the ID CARE and TMHP systems. The DADS Claims Management System is responsible for the adjudication of claims and the submission of vouchers through HHSAS to USAS for payment. Payment information is sent back to the DADS Claims Management System in a paid warrants file and reconciled to provider claims.

The IG Audit Division work focused on the controls and efficiency over the transfer of claims data entered into the DADS Claims Management System through each step of the adjudication process. The IG Audit Division also examined file movement until submission to USAS for payment. Payment files received from USAS were reconciled back to the claims submitted for payment. Payments were examined to determine the effectiveness of the controls in place to prevent duplicate payments. Additionally, the security over claims data being transmitted across interfaces was tested. The IG Audit Division did not examine the entry of claims by providers or the processing logic for claims adjudication.

The IG Audit Division conducted the audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Unless otherwise described, any year that is referenced is the state fiscal year, which covers the period from September 1 through August 31.

RESULTS, ISSUES, AND RECOMMENDATIONS

The IG Audit Division conducted an audit of IT interfaces between systems used to process Medicaid provider fee-for-service claims within the DADS Claims Management System. The audit focused on whether (a) payment files and related information were completely and accurately transmitted from one system to one or more other systems across interfaces within the DADS Claims Management System and (b) interfaced data in motion and at rest was protected from unauthorized access, modification, and deletion.

Completeness and Accuracy of Transmitted Data

Audit results indicated that claims payment files were transmitted across interfaces completely and accurately, and controls were in place to omit duplicate claims and prevent duplicate payments. Issues that detail (a) inefficiencies in the file transfer process for one interface and (b) risks related to the integrity of data being transferred, follow.

ISSUE 1: AUTOMATED RELEASE OF BATCH FILES FOR PROCESSING WAS NOT ALWAYS ENABLED

Computer systems, which process a large amount of data using routine tasks, benefit from automated processing, as opposed to manual processing. Job schedulers are software applications that run tasks automatically to control and monitor processing. Automated job schedulers can better control batch job processing by functioning in a sequential and logical manner, allowing any deviations in processing to be logged for analysis.

HHSC IT was not using the job scheduler to automatically release batch files for HCBS claims through the DADS Provider Payment System. HHSC IT staff manually released batch files through each phase of processing resulting in the diversion of staff from other job duties. Manual intervention may result in unnecessary delays and errors in processing. Management indicated that past errors in processing led to a lack of confidence in the automation of claims processing. Automation, when properly applied, could reduce cost and increase reliability and timeliness of processing, resulting in increased efficiency.

HHSC IT management implemented automated release of batch job processing through the DADS Provider Payment System before the completion of the audit.

Recommendation 1

HHSC IT should continue to utilize the job scheduler's automated release for processing batch files in order to increase efficiencies and consistency in processing. Additionally, the automation of batch file processing using the job scheduler should enable the logging of any errors for analysis and corrective action.

HHSC Management Response

HHS IT acknowledges the finding as the identified conditions did exist during the audit scope timeframe within Financials Data Warehouse HCS provider payment system. HHS IT accepts this recommendation with the following clarification: HHSC IT had the HCS jobs set up on the Tivoli scheduler and manually released the jobs which allowed the scheduler to automatically complete the job.

Work has since been completed to resolve the issues identified in this recommendation.

Action Plan

HHSC IT Applications updated the job scheduler to automatically release the scheduled jobs and to enable logging of errors for analysis and corrective action.

Responsible Manager

Director, IT Enterprise Services, HHS IT Applications

Target Implementation Date

October 2016

ISSUE 2: CONTROL WEAKNESSES IN THE DADS LONG-TERM CARE PROVIDER SYSTEM AND IN THE TMHP SYSTEM COULD ALLOW IMPROPER PROVIDER PAYMENTS

The DADS Long-Term Care Provider System is used to manage data associated with contracts between DADS and providers who deliver services to Medicaid clients in DADS programs, including information about whether a contract with a provider is active. When a provider contract is not active because it has been terminated, a field within the DADS Long-Term Care Provider System indicates "terminated," and another field contains the ending service, or contract termination, date.

Data from the DADS Long-Term Care Provider System is shared through a daily IT interface with TMHP. As part of TMHP's claims adjudication process, the data TMHP receives from the DADS Long-Term Care Provider System is utilized to determine whether a provider who submitted a claim has an active contract with DADS. If the provider does not have an active contract with DADS, TMHP will not adjudicate the claim and the claim will not be paid.

