TEXAS HEALTH AND HUMAN SERVICES COMMISSION

OFFICE OF INSPECTOR GENERAL

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Community First Health Plans

August 2, 2018
OIG Report No. AUD-18-031

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

WHY THE OIG CONDUCTED THIS AUDIT

Community First 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, Community First processes and pays medical provider claims, which contain protected health information and other confidential information. Community First is required to protect and secure confidential Health and Human Services (HHS) System claims data in accordance with criteria established in the Uniform Managed Care Contract (UMCC).

WHAT THE OIG RECOMMENDS

Medicaid and CHIP Services (MCS) should coordinate with HHSC Information Technology (IT) to review Community First system security plans, address deficiencies, and approve the plans. Formal protocols should be established to ensure timely and effective reviews of both MCO security and risk management plans.

MCS should also require Community First to:

- Update its risk management plan.
- Improve controls over the secondary application.
- Strengthen user account controls.
- Document and maintain baseline configurations.
- Conduct disaster recovery training.
- Improve its incident response plan, and associated training and testing.
- Update IT security policies and procedures consistent with its system security plan.

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

August 2, 2018

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

Community First Health Plans

WHAT THE OIG FOUND

Community First submitted system security plans documenting its systems and applications to MCS as required for both 2016 and 2017. It also submitted system security plans prepared by its pharmacy benefit administrator, Navitus, for both years. HHSC IT Applications reviewed and approved only the Navitus system security plans as if they were Community First's plans. The system security plans submitted by Community First were not reviewed.

The Community First risk management plan included a risk assessment that had not been updated for six years to reflect changes to its IT environment. Community First used a secondary application to access and change claims information, and did not adequately control access to the application or monitor changes made to claims using the secondary application.

Community First also did not (a) adequately manage user access to systems storing confidential HHS System information, (b) have documented server configuration settings that met required security standards, (c) conduct disaster recovery training, or (d) have an effective incident response plan. Finally, Community First's security policy and procedures were inconsistent with the system security plan submitted to HHSC.

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

MCS generally agreed with the audit recommendations, and indicated some action plans have already been implemented and others were in progress. Community First, in a comment letter included in Appendix D of the report, generally agreed with the OIG Audit Division recommendations, but did not agree that (a) a secondary application was used to change claims data or (b) active accounts belonging to terminated employees placed confidential HHS System information at risk of unauthorized access. Auditor comments follow the Community First comment letter.

LESSONS LEARNED

HHSC and MCOs must collaborate to ensure security of confidential HHS System information processed and stored by an MCO is sufficient to meet 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, coupled with the absence of effective oversight by HHSC, creates 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 Community First Health Plans (Community First). Community First 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. Community First processes and pays Medicaid and CHIP managed care provider claims, which contain confidential data, including protected health information. Community First is required to protect and secure confidential HHS System information, such as claims data.

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

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

Objective and Scope

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

The audit scope included the design and operating effectiveness, for 2016 and 2017, of:

- Selected logical security controls implemented to protect access to data in the AMISYS Advance application database, data warehouses, and servers in the production and development environments.
- Physical security over information technology (IT) infrastructure.
- General controls supporting backup and recovery.
- Community First system security plans and associated HHS System processes for reviewing the plans.
- Controls for user account management, information system monitoring, and physical access to the data center.

Background

Community First coordinates health services for members[1] in the Medicaid State of Texas Access Reform (STAR) and CHIP programs, and supports Medicaid and CHIP provider claims processing and provider and member benefits administration. The AMISYS Advance application adjudicates and stores provider claims. A third-party vendor, Change Healthcare, pays adjudicated claims and provides explanations of benefits to Community First providers and members.

Third-party clearinghouses[2] transmit provider claims electronically to Community First. All Community First providers use clearinghouses to create claims in a format compliant with the Health Insurance Portability and Accountability Act (HIPAA). Clearinghouses submit claims via secure transmissions to Community First's file transfer server. The AMISYS Advance application adjudicates all claims. Claims information is stored on an Oracle database and replicated daily to Community First's data warehouse,[3] where it is available for reporting and data analysis.

Community First's workforce accesses the AMISYS Advance application through an internal company network, and are authenticated in Active Directory.[4] 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. Community First receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) through secure file transfers using TexMedCentral.

A diagram of these systems is illustrated in Figure 1.

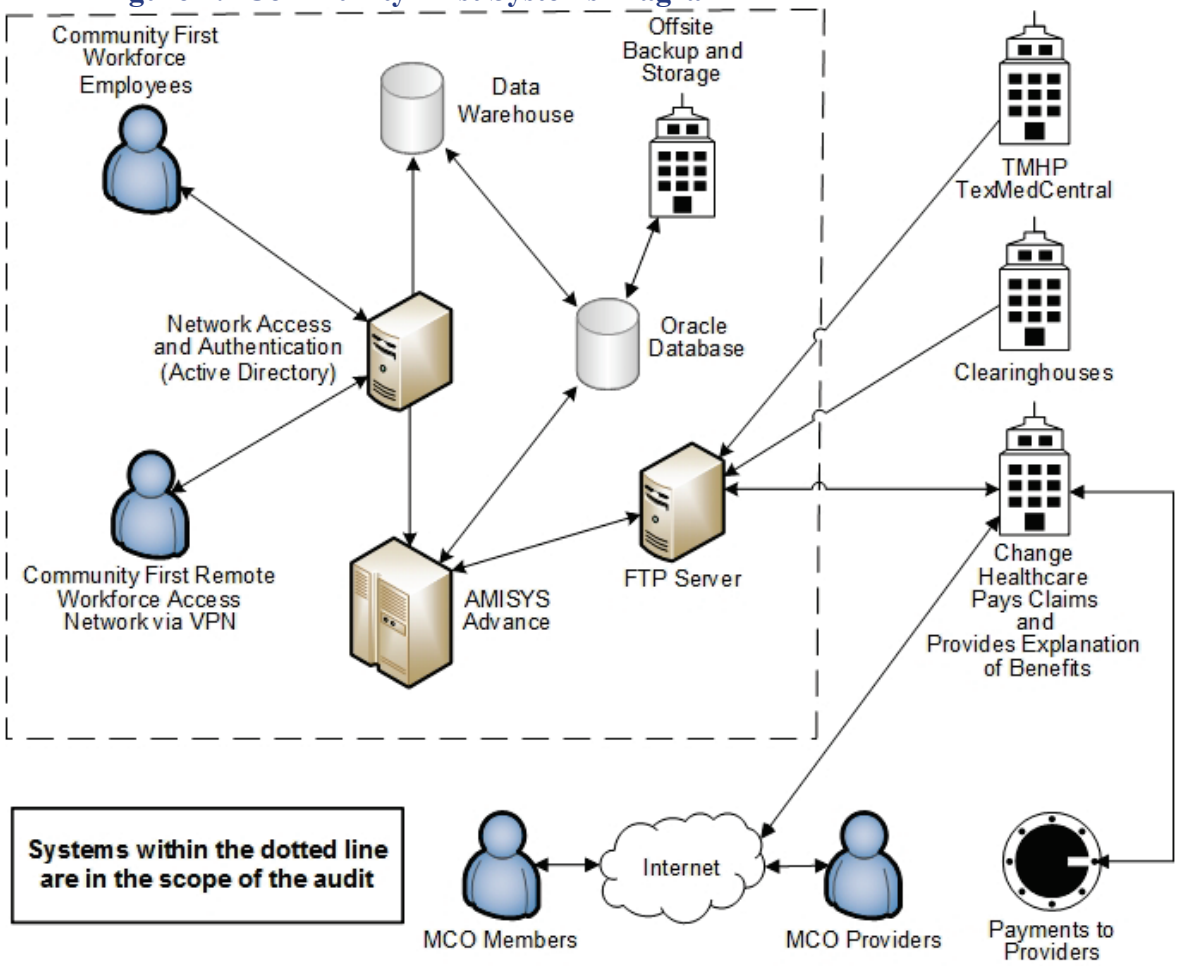
[1] A "member" is an individual who is enrolled with a state contracted Medicaid MCO as a subscriber or dependent.

