TEXAS HEALTH AND HUMAN SERVICES COMMISSION

INSPECTOR GENERAL

AUDIT OF SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

FirstCare Health Plans

August 22, 2017
OIG Report No. AUD-17-017

HHSC IG

TEXAS HEALTH AND HUMAN SERVICES COMMISSION

INSPECTOR GENERAL

WHY THE IG CONDUCTED THIS AUDIT

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

WHAT THE IG RECOMMENDS

The HHSC Medicaid and CHIP Services Department should:

Require FirstCare to:

- Submit a complete security plan for applications that process or store confidential HHS System information.
- Improve access controls for systems containing confidential HHS System information.
- Strengthen password configurations.
- Document and test its incident response program.
- Track access to its data center.

Coordinate with HHS IT to establish protocols designed to ensure that any deficiencies in MCO security plans are identified and addressed before approval.

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

August 22, 2017

AUDIT OF SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

FirstCare Health Plans

WHAT THE IG FOUND

FirstCare submitted annual security plans, as required by the UMCC, to detail the design of IT security control structures for systems that process or store confidential HHS System information, for its HealthRules application that did not contain all required information. The incomplete plans were reviewed by HHSC and accepted, even though required information was missing.

In addition, FirstCare did not (a) adequately manage access to confidential HHS System information in its HealthRules application, (b) use password and server configuration settings that met required security standards, (c) document and test incident response procedures, and (d) effectively track physical access to its data center.

IT control areas in which FirstCare's existing controls did not fully comply with HHS Enterprise Information Security Standards and Guidelines (EISSG), as required by UMCC, are indicated in the table below.

Control Areas Tested	Operating System	Application	Database
Information Security Oversight	X	X	X
User Account Management	X	X	X
Configuration Settings	X	X	X
Information Systems Monitoring	X	X	X
Vulnerability Assessment and Remediation			

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

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

APPENDICES

INTRODUCTION

The Texas Health and Human Services Commission (HHSC) Inspector General (IG) Audit Division conducted an audit of security controls over confidential Health and Human Services (HHS) System information at FirstCare Health Plans (FirstCare). FirstCare 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. FirstCare processes and pays Medicaid and CHIP managed care provider claims, which contain confidential data, including protected health information. FirstCare 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 FirstCare 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

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

Background

FirstCare 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 through the HealthRules application. HealthRules adjudicates claims automatically using the Claims Edit System, which provides the logic rule sets and coding and claim edit tables for the adjudication of provider claims for payment.

Claims from providers are provided to FirstCare through a third-party clearinghouse,[2] Availity, which places the claims on its secure file server where FirstCare retrieves them utilizing secure file transfer protocol. A small number of providers, roughly five percent, submit paper claims by mail to a third-party

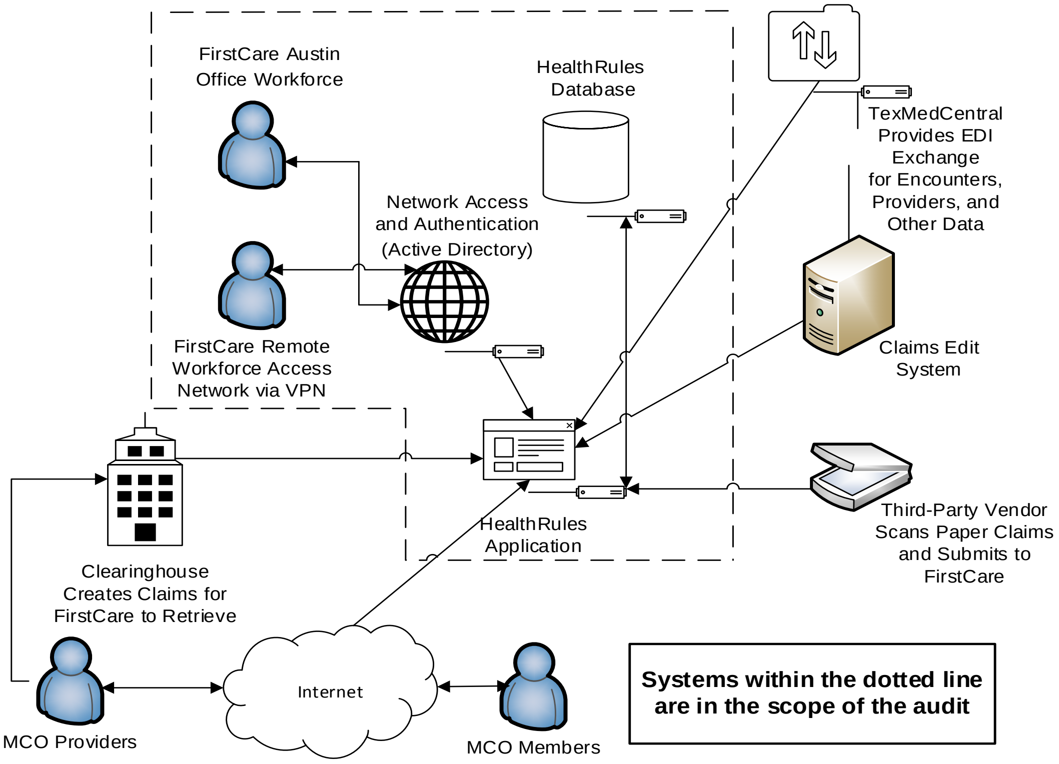
[1] A "member" is an individual who is enrolled with a state contracted Medicaid MCO as a subscriber or dependent. This term is used in the context of MCO, rather than fee-for-service, Medicaid administration.