The interface between the DADS Long-Term Care Provider System and TMHP worked as intended. Results of audit test work confirmed that the data TMHP received through the IT interface with the DADS Long-Term Care Provider System, for the period tested, was transmitted without error to the DADS Long-Term Care Provider System sent through the

interface. This indicated that the interface was working as intended by completely and accurately transferring all of the data.

Controls in the DADS Long-Term Care Provider System to update and track provider contract status were not effective. Audit tests conducted by the IG Audit Division compared the provider contracts in the TMHP system to the provider contracts in the DADS Long-Term Care Provider System. The results revealed discrepancies between the two systems in the information that determined whether a contract was active or terminated. Results of this test work indicated that eight contracts were listed as active in the TMHP system but listed as terminated in the DADS Long-Term Care Provider System.

The IG Audit Division then examined whether payments were made on terminated contracts for each provider with a contract terminated status in the DADS Long-Term Care Provider System. This additional audit work confirmed that no inappropriate payments were made. The results of this audit work indicated that the control structure designed to ensure only providers with current DADS contracts are paid for Medicaid claims was not working as intended, and could result in inappropriate provider payments. Details of weaknesses within that control structure follow.

- DADS staff can enter contract termination data in the DADS Long-Term Care Provider System for providers whose contracts are still active.
- Records within the DADS Long-Term Care Provider System, which indicate a provider contract has been terminated, may not always prevent an improper payment from taking place.
- If any of these provider contracts, however, had actually filed claims, improper payments could still have been made. Payments could be processed for a provider with a terminated contract because key fields in the DADS Long-Term Care Provider System were left blank, which, after being updated with data that is transferred to TMHP through the daily interface, prevents a payment from being processed when a contract has been terminated, such as the contact termination date and the reason code fields. The records identified during the audit work indicated that the termination date field was blank for one contract and the reason codes for termination were blank in others. Because of the blank fields, TMHP processing continued. If a record in the DADS Long-Term Care Provider System for a terminated contract does not contain all of the required information, such as the termination date or reason code, then TMHP would process a claim, resulting in an improper payment.
- The DADS Long-Term Care Provider System does not require key fields to be completed and saved by the end user when entering a contract termination transaction. Data in key fields, including the ending service (or termination) date, are utilized to trigger termination of the contract at TMHP where payments are initiated. The lack of adequate system validations, edit checks, and required completion of key fields, could allow a provider contract to be terminated in the DADS Long-Term Care Provider System but remain active in TMHP, allowing claims to be improperly paid.

Recommendations 2.1 - 2.3

HHSC Contracted Community Services should protect the integrity of provider contract data by:

2.1 Validating, through a second level review, that each contract for which a transaction in the DADS Long-Term Care Provider System has been entered to indicate a provider contract has been terminated, has actually been terminated.

2.2 Developing detective controls, such as a periodic reconciliation of data between the DADS Long-Term Care Provider System and TMHP, to verify that the status of contracts as terminated or active is consistent in both systems.

2.3 Implementing preventive controls that require the entry of valid information in key data fields when processing a contract termination in the DADS Long-Term Care Provider System.

HHSC Management Response

Of 10,500 contracts reviewed in the audit, 8 were found to have missing data fields in the Long Term Care (LTC) Provider System causing them to appear open in TMHP. Although some data entry fields were missing, system edits already in place to prevent erroneous payments resulted in no erroneous payments on the 8 contracts identified in the audit. Access and Eligibility Services (AES) will work with DADS IT to correct the data in the eight cases identified in the audit.

Action Plan

Effective September 1, 2017, staff will begin using CAPPS to terminate contracts. Information entered in CAPPS will update the System of Contract Operation and Reporting (SCOR) and then the DADS LTC Provider System. AES will communicate the need for the required fields to trigger the contract closure in both the LTC Provider System and TMHP to be included in CAPPS to the project team.

AES will:

2.1 Develop a job reference aid for staff on the Provider Payment System data entry requirements. Detailed timelines include: Correction of contracts identified in the audit - March 31, 2017; Communication with CAPPS Project - March 31, 2017; Resource guide - April 30, 2017.

2.2 Develop a process to review a sample of terminated contracts each month to determine if entries are correctly made. AES and DADS IT explored the possibility of developing an exception report from the LTC Provider System but determined it isn't possible in the short term. Process for monthly sample review - April 30, 2017.

2.3 Work with IT to determine the feasibility of developing a quarterly match with TMHP to ensure the TMHP system remains in sync with the LTC Provider System. Specific timelines include: Feasibility of quarterly match - April 30, 2017; Implementation of quarterly match - June 30, 2017.