[2] In medical billing, "clearinghouses" are companies that function as intermediaries that forward healthcare provider claims information to payers.

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

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

Figure 1: Community First Systems Diagram



Source: Prepared by the OIG Audit Division

The audit examined the AMISYS Advance application and the associated infrastructure, operating system, and database that process and store claims detail information.

Community First's data center provides the facility and IT infrastructure for the AMISYS Advance application. The OIG Audit Division performed a physical security review at this location. Community First's data backup and disaster recovery planning activities were also included in the scope of this audit.

Medicaid and CHIP Services (MCS), HHSC IT, and Community First 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.[5] The system security plan should contain 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,[6] including but not limited to:

- Health and Human Services Information Security Standards and Guidelines (ISSG),[7] 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[8]

The system security plan is designed to document current system security controls that protect the confidentiality, integrity, and availability of HHS System data processed, stored, and transmitted by Community First. 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 ISSG guidelines and Community First's security policy and procedures, to develop audit tests to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by Community First.

The OIG Audit Division conducted the audit in accordance with:

- Generally accepted government auditing standards issued by the Comptroller General of the United States
- Standards for Information Systems Audit and Assurance issued by ISACA

Methodology

The OIG Audit Division reviewed relevant security controls protecting confidential HHS System information in the custody of Community First. The key control areas and the associated control groups tested during the audit are identified in

[5] Uniform Managed Care Contract, Attachment A, § 8.1.18.2 MCO Deliverables related to MIS Requirements, v. 2.16 (Sept. 1, 2015) through v. 2.23 (June 1, 2017).

[6] Uniform Managed Care Contract, Attachment A, § 11.08 Information Security, v. 2.16 (Sept. 1, 2015) through v. 2.23 (June 1, 2017).

[7] This document was previously entitled Enterprise Information Security Standards and Guidelines and then Information Security Standards and Guidelines (the term used in this report). In February 2018, the title of the document was changed to Information Security Controls.

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

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 ISSG-defined groupings of security controls. Each control group contains multiple controls which can be layered, based on data risks, to provide customized controls for information security.

Table 1: Key Control Areas and Control Groups

Key Control Areas Selected for Audit	ISSG Control Groups	Issue Number
Information Security Oversight and Risk Management	Planning Risk Assessment	1 & 2
Information Integrity	System and Information Integrity Audit and Accountability	3
User Account Management	Access Identification and Authentication	4 & 5
Configuration Management	Configuration Management	6
Disaster Recovery	Contingency Planning	7
Incident Response	Incident Response	8
IT Security Policies and Procedures	All	9
Vulnerability Assessment and Remediation	Security Assessment and Authorization	N/A
Physical Security	Physical and Environmental Protection	N/A

Source: Prepared by the OIG Audit Division mapping tested control areas to ISSG

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

The OIG Audit Division examined IT security controls and relevant activities supporting data security at Community First. 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 or data was stored. Third-party subcontractors such as Navitus Health Solutions (Navitus), the pharmacy benefit manager for Community First, were not included in the scope of this audit.

The OIG Audit Division presented audit results, issues, and recommendation to MCS and to Community First in a draft report dated June 7, 2018. Each was provided with the opportunity to study and comment on the report. The MCS management response to the audit recommendations contained in the report is included in the report following the recommendations.

MCS concurred with the OIG Audit Division recommendations outlined in this report, and will implement corrective actions plans to be completed by February 2019.

Community First's comments are included in Appendix D. Community First generally agreed with the OIG Audit Division recommendations, but did not agree that (a) claims data was changed utilizing a secondary application or (b) active

accounts belonging to terminated employees placed confidential HHS System information at risk. Auditor comments follow the Community First comment letter.

AUDIT RESULTS

Audit results indicated that Community First had an adequate physical security environment in its primary data center to protect confidential HHS System information, and appropriately controlled backups and coordinated offsite storage at third-party facilities. Additionally, Community First contracted with a third party to perform annual vulnerability assessments as required by ISSG, and actively remediated identified issues.

However, improvements are needed in several control areas to further protect confidential HHS System information from unauthorized access, loss, or disclosure, including:

- Information security oversight
- Risk management
- Information integrity
- User account management
- Configuration management
- Disaster recovery
- Incident response
- IT security policies and procedures

Discussion and recommendations for each of these areas are contained in the issues that follow.

INFORMATION SECURITY OVERSIGHT

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

UMCC requires Community First to submit a system security plan annually.[9] ISSG requires MCS, as the contract manager, to collaborate with the HHSC Information Security Officer within HHSC IT to evaluate whether the system security plan submitted by Community First is complete in accordance with the HHS information system security plan template.[10] TAC requires the HHSC

[9] Uniform Managed Care Contract, Attachment A, § 8.1.18.2 MCO Deliverables related to MIS Requirements, v. 2.16 (Sept. 1, 2015) through v. 2.23 (June 1, 2017).

[10] HHS Information Security Standards and Guidelines Controls Catalog, § 2.3.2 Compliance Monitoring, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Information Security Officer to coordinate the review of data security requirements and specifications and, if applicable, third-party risk assessments of any new computer applications or services that receive, maintain, or share confidential data.[11] The HHS information system security plan template[12] is to be used to document required system security controls for contractors.[13]

Community First must identify and, based on the categorization, document the mission critical applications[14] and the security controls in Community First's system security plan in accordance with ISSG. Community First is required to assign a security categorization to each critical application that stores, processes, or transmits confidential HHS System information. The security categorization would be high, moderate, or low, depending on the information the application stores, processes, or transmits. Based on the security categorization, security controls are designed and implemented per the ISSG control catalog.[15]

Issue 1: HHSC IT Applications Did Not Review Community First's 2016 and 2017 System Security Plans

Community First submitted system security plans documenting its systems and applications to MCS as required for both 2016 and 2017. It also submitted system security plans prepared by its pharmacy benefit administrator, Navitus, for both years. Navitus does not host or support Community First information systems, but does manage pharmacy benefits and claims for Community First members and has custody of and utilizes confidential HHS System information.

Although HHSC IT Applications received the system security plans submitted by Community First, it reviewed and approved only the Navitus system security plans. The Community First system security plans were not reviewed because HHSC IT Applications erroneously determined that Navitus hosted Community First applications and had developed and submitted system security plans on behalf of Community First.

By not reviewing the Community First system security plans, but indicating to MCS that Community First system security plans were approved, HHSC IT Applications created a false assurance that Community First's security control design was adequate to protect confidential HHS System information, and hindered

[11] 1 Tex. Admin. Code, § 202.21 (Mar. 17, 2015, and Mar. 16, 2016).

[12] HHS Information System Security Plan Template, v. 1.3 (July 2015) through v. 1.6 (May 2016).

[13] HHS Information Security Standards and Guidelines Controls Catalog, § 2.3.2 Compliance Monitoring, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[14] A mission critical application is an application that is essential to the mission and survival of a business.

[15] HHS Information Security Standards and Guidelines Controls Catalog, § 2.1 Information System Security Categorization, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

HHSC's ability to hold Community First accountable for any system security plan deficiencies.

Recommendation 1a

MCS should coordinate with HHSC IT to review the current Community First system security plan as soon as practical, address any deficiencies identified during the review, and approve the plan.

Management Response

Action Plan

Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS has coordinated with Texas HHS Information Security and confirmed that the System Security Plan (SSP) currently utilized by Community First Health Plans (and referred to within this audit) is not sufficient to meet requirements established within the Texas HHS Information Security Policy (IS-Policy). The Texas HHS Information Security Office, in conjunction with the Managed Care Compliance and Operations (MCCO) team, have proposed modifications to the managed care contracts to require the appropriate security requirements from MCOs. MCS anticipates those requirements will be included in the managed care contract amendment to be effective September 1, 2018.

After the HHSC managed care contract amendment is executed, it will include specific security requirements for the MCOs as well as an SSP template. Per the Texas HHS Information Security Risk Assessment Monitoring Procedures (IS-RAMP), MCOs will be required to submit a Risk Assessment Report (RAR) annually using the provided RAR template, and if requested, an SSP within 90 days using the SSP template.

HHSC IT Applications will be required to coordinate all RARs in which the MCOs self-assess non-compliance with the Texas HHS Information Security Office and all impacted Texas HHS Information Owners. Only the Information Security Office may initiate a Security Assessment, which requires MCOs to deliver an SSP.

In the interim, HHSC IT Applications will continue to review SSPs submitted in the MCO's format, and will coordinate with the Information Security Office if any security concerns are identified.

Responsible Manager

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

Target Implementation Date

August 2018	*Submission of Community First System Security Plan*
August 2019	*Submission of Community First Risk Assessment Report*

Recommendation 1b

MCS, in coordination with HHSC IT, should establish formal protocols for review and approval of MCO system security plans.

Management Response

Action Plan

Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT to establish policies and procedures for formal protocols for review and approval of MCO system security plans and checklists.

Responsible Manager

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

Target Implementation Date

August 2018

RISK MANAGEMENT

Risk assessment is a structured and systematic process to identify potential security weaknesses and analyze the impact to the confidentiality, integrity, and availability of information in the event a weakness were to be exploited. Effective risk management requires that Community First:

- Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits.
- Document risk assessment results in a risk assessment report.
- Review risk assessment results annually or biennially depending on the risk designation of the system.

- Disseminate risk assessment results to applicable personnel.

- Update its risk assessment annually, biennially, or whenever there are significant changes to information systems or the operating environment (including the identification of new threats and vulnerabilities), or other conditions that may impact the security of the system.[16]

The risk assessment drives the approach to risk mitigation strategies intended to reduce risk to an acceptable level. For risks identified, management may choose to implement controls to mitigate or reduce risk, take no action and accept the risk, or outsource the risk to another organization.

UMCC requires Community First to submit, for HHSC's review and approval, a risk management plan.[17] Additionally, HHSC utilizes a risk management plan checklist to evaluate the risk management plan.[18] A key component of the risk management plan is the information systems risk assessment to categorize applications and the information they contain. The categorization assigned to each application defines the security baselines and the appropriate controls to apply for security. ISSG requires that Community First review and update the risk assessment to address information system or operating environment changes.[19] MCS is responsible for contractual oversight, and HHSC IT is responsible for the review and approval of the risk management plan, including changes to the plan based on an updated risk assessment.

Issue 2: Community First Did Not Update Its Risk Assessment in Accordance With ISSG

Community First submitted a risk management plan to HHSC that contained an outdated risk assessment. The risk management plan was received and approved by HHSC IT Applications even though the risk assessment was not current. The risk assessment had not been updated in six years and did not accurately reflect the current risk environment related to its systems' storing and transmitting of confidential HHS System information.

Community First developed a comprehensive risk management plan in 2011, but submitted the same, unchanged risk management plan on an annual basis to HHSC

[16] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 Risk Assessment, RA-3, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[17] Uniform Managed Care Contract, Attachment A, § 8.1.18.2 MCO Deliverables related to MIS Requirements, v. 2.16 (Sept. 1, 2015) through v. 2.23 (June 1, 2017).

[18] HHSC Uniform Managed Care Manual, Chapter 5: Consolidated Deliverables Matrix, v. 2.3 (Jan. 5, 2015) through v. 2.5 (Mar. 1, 2017).

[19] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 Risk Assessment, RA-3, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

IT Applications, which approved the risk management plan, including the outdated risk assessment. Changes made to the Community First information system environment since 2011 included the addition of Navitus as the subcontracted pharmacy benefit manager and the updating of file layouts for interfaces with the enrollment broker.

These changes were not reflected in the most recent risk management plan submitted to HHSC. Although Community First had a documented risk management process, management failed to follow the process or the ISSG, which both require the risk assessment contained in the risk management plan to be updated to reflect the current information systems environment.