Responsible Manager

Director, Community Supports Section, Access and Eligibility Services Department

Target Implementation Dates

September 2017

Security of Data in Motion and at Rest

Audit results indicated that files in motion utilized secure transmission protocols to encrypt and protect data. Files are batched and control totals established before transmission through the interfaces and the control totals are verified at receipt by the next system in the processing stream. Access to job schedulers and batch creation modules was tested for access controls and change management processes. The analysis of change management logs for the job scheduler identified a compromised password in the workflow of one system that could impact the security of data at rest.

ISSUE 3: A DADS PROVIDER PAYMENT SYSTEM MACHINE ACCOUNT NAME AND PASSWORD WERE PUBLISHED IN SYSTEM PROCESSING LOGS

Machine accounts exist in order for computers to access other computers, databases, routines, and tasks for the purpose of running automated processes. Each machine account must be unique. Machine accounts have a username and password just like individual users. Machine accounts should be managed and provisioned the same as other user accounts, and passwords should meet the requirements of HHS policy.

A system log file that was accessible to users who did not have administrator access inappropriately contained a machine account name and the associated password. The machine account had administrator access. Administrator access allows unrestricted privileged access to modify or delete processing logs, programmed logic, and data such as claims and payment information. The compromised password created the possibility of unauthorized access or modification to the provider payment files.

The machine account was compromised due to access and change control weaknesses that allowed a script to be inserted into the DADS Provider Payment System software without review, approval, or notification. The script copied the username and password to a file location accessible to many IT staff that should not have administrator access.

The HHS Enterprise Information Security Standards and Guidelines defines appropriate security controls for all HHS agencies. Specifically, the access controls, configuration management, and system integrity sections define the appropriate levels of protection to be implemented.

The compromised account and password could allow deliberate unauthorized changes to, or accidental modification or deletion of, claims information and payable accounts. No evidence was found to indicate files were modified during the months tested.

Additionally, the exposed password did not meet the HHS rules for complexity and length. The database administrator changed the password immediately after the audit team identified the issue.

Recommendations 3.1 - 3.4

HHSC IT should:

3.1 Implement change management processes to ensure that unauthorized changes do not occur.

3.2 Monitor scripts and production logs on at least a weekly basis and research anomalies to determine whether corrective action is needed.

3.3 Verify user and machine accounts that access the DADS Provider Payment System are appropriate and authorized, and perform account reviews as required by HHS Enterprise Information Security Standards and Guidelines.

3.4 Configure machine account passwords to adhere to the HHS Enterprise Information Security Standards and Guidelines requirements for periodic modification, length, and complexity. If changing passwords creates hardships in automated processes or is unreasonable, exceptions must be approved and documented, evidence of the hardship maintained, and the exception recertified annually.

HHSC Management Response

HHS IT acknowledges the findings, as the identified conditions did exist during the audit scope timeframe. HHS IT accepts the recommendations.

Work is in progress to bring the issues identified into compliance with the current HHS Enterprise Information Security Standards and Guidelines (EISSG).

Action Plan

HHS IT Applications:

3.1 Will implement a change management process to ensure unauthorized changes do not occur.

3.2 Will add monitoring of Home and Community-Based Services (HCS) scripts on a weekly basis; add monitoring of production logs to the Financials Data Warehouse (FDW) Daily Checklist to identify anomalies and determine corrective action as needed.

3.3 FDW Manager will perform a review and verify user account access is appropriate as required by the EISSG. In addition, HHSC IT will direct the Data Center Services provider, Atos, to perform a review and verify machine account access is appropriate.

3.4 Updated the database password configurations on February 10, 2017 bringing them into compliance with the EISSG.

In addition, HHSC IT Data Center Services will coordinate with the DCS service provider, Atos, to update the server password configurations to be in compliance with the EISSG.

Responsible Manager

Director, IT Enterprise Services, IT HHS Applications
Director, IT Sourcing Management Services

Target Implementation Dates

April 2017 for Recommendation 3.1
March 2017 for Recommendation 3.2
March 2017 for Recommendation 3.3
March 2017 for Recommendation 3.4

CONCLUSION

The IG Audit Division completed an audit of DADS Claims Management System IT interfaces. Claims data is processed through a complex system of applications and interfaces. The audit examined the adequacy of IT interface processing controls designed to (a) ensure systems transmit information accurately and completely and (b) protect data from unauthorized access, modification, and deletion. The audit did not include verification of the correctness and accuracy of the adjudication and payment of each individual claim processed.

HHS System IT and TMHP share accountability for ensuring Medicaid provider claims payment requests are processed accurately and completely, and for ensuring data is protected from unauthorized access and modification. The audit did not test the adjudication process to determine whether an individual claim was appropriately accepted or rejected for payment.

Based on the results of its audit, the IG Audit Division concluded that:

- Data files tested by the IG Audit Division, which were processed through DADS Claims Management System's IT interfaces, were completely and accurately transferred and received.
- HHSC IT manually released batched claims files instead of using automation, resulting in staff being diverted from other job duties, which may also result in unnecessary delays and errors in processing.
- The DADS Long-Term Care Provider System did not enforce completion of key data fields for processing terminated contracts.
- Files in motion utilized secure transmission protocols to encrypt and protect data.
- A DADS Provider Payment System machine account was compromised in a processing log due to an access and change control weakness, and credentials written to a file location were accessible to persons without a need to know.

The IG Audit Division offered recommendations to HHSC IT and HHSC Contracted Community Services, which, if implemented, will:

- Improve the efficiency of computer operations at HHSC IT by using the job scheduler's automatic release function.
- Require the entry of valid information in key data fields to protect the integrity of contract data in the DADS Long-Term Care Provider System.
- Identify discrepancies in provider contract status of active or terminated between the DADS Long Term Care Provider System and the TMHP system.
- Ensure claims payments are not permitted for providers with terminated contracts.
- Prevent unauthorized changes to scripts that potentially impact claims processing.

- Identify unauthorized changes to scripts.
- Verify and recertify machine accounts.
- Ensure machine account passwords adhere to HHS requirements.

The IG Audit Division thanks management and staff at DADS, HHSC, and TMHP for their cooperation and assistance during this audit.

Appendix A: Objective, Scope, and Methodology

Objective

The objective of the audit was to evaluate the adequacy of IT interface processing controls designed to (a) ensure systems transmit information accurately and completely and (b) protect data from unauthorized access, modification, and deletion.

Scope

The scope of the audit included Medicaid provider fee-for-service claims processed during March and June 2016. The scope of this audit included:

- Processes and controls over fee-for-service Medicaid provider claims payment data processed and transmitted to and from the DADS Claims Management System.
- Relevant data files from HHSC and TMHP systems.
- HHSC monitoring and oversight of contractor activities relevant to the audit objective.

Methodology

To accomplish audit objectives, the IG Audit Division collected information for this audit through discussions and interviews with responsible parties at DADS, HHSC, and TMHP. The IG Audit Division also requested and reviewed the following information:

- Medicaid provider claims payment process flowcharts
- Security controls documentation
- Program information
- System manuals and user documentation

Claims data testing was performed using Audit Control Language and Microsoft Excel, and included the following:

- Approved claims data
- Claims data in batch processing files
- Batch files transmitted across interfaces
- Claims data in voucher files compared to batch processing files
- Claims reconciliation data
- Fee-for-service claims files contained in managed care organization payment data

The IG Audit Division issued an engagement letter on June 13, 2016, to relevant HHSC and DADS management. The IG Audit Division conducted fieldwork at DADS, HHSC and TMHP facilities in Austin, Texas from June 14, 2016, through September 29, 2016. The

scope of the audit was adjusted during fieldwork because batch files containing provider inputs which initiated the processing of claims submissions were only kept by DADS IT and HHSC IT for the prior six months. The process for maintaining a batch file for a limited amount of time was reasonable and the months selected for testing were adjusted accordingly to March and June 2016.

While on-site, the IG Audit Division interviewed responsible personnel, evaluated controls, and reviewed relevant documents related to provider fee-for-service claims payment requests and vouchers.

The IG Audit Division used the following criteria to evaluate the information provided:

- Global Technology Audit Guide (GTAG), Version 8
- HHS Enterprise Information Security Standards and Guidelines, Version 6
- National Institute of Standards and Technology (NIST) Special Publication 800-053A, Revision 1

The IG Audit Division analyzed information and documentation collected to determine whether IT interfaces transmitted information accurately and completely to and from the DADS Claims Management System, and whether data was protected from unauthorized access, modification, and deletion. Professional judgment was exercised in planning, executing, and reporting the results of this audit.