Without a risk management plan that reflects the current information systems environment, Community First management may not be aware of potential risks and, as a result, could fail to implement appropriate mitigation strategies to protect the confidentiality and integrity of confidential HHS System information.

Recommendation 2a

MCS, through its contract oversight responsibilities, should require Community First to improve processes for ensuring its risk management plan reflects the current information system operating environment.

MCS should consider tailored contractual remedies to compel Community First to submit updated risk management plans to HHSC, and maintain a current risk assessment.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. Following the September 2018 managed care contract amendment, the Risk Management Plan (RMP) requirement should be satisfied by the MCOs submission of a Risk Assessment Report (RAR) using the provided template as documented in Issue 1, Recommendation 1a. The RAR will document current risks due to non-compliance and include the MCOs' plans to manage/remediate such risks.

In the interim, HHSC IT Applications will require an updated RMP from Community First using their current format that will identify risks and include MCO remediation strategies.

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

Target Implementation Date
December 2018 *Submission of Interim Risk Management Plan*
August 2019 *Submission of Community First's Risk Assessment Report*

Recommendation 2b

MCS, in coordination with HHSC IT, should establish formal protocols for review and approval of MCO risk management plans.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in establishing policy and procedures for formal protocols for review and approval of MCO risk management plans including the system security plans and checklists.

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

Target Implementation Date
August 2018

INFORMATION INTEGRITY

Information integrity refers to the accuracy and reliability of information stored in a file, database, or data warehouse. As a process, information integrity verifies that information has remained unaltered in transit from the source system to the destination system. As a security function, information integrity services check information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.[20] Information integrity also requires that the actions of individual information system users can be uniquely traced to users so the users can be held accountable for their actions.[21]

Information undergoes any number of operational changes or processing to support decision-making, such as input capture, storage, retrieval, update, and transfer. To maintain integrity necessary to enable and support business decisions, information must be kept free from corruption, modification, or unauthorized disclosure. Inaccuracies can occur accidentally through programming errors, maliciously, or

[20] HHS Information Security Standards and Guidelines Controls Catalog, § 7.18 System and Information Integrity, SI-10, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[21] HHS Information Security Standards and Guidelines Controls Catalog, § 7.3 Audit and Accountability, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

through breaches or hacks. Secure environments may utilize a number of control practices to assure information integrity, including:

- Encryption, which locks the information and makes it unreadable without a cipher key.
- Backup, which stores a copy of information in an alternate location for retrieval if original data is lost or destroyed.
- Access controls, including assignment of read and write privileges.
- Input validation, to prevent incorrect data entry.
- Information validation, to certify uncorrupted transmission.

Community First is contractually responsible for the design, implementation, and effectiveness of security controls over confidential HHS System information in its custody, or in the custody of any subcontractors or business partners with which it shares confidential HHS System information.

Issue 3: Community First Used a Secondary Application to Change Claims Information

Community First management was aware of and allowed users to change groups of Medicaid and CHIP claims data through the use of a secondary[22] application. The secondary application was used outside of the AMISYS Advance claims adjudication process.

Community First indicated that staff used the secondary application to assist in the processing of claims because AMISYS Advance was antiquated and unable to support the processing of certain claims, and changed certain information, including National Provider Identification numbers and Patient Control Numbers, available within AMISYS Advance.

While this approach may have enabled Community First to process claims AMISYS Advance was otherwise unable to process, changing claims information using a secondary application circumvented data integrity controls in AMISYS Advance. User account management processes were not adequate to control user access to the secondary application or to track users' actions to change claims using the secondary application. Community First did not ensure changes were reviewed and approved by a responsible level of management before changed data was

[22] "Secondary" applications have the capability to communicate with a resource or database outside of the usual process, bypassing user access, application processing, and audit logging controls.

processed. The use of the secondary application impacts data reliability and could result in:

- Claims that are not representative of services provided
- Claims inconsistent with encounter data submitted to HHSC
- Payments to incorrect providers or providers not enrolled in Medicaid

The OIG Audit Division is conducting additional work outside of this audit to identify users of the secondary application, the extent of any changes to claims data, and the impact of those changes.

Community First indicated that the AMISYS Advance application will be replaced in 2018. Until Community First ceases its use of the secondary application, the risks to the integrity of claims information will remain.

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

Recommendation 3a

MCS, through its contract oversight responsibilities, should require Community First to strengthen controls to ensure that (a) information processed in the AMISYS Advance application is accurate and reliable and (b) user activity in the secondary application is monitored to facilitate user accountability.

See separate document, "Confidential Issues: Security Controls Over Confidential HHS System Information at Community First Health Plans."

Management Response

Action Plan

Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First to strengthen controls to ensure that (a) information processed in the AMISYS Advance application is accurate and reliable and (b) user activity in the secondary application is monitored to facilitate user accountability.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system

security plans and checklists prepared by the MCOs. MCS will require Community First to submit monthly updates detailing the status of each milestone.

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

Target Implementation Date
February 2019

Recommendation 3b

MCS, through its contract oversight responsibilities, should require Community First to monitor use of the secondary application to ensure that modifications to claims data are justified and adequately tracked.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First monitors use of the secondary application to ensure that modifications to claims data are justified and adequately tracked.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

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

One key control for managing system access is the principle of least privilege. Least privilege access is the practice of allowing only the access for users that is necessary to accomplish assigned tasks in accordance with business functions.[23] To accomplish least privilege access control practices, roles are created for various job functions, and the permissions to perform certain operations are assigned to specific roles. System users are assigned particular roles, and through those role assignments acquire the permissions to perform functions within the system. Permissions are not assigned to users directly, but rather are granted to certain role assignments.

ISSG requires account access levels to be reviewed, at a minimum, every 12 months for appropriateness.[24] ISSG also requires that information systems automatically disable inactive privileged accounts after 60 days and non-privileged accounts after 90 days.[25]

Audit results indicated that Community First maintained adequate control over generic privileged accounts.

Issue 4: Community First Failed to Disable User Accounts of Terminated Employees

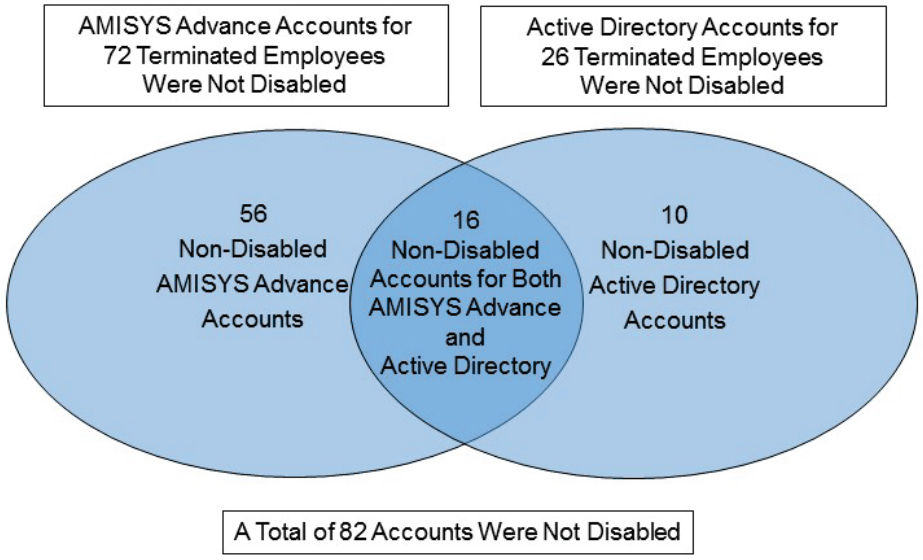
Community First did not immediately disable user accounts for terminated employees in Active Directory and in the AMISYS Advance application. Specifically, 16 accounts belonging to terminated employees were not disabled and retained access to both Active Directory and AMISYS Advance. In addition, 66 accounts belonging to terminated employees or contractors were not disabled and retained access to either Active Directory (10 accounts) or AMISYS Advance (56 accounts).

[23] HHS Information Security Standards and Guidelines Controls Catalog, § 7.1 Access Control, AC-6, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[24] HHS Information Security Standards and Guidelines Controls Catalog, § 7.1 Access Control, AC-2, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[25] HHS Information Security Standards and Guidelines Controls Catalog, § 7.1 Access Control, AC-2(3), v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Figure 2: Active Directory and AMISYS Advance Access Diagram



Source: OIG Audit Division

ISSG requires that management disable information system access immediately upon termination of employment and revoke any authenticators or credentials associated with the terminated individual.[26] Community First indicated it relies on manual notifications from management of employment terminations and, when notified, changes the account password for terminated employees. It acknowledged that it does not always receive timely notification of terminated employees, and sometimes is not notified at all. Until disabled, Active Directory accounts belonging to terminated employees could be used to gain unauthorized access to the Community First network and other resources accessible on the network, including AMISYS Advance.

Of the 26 non-disabled Active Directory accounts that remained assigned to terminated employees, 20 accounts had still not been disabled more than 60 days after the employees' terminations and, of those, 3 accounts had still not been disabled more than 12 months after termination.

Of the 72 non-disabled AMISYS Advance accounts that remained assigned to terminated employees, 62 accounts had not been disabled more than 60 days after the employees' terminations and, of those, 12 accounts had still not been disabled more than 12 months after termination.

Community First did not have a process in place to automatically disable Active Directory accounts after an employee was terminated, but for AMISYS Advance,

[26] HHS Information Security Standards and Guidelines Controls Catalog, § 7.14 Personnel Security, PS-4, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Community First indicated a secondary control was configured to disable accounts that had been inactive for 60 days. This control did not actually disable an account after 60 days. Instead, the configuration set the account password to be disabled upon the first attempted login that occurred more than 60 days after the previous logon. This configuration, however, did not address accounts belonging to terminated employees that were accessed inappropriately within 60 days of the last logon since, in that situation, the account would not have been inactive for over 60 days.

Community First's account management practices did not meet ISSG requirements and placed confidential HHS System information at risk of unauthorized viewing, modification, or deletion.

Recommendation 4

MCS, through its contract oversight responsibilities, should require Community First to develop and strengthen control activities for user account management, to ensure that accounts are disabled upon termination of employment and privileges for active accounts are appropriate, in accordance with ISSG requirements.

MCS should consider tailored contractual remedies to compel Community First to effectively perform required account management activities.

Management Response

Action Plan

Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First to develop and strengthen control activities for user account management to ensure that accounts are disabled upon termination of employment and privileges for active accounts are appropriate, in accordance with ISSG requirements.

MCS will consider tailored contractual remedies to compel Community First to effectively perform account management activities.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

Issue 5: Community First Did Not Review and Recertify Permissions Granted to AMISYS Advance Users

Community First did not perform periodic reviews and recertification of AMISYS Advance accounts and associated permissions to ensure access of individual account holders was appropriate and justified.

Community First conducted a quarterly review of selected AMISYS Advance security group settings, but did not review (a) individuals with access to AMISYS Advance to ensure access was warranted or (b) users assigned to each security role to ensure privileges granted to individual users was appropriate. Additionally, account permissions for individual employees were frequently modified outside of the application with a manual request and approval process. Community First management asserted that frequent modifications to individual account permissions were necessary due to AMISYS Advance limitations.

The 12 active AMISYS accounts belonging to employees terminated for more than one year, detailed in Issue 4 above, may have been detected and disabled had Community First conducted required annual reviews and recertification of accounts and permissions. In addition, some of the additional 62 accounts belonging to employees terminated for more than 60 days may have also been detected in an annual review.

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

Recommendation 5

MCS, through its contract oversight responsibilities, should require Community First to strengthen practices for performing and documenting the annual review of (a) individuals with access to AMISYS Advance and the permissions granted to each individual and (b) roles with access to AMISYS Advance and the users assigned roles granting access to confidential HHS System information.

MCS should consider tailored contractual remedies to compel Community First to effectively control access to confidential HHS System information.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First to conduct a documented review and recertification, at least annually, of (a) individuals with access to AMISYS Advance and the permissions granted to each individual and (b) roles with access to AMISYS Advance and the users assigned roles granting access to confidential HHS System information.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

CONFIGURATION MANAGEMENT

ISSG specifies that documentation and maintenance of current baseline configuration settings for network components are key controls in securing systems.[27] Baseline security configurations should be made in accordance with documented standards about information system components' settings and parameters to protect data. Configuration standards include password settings, software installation parameters, including patch management, and server settings for ports, protocols, services, and remote connections.

The OIG Audit Division observed and tested Community First's configuration settings for the Active Directory server, the data warehouse server, and the secure file transfer server used by third-parties to send or receive Community First claims information. The OIG Audit Division also tested a sample of the patches applied to the file transfer server, the data warehouse server, and the Active Directory server

[27] HHS Information Security Standards and Guidelines Controls Catalog, § 7.5 Configuration Management, CM-2, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

in order to verify that security patches were installed in accordance with documented security patch management practices at Community First. No issues were identified with the examined configuration settings for these servers or with documented patch management practices.

Community First did not document baseline server configurations as required by ISSG.

Issue 6: Community First Did Not Document Baseline Configurations

Community First did not have documented baseline configuration settings for servers. While Community First provided a high-level policy document to the OIG Audit Division, the document did not contain detailed configuration settings that, when applied, would adequately protect confidential HHS System information. Detailed configuration settings help ensure that servers that process or store confidential HHS System information meet required configuration standards, and that any deviations are documented and approved.[28]

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.