The IG Audit Division assessed the reliability of data provided for analysis by (a) interviewing agency management and staff knowledgeable about the data, (b) reviewing existing information about the data and related IT systems, (c) reviewing system access, change management, and application controls, and (d) verifying the accuracy and completeness of data transmitted between systems. The IG Audit Division determined the data was sufficiently reliable for the purposes of the audit.

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

Appendix B: Sampling Methodology

Population

The IG Audit Division examined Medicaid provider claims payment activities that occurred during March and June 2016. The IG Audit Division performed testing from the population of Medicaid providers, claims payment requests, and IT claims payment processing activities for the months tested.

Accuracy and Completeness of Claims Data

The IG Audit Division evaluated the accuracy and completeness of claims data processed through ID CARE and the DADS Provider Payment System, and returned from USAS for payment reconciliation.

The IG Audit Division conducted a 100 percent review of claims payment requests for the months tested. The IG Audit Division used data analytics tools to test interfaces and security associated with approximately 2.9 million Medicaid provider claims payments. The claims payment amount of ID CARE and DADS Provider Payment System processed claims was approximately $230 million.

The IG Audit Division tested the completeness and accuracy of 40,368 Medicaid claims payment vouchers processed by TMHP. The claims payment amount of TMHP processed claims was approximately $323 million.

Job Scheduler Access and Change Management

The IG Audit Division evaluated job scheduler access lists to determine whether users had valid business reasons for job scheduler access. The IG Audit Division tested 100 percent of users with access to the job scheduler. The job scheduler testing also included an evaluation of 100 percent of job scheduler changes from January 2015 through June 2016 to determine whether changes made were documented and completed.

Job Processing Control in Case of an Abnormal Event

The IG Audit Division conducted testing to assess the controls in place when a batch job processing abnormal event occurred. The IG Audit Division reviewed 100 percent of documentation of computer processing for abnormal events provided by DADS IT, HHSC IT, and TMHP to determine whether job errors were being recorded, tracked, and resolved.

Data Security Controls Over Data in Motion and at Rest

The IG Audit Division conducted testing to assess whether claims payment data was adequately secured when data was being transmitted across each system. The IG Audit Division evaluated security controls, including access to job schedulers and interface engines, for ID CARE and TMHP. For systems in the claims payment process, data is generally not at

rest because jobs are processed immediately upon completion of the prior job. Data in motion for TMHP was tested by evaluating the transmission protocols, control settings, and access to the servers used to transmit data between systems and modules within the system.

The IG Audit Division tested 100 percent of the population for data security controls over data in motion.

Appendix C: Report Team and Report Distribution

Report Team

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

- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Melissa Larson, CIA, CISA, Audit Manager
- James A. Hicks, CISA, IT Audit Project Manager
- Amy Berhnes, MBA, CIA, IT Audit Project Manager
- Netza Gonzalez, MBA, CISA, CFE, IT Audit Project Manager
- Keven Holst, Quality Assurance Reviewer
- Scott Miller, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Charles Smith, Executive Commissioner
- Cecile Erwin Young, Chief Deputy Executive Commissioner
- Kara Crawford, Chief of Staff
- Heather Griffith Peterson, Chief Operating Officer
- Bowden Hight, Deputy Executive Commissioner for IT and CIO
- Ivan Hovey, Director, HHSC IT Applications
- Karin Hill, HHSC Director of Internal Audit
- David Rodney Cook, DADS Chief Financial Officer
- Ying Chan, Interim DADS IT Director

Texas Medicaid Healthcare Partnership

- Jon Andrews, Chief Executive Officer
- Terry Westropp, Chief Operations Officer
- Brad Jackson, Chief Information Officer
- Allan Budweg, Chief Financial Officer
- Eva Riquelme, Chief Administrative Officer
- John Spann, Director of Internal Audit

Appendix D: IG Mission and Contact Information

Inspector General Mission

The mission of the IG 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 IG's mission and statutory responsibility includes:

- Stuart W. Bowen, Jr. — Inspector General
- Sylvia Hernandez Kauffman — Principal Deputy IG
- Christine Maldonado — Chief of Staff and Deputy IG for Operations
- Olga Rodriguez — Senior Advisor and Director of Policy and Publications
- Roland Luna — Deputy IG for Investigations
- David Griffith — Deputy IG for Audit
- Quinton Arnold — Deputy IG for Inspections
- Debbie Weems — Deputy IG for Medical Services
- Alan Scantlen — Deputy IG for Data and Technology
- Anita D'Souza — Chief Counsel

To Obtain Copies of IG Reports

- IG website: https://oig.hhsc.texas.gov

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 Inspector General

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