Community First indicated it was not aware of the ISSG requirement to have documented baseline configurations in place, and did not maintain documentation of server baselines. Because it does not maintain baseline configurations, Community First 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 event or incident.

Recommendation 6

MCS, through its contract oversight responsibilities, should require Community First to improve control activities for documenting baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

[28] HHS Information Security Standards and Guidelines Controls Catalog, § 7.5 Configuration Management, CM-6, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

MCS should consider tailored contractual remedies to compel Community First to adequately document the configuration of servers.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First to improve control activities for documenting baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

DISASTER RECOVERY

Disaster recovery planning ensures the availability of critical information resources in emergency situations.[29] Well-designed disaster recovery plans for information systems must identify essential functions, provide recovery objectives and restoration priorities, and identify contingency roles, responsibilities, and assigned individuals with contact information.[30] The goals associated with the recovery of information systems include restoration of the security safeguards as originally planned and implemented.

[29] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[30] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, CP-2, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

ISSG requires Community First to have a disaster recovery plan containing specified elements,[31] and to develop contingency planning policies and procedures for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information systems and continuity of operations in emergency situations.[32] In addition, Community First is required to annually (a) provide disaster recovery training[33] to certain users as defined in its disaster recovery plan and (b) test its disaster recovery plan using NIST guidelines.[34]

Audit results indicated that Community First had a disaster recovery plan that included required elements, and that the plan was tested annually by a third-party cloud vendor. However, opportunities for improvement exist at Community First related to disaster recovery training.

Issue 7: Community First Did Not Conduct Disaster Recovery Training

Community First's IT personnel with assigned disaster recovery plan roles and responsibilities did not receive annual disaster recovery training. Community First was not aware of the ISSG control standard for training and had not provided the information system users with disaster recovery training consistent with their assigned roles and responsibilities.

In the event of an actual disaster that required the activation of the Community First disaster recovery plan, the lack of training could result in inadequate and delayed restoration of computer systems.

Recommendation 7

MCS, through its contract oversight responsibilities, should require Community First to perform disaster recovery planning activities to include conducting annual training of IT personnel tasked with disaster recovery activities.

MCS should consider tailored contractual remedies to compel Community First to provide annual disaster recovery training to appropriate staff.

---

[31] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, CP-2, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[32] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, CP-1, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[33] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, CP-3, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[34] HHS Information Security Standards and Guidelines Controls Catalog, § 7.6 Contingency Planning, CP-4, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First to perform disaster recovery planning activities to include conducting annual training of IT personnel tasked with disaster recovery activities.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

INCIDENT RESPONSE

Incident response is a key component of security monitoring, as an increasing number of information security threats can disrupt business activities and expose data to unauthorized access, loss, or disclosure. While a sound security monitoring program and supporting tools can minimize the risk and impact of incidents, there are some incidents that cannot be anticipated or avoided. Consequently, incident response capabilities are necessary components of an effective security program and are required by ISSG.[35] An effective incident response capability provides for prompt response to security events and incidents, mitigates impact, and helps ensure operations are restored in a safe, secure, and timely manner.

ISSG requires Community First to have an incident response plan[36] that includes a roadmap for tracking, documenting, and reporting incidents to appropriate HHS System personnel, and to develop incident response planning policies and

[35] HHS Information Security Standards and Guidelines Controls Catalog, § 7.8 Incident Response, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[36] HHS Information Security Standards and Guidelines Controls Catalog, § 7.8 Incident Response, IR-8, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

procedures[37] for adequate preparation, detection, analysis, containment, recovery, and user response activities. In addition, Community First is required to annually (a) provide incident response training[38] to certain users as defined in its incident response policy and (b) test its incident response capability.[39]

Audit results indicated that Community First had incident response policies and procedures, but did not have an incident response plan. Because it did not have an incident response plan, Community First did not provide incident response plan training to its staff, or test an incident response plan.

Issue 8: Community First Did Not Have an Incident Response Plan

Community First utilized a variety of software and devices to prevent and detect security events over its network, and had a breach response process, which included notifying IT security personnel of network events. However, Community First did not have a detailed and tested incident response plan, and did not train its workforce on how to properly respond to security events.

Security incidents may involve exploited vulnerabilities, such as allowing a computer virus to infect the network. An effective incident response plan defines reportable incidents and describes the structure, organization, and resources of the incident response capability.

Until Community First develops an incident response plan, HHSC does not have assurance that security incidents will be identified and appropriately handled. In addition, Community First's staff cannot be trained in incident response until a plan is developed.

Recommendation 8

MCS, through its contract oversight responsibilities, should require Community First to improve control activities for incident response, to include:

- Developing and documenting an incident response plan that is aligned with ISSG requirements.

[37] HHS Information Security Standards and Guidelines Controls Catalog, § 7.8 Incident Response, IR-1, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[38] HHS Information Security Standards and Guidelines Controls Catalog, § 7.8 Incident Response, IR-2, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[39] HHS Information Security Standards and Guidelines Controls Catalog, § 7.8 Incident Response, IR-3, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

- Conducting annual training of IT security personnel tasked with incident response activities.

- Conducting annual incident response tests and simulations.

MCS should consider tailored contractual remedies to compel Community First to (a) develop and maintain an incident response plan, (b) provide annual training to its workforce, and (c) test its incident response capability at least annually.

Management Response

Action Plan
Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring Community First improve control activities for incident response, to include (a) developing and documenting an incident response plan that is aligned with ISSG requirements; (b) conducting annual training of IT security personnel tasked with incident response activities; and (c) conducting annual incident response tests and simulations.

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

IT Security Policies and Procedures

IT security policies consists of high-level strategic statements relating to the protection of confidentiality, integrity, and availability of information resources across the organization. Procedures consist of documented operational instructions that may prescribe a process or contain a series of steps for assisting the workforce with implementing security requirements. They are a direct link between an organization's vision and mission statement to daily operations.

Together, policies and procedures provide a roadmap for day-to-day operations. They ensure compliance with laws and regulations, give guidance for decision-making, and streamline internal processes. Policies and procedures provide consistent and structured processes that are essential in a well-run organization.

In the ISSG control catalog, 17 of the 18 control groups include as the first control activity implementation policy and procedures for meeting the control objective.

Issue 9: Community First's Information Security Policies and Procedures Were Inconsistent With Its System Security Plan

Community First's information security policies and procedures did not exist as stated in Community First's system security plan. ISSG requires the organization to develop, document, and disseminate security policies and procedures to applicable personnel, and update the policies and procedures when significant changes occur in the environment.[40]

Without fully developed policies and procedures, Community First personnel may not be aware of their responsibilities to protect confidential HHS System information or be prepared to effectivity execute job responsibilities associated with information system security.

Recommendation 9

MCS, through its contract oversight responsibilities, should require Community First to document information system security policies and procedures consistent with the stated practices within the system security plan.

MCS should consider tailored contractual remedies to compel Community First to develop and implement policies and procedures that are consistent with those the system security plan indicates are in place.

Management Response

Action Plan

Medicaid and CHIP Services (MCS) agrees with the recommendation. MCS, through its contract oversight responsibility, will coordinate with HHSC IT in requiring require Community First to document information system security policies and procedures consistent with the stated practices within the system security plan.

[40] HHS Information Security Standards and Guidelines Controls Catalog, §§ 7.1 through 7.18, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

MCS expects Community First to take immediate corrective action under the CAP and will allow 180 calendar days to implement all actions within the CAP. MCS will require Community First to submit monthly updates detailing the status of each milestone.

Prior to approving actions within the CAP, MCS will coordinate with HHSC IT to perform a joint review of the CAP since it currently reviews the submitted system security plans and checklists prepared by the MCOs.

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

Target Implementation Date
February 2019

CONCLUSION

The OIG Audit Division completed an audit of selected security controls over confidential HHS System information in the custody of Community First. The audit included an evaluation of IT security controls over the AMISYS Advance application and its operating environment. The OIG Audit Division conducted a site visit at Community First in July 2017.

The OIG Audit Division concluded:

- Community First had an adequate physical security environment in its primary data center to protect confidential HHS System information.
- Community First had appropriate controls over its system backup and offsite storage.
- In 2016 and 2017, HHSC IT Applications reviewed and approved system security plans for Navitus, but did not review Community First's system security plans.
- Community First had not updated its risk management plan in six years, and the information in the plan no longer reflected the current IT risk environment.
- Community First allowed groups of claims to be changed utilizing a secondary application.
- Community First did not effectively manage user access to information systems that contained confidential HHS System information.
- Community First did not document baseline configuration settings for its servers.
- Community First had a disaster recovery plan that was tested annually.
- Community First did not conduct disaster recovery training.
- Community First did not have an effective and tested incident response plan, and staff were not trained on incident response.
- Community First's information security policies and procedures were inconsistent with its system security plan.

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

- Reviewed and approved system security and risk management plans that meet ISSG requirements.
- Increased information integrity and tracking of changes made to claims before and after adjudication.
- 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.
- Personnel with disaster recovery training.
- An effective and tested incident response plan, and workforce trained to respond to security incidents.
- Policies and procedures aligned with its system security plan.

The OIG Audit Division thanks the management and staff of MCS, HHSC IT Applications, HHSC Information Systems Security, and Community First for their cooperation and assistance during this audit.

Appendix A: Objective, Scope, and Methodology

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 Community First.

Scope

The audit scope included the design and operating effectiveness of:

- Selected logical security controls implemented to protect access to data in the AMISYS Advance application database, data warehouses, and servers in the production and development environments.
- Physical security over IT infrastructure.
- General controls supporting backup and recovery activities for the period September 2015 through August 2017.
- System security plans and associated HHS system security plan review processes for 2016 and 2017.
- Controls for user account management, information system monitoring, and physical access to the data center in effect from September 2015 through August 2017.

Methodology

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

- Network penetration reports
- Service organization controls reports
- Community First system security plans and associated IT contract deliverables
- Community First IT security policies and procedures

The OIG Audit Division issued an engagement letter to Community First on July 7, 2017, providing information about the upcoming audit, and conducted fieldwork at Community First's facility in San Antonio, Texas, on July 12 and 13, 2017. While on site, the OIG Audit Division interviewed

responsible personnel, observed and tested configuration settings, and reviewed documentation relevant to support the control environment.

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, Attachment A, v. 2.16 (2015) through v. 2.23 (2017)
- Uniform Managed Care Manual, Chapter 5: Deliverables, Report Formats, Due Dates, §§ 5.0, Consolidated Deliverables Matrix, v. 2.3 (2015) through v. 2.4 (2016) and 5.2, MIS Deliverables/Formats, v. 2.0 (2015)
- HHS Information Security Standards Guidelines Controls Catalog, v. 5.1 (2013) through v. 6 (2015)
- HHS Information System Security Plan Template, v. 1.3 (2015) through v. 1.6 (2016)

Auditing Standards

GAGAS

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

ISACA

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

Appendix B: Testing Methodology

The OIG Audit Division examined Community First IT security controls that were in effect during the period from September 2015 to August 2017. After performing a risk and controls assessment of Community First's documented IT security control structure, the OIG Audit Division performed testing of selected security controls over the AMISYS Advance production and development environment and supporting infrastructure.

Information Security Oversight and Risk Management

The OIG Audit Division examined processes over HHSC's review and approval of annual Community First system security plans to determine whether the plans were complete, accurate, and approved. Additionally, the OIG Audit Division reviewed the risk management plan and associated risk assessment for Community First to verify the information system environment.

Information Integrity

The OIG Audit Division reviewed the security tables and user access to the secondary application used to update claims processed and stored by the AMISYS Advance application. Additionally, the OIG Audit Division examined claims and subsequent encounter data submitted by Community First to determine the types of changes made by the secondary application.

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. The OIG Audit Division tested all user accounts for AMISYS Advance and the Community First network environment.

Configuration Management

The OIG Audit Division interviewed Community First IT staff and examined applicable IT policies and system configurations.

Disaster Recovery

The OIG Audit Division reviewed Community First's disaster recovery plan and interviewed responsible personnel to determine the effectiveness of the disaster recovery plan and the organizational readiness to execute the plan.

Incident Response

The OIG Audit Division interviewed Community First 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 Community First network.

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

IT Security Policies and Procedures

The OIG Audit Division reviewed the system security plans and Community First's associated policy and procedures to determine if the policies were updated to reflect the current process and implemented as stated in the system security plans.

Vulnerability Assessment and Remediation

The OIG Audit Division reviewed the results of the most recent vulnerability assessments and penetration tests conducted on behalf of Community First by a third-party vendor and examined Community First's remediation plans associated with those assessments and tests to determine whether the activities detailed in the plans appeared designed to address identified risks.

Physical Security

The OIG Audit Division performed a physical security inspection of the Community First data center and evaluated badge access logs to 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	CE	5 & 9
AC-2	Account Management		
AC-5	Separation of Duties		
AC-6	Least Privilege		
AC-6(1)	(1) Authorize Access to Security Functions	CD	5
AC-6(5)	(5) Privileged Accounts		
AC-17	Remote Access		
Audit and Accountability (AU) Controls			
AU-2	Audit Events	CD	4
Security Assessment and Authorization (CA) Controls			
CA-1	Security Assessment and Authorization Policy and Procedures	CE	9
CA-2	Security Assessments	CE	
CA-6	Security Authorization	CE	
CA-8	Penetration Testing		
Configuration Management (CM) Controls			
CM-1	Configuration Management Policy and Procedures	CE	6 & 9
CM-2	Baseline Configuration	CD	6
CM-6	Configuration Settings		6
Contingency Planning (CP) Controls			
CP-1	Contingency Planning Policy and Procedures	CD	7 & 9
CP-3	Contingency Training	CD	7
CP-4	Contingency Plan Testing		
CP-6	Alternate Storage Site		
CP-7	Alternate Processing Site		
Identification and Authentication (IA) Controls			
IA-1	Identification and Authentication Policy and Procedures	CE	9
IA-2	Identification and Authentication [Organization Users]		
IA-3	Device Identification and Authentication		
IA-8	Identification and Authentication [Non-organizational Users]		
Incident Response (IR) Controls			
IR-1	Incident Response Policy and Procedures	CD	8
IR-3	Incident Response Testing	CD	8
IR-8	Incident Response Plan	CD	8

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
Physical and Environmental Protection (PE) Controls			
PE-3	Physical Access Control		
PE-6	Monitoring Physical Access		
PE-8	Visitor Access Records		
Planning (PL) Controls			
PL-1	Security Planning Policy and Procedures	CE	1 & 9
PL-2	System Security Plan		
PL-8	Information Security Architecture		
Risk Assessment (RA) Controls			
RA-1	Risk Assessment Policy and Procedures	CE	2 & 9
RA-2	Security Categorization		
RA-3	Risk Assessment	CD	2
RA-5	Vulnerability Scanning		
System and Information Integrity (SI) Controls			
SI-1	System and Information Integrity Policy and Procedures	CE	3 & 9
SI-10	Information Input Validation	CD	3
SI-11	Error Handling	CD	3

Source: Prepared by the OIG Audit Division based on controls tested

Appendix D: Community First Management Comment

June 22, 2018

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

Re: *Audit of Security Controls over HHS System Confidential Information 2017*

Dear Mr. Sizemore:

Community (CFHP) is sending this letter in response to the audit results that were made available in the Draft Report entitled, *Audit of Security Controls over HHS System Confidential Information* and in the subsequent discussions with HHSC IG. CFHP appreciates the opportunity to provide comments on the findings that were identified regarding CFHP effectiveness of IT security controls for systems that process and/or store confidential information. Please see the attached comments from CFHP.

For any questions or concerns, please call at (210) 510-2482.

Respectfully,

Laura Ketterman JD, CHC, CPHC
Director, Compliance & Regulatory Affairs

CC: Greg Gieseman, CEO/President
Terry Fehlhaber, Director IS

Keeping our commitment to you

(210) 227-2347 ● Toll-Free 1-800-434-2347● Fax (210) 358-6014 ● 12238 Silicon Drive, Suite 100 ● San Antonio, Texas 78249 ● www.cfhp.com

Lessons Learned Section

Finding: Weaknesses in the design or implementation of IT security controls for MCO systems that contain confidential HHS System information, coupled with the absence of effective oversight by HHSC, creates 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

CFHP comment: CFHP would like clarification added that CFHP safeguards were not *sufficien*t according to Enterprise Information Security Standards and Guidelines (EISSG) standards.

Issue #3

Finding: Community First Utilized a Secondary Application to Update and Change Claims Information

CFHP comment: CFHP claim examiners are trained to go to the electronic/EDI copy to check and correct claims only when the clearinghouse employed to convert paper claims to electronic format does not populate correctly. There are no secondary application commands that would facilitate this change.

Issue #4

Finding: Community First Failed to Disable User Accounts of Terminated Employees

CFHP comment: CFHP agrees that CFHP failed to successfully disable user accounts of terminated employees. However, CFHP does have controls in place that prevent terminated employees from gaining unauthorized access into AMISYS Advance.

Keeping our commitment to you

(210) 227-2347 ● Toll-Free 1-800-434-2347● Fax (210) 358-6014 ● 12238 Silicon Drive, Suite 100 ● San Antonio, Texas 78249 ● www.cfhp.com

Auditor Comments

The OIG Audit Division respects the Community First position related to the Lessons Learned section of the Executive Summary and Issues 3 and 4 of the report. The OIG Audit Division offers the following comments in response to the Community First letter:

- Lessons Learned
  As acknowledged by Community First, safeguards identified in this report were not sufficient to meet ISSG requirements. The safeguards also did not meet TAC and HIPAA requirements.

- Issue 3
  The OIG Audit Division evaluated the secondary application, and validated that the secondary application was used by claims processors to update or change data. The evaluation determined that changes to claims information were made during multiple phases of claims processing.

- Issue 4
  As acknowledged by Community First, access controls were not sufficient and accounts of former employees remained active after termination. Community First indicates controls were in place to prevent unauthorized access to AMISYS Advance but, as detailed in Issue 4, this audit identified 16 accounts belonging to former employees that retained access to both Active Directory and AMISYS Advance. Removing access to user accounts of former employees is a key control for protecting confidential HHS System information from unauthorized access, loss, and disclosure, and is required by ISSG, TAC, and HIPAA.

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
- Melissa Larson, CIA, CISA, CFE, IT Audit Manager
- Jim Hicks, CISA, IT Audit Project Manager
- Sarah Corrine Warfel, IT Staff Auditor
- Brian Baker, Staff Auditor
- Kathryn Messina, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Cecile Erwin Young, Acting Executive Commissioner
- Kara Crawford, Chief of Staff
- Victoria Ford, Chief Policy Officer
- Enrique Marquez, Chief Program and Services Officer
- 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
- Ying Chan, Chief Information Technology Officer
- Ivan Hovey, Director, HHSC IT Applications
- Shirley Erp, HHS Chief Information Security Officer

Community First

- Greg Gieseman, President and Chief Executive Officer
- Terry Fehlhaber, Chief Security Officer, and Director of Information Systems
- Laura Ketterman, Compliance and Privacy Officer

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 the OIG's mission and statutory responsibility includes:

- Sylvia Hernandez Kauffman, Inspector General
- Anita D'Souza, Chief of Staff and Chief Counsel
- Olga Rodriguez, Chief of Strategy
- Christine Maldonado, Chief of Operations and Workforce Leadership
- Brian Klozik, Deputy IG for Medicaid Program Integrity
- Lizet Hinojosa, Deputy IG for General Investigations
- David Griffith, Deputy IG for Audit
- Quinton Arnold, Deputy IG for Inspections and Interim Deputy IG for 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