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

vendor, BankTec, for scanning and formatting into electronic claim files. The vendor places these files on a FirstCare secure server, also using secure file transfer protocol. Therefore, all claims are received electronically via secure transmissions to FirstCare. Additionally, HealthRules provides explanations of benefits to providers and members through an online portal. FirstCare workforce in the Austin headquarters access the HealthRules application through the internal company network and are authenticated in Active Directory.[3] Remote workforce must log in through a secure virtual private network (VPN) and are authenticated to the network in Active Directory as well.

FirstCare receives and exchanges Medicaid and CHIP information with the Texas Medicaid and Healthcare Partnership (TMHP) through secure file transfers with TexMedCentral. A diagram of the system is illustrated in Figure 1.

Figure 1: FirstCare Systems Diagram


FirstCare Austin Office Workforce
HealthRules Database
TexMedCentral Provides EDI Exchange for Encounters, Providers, and Other Data
Network Access and Authentication (Active Directory)
FirstCare Remote Workforce Access Network via VPN
Claims Edit System
HealthRules Application
Third-Party Vendor Scans Paper Claims and Submits to FirstCare
Clearinghouse Creates Claims for FirstCare to Retrieve
Internet
MCO Providers
MCO Members
Systems within the dotted line are in the scope of the audit

Source: Prepared by IG Audit Division

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

The audit examined the HealthRules application and the associated infrastructure, operating system, and database that process and store claims detail information. The Claims Edit System was not included in the scope of this audit because the application does not store any confidential data.

FirstCare's data center provides the facility and information technology (IT) infrastructure for the HealthRules application. The IG Audit Division performed a physical security review at this location. FirstCare's backup and failover[4] locations were not included in the scope of this audit.

The Medicaid and CHIP Services Department (MCSD), HHS IT, and FirstCare share accountability for safeguarding state information systems in order to protect confidential information from accidental or unauthorized access, loss, or disclosure. The Uniform Managed Care Contract (UMCC) requires MCOs to submit a security plan annually for HHSC's review and approval.[5] The 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 Enterprise Information Security Standards and Guidelines (EISSG)
- 1 Tex. Admin. Code, §§ 202.1 and 202.3 and Subchapter B (Mar. 17, 2015) and (Mar. 16, 2016)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Health Information Technology for Economic and Clinical Health Act (HITECH Act)

The 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 FirstCare. Security controls must follow guidance provided in the EISSG catalog of security controls, which is based on the National Institute of Standards and Technology (NIST) security standards. The IG Audit Division applied the EISSG criteria, along with FirstCare's security policy

[4] "Failover" is a method of protecting computer systems from failure, in which standby equipment automatically takes over when the main system fails.

[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. 2.21 (Feb. 1, 2017).

[6] Uniform Managed Care Contract, Attachment A, § 11.08 Information Security, v. 2.16 (Sept. 1, 2015) through v. 2.21 (Feb. 1, 2017).

and procedures, to design audit tests to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by FirstCare.

The IG 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.

AUDIT RESULTS

The IG Audit Division assessed relevant security controls protecting confidential HHS System information in the custody of FirstCare, and specifically its HealthRules application. The key control areas and the associated control groups tested during the audit are identified in Table 1. Key control areas for information security contain controls that are required in order to provide reasonable assurance that material errors will be prevented or timely detected. Control groups are the EISSG-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	EISSG Control Groups
Information Security Oversight	Planning Controls Risk Assessment Controls
User Account Management	Access Controls Identification and Authentication
Configuration Settings	Configuration Management
Information Systems Monitoring	Incident Response
Vulnerability Assessment and Remediation	Security Assessment and Authorization Controls
Physical Security	Physical and Environmental Protection Controls

Source: Prepared by IG Audit Division based on EISSG

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

The IG Audit Division examined the IT security controls and relevant activities supporting data security at FirstCare. Audit work included (a) detailed tests of activities, supporting technologies, and data and (b) site visits to locations where key activities are performed or data is stored.

Audit results indicated that FirstCare had an adequate physical security environment in its primary data center to protect confidential information. However, improvements are needed in several control areas to further protect confidential information from unauthorized access, loss, or disclosure, including:

- Information security oversight
- User account management
- Configuration settings
- Information systems monitoring
- Physical security

Issue 1: Information Security Oversight

The UMCC requires FirstCare to submit a security plan annually. The EISSG requires MCSD, as the contract manager, to collaborate with the HHS Information Security Officer to ensure the security plan submitted by FirstCare is complete in accordance with the HHS information system security plan template.[7] Texas Administrative Code requires that the HHS Information Security Officer coordinate the review of data security requirements, specifications, and, if applicable, third-party risk assessments of any new computer applications or services that receive, maintain, and share confidential data.[8] The HHS information system security plan template[9] is to be used to document the required system security controls and satisfy the security monitoring requirements for contractors.[10]

The MCO is required to assign a security categorization to the system, such as high, moderate, or low, depending on the information it stores, processes, or transmits. Based on the security categorization, security controls are designed and implemented per the EISSG control catalog.[11] To comply with these requirements, FirstCare must document critical systems and facility security in accordance with the EISSG.

FirstCare Did Not Submit a Complete Security Plan as Required by the UMCC

FirstCare did not use the HHS information system security plan template to document its control environment. Each year, beginning in October 2014, FirstCare submitted an annual security plan to HHS. The annual security plans contained different content and levels of detail than they would have if FirstCare had used the HHS information system security plan template. Additionally, FirstCare was required to submit a security plan checklist that asserted the inclusion of all required elements in the submitted security plan. Although the checklist represented that all required details were included in FirstCare’s security plan, the security plans submitted for 2016 and 2017 were incomplete. FirstCare’s annual security plans did not provide sufficient detailed information to comply with the EISSG, as required by UMCC. The HHS information system security plan template contains requirements from each security control group defined by the

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

[8] 1 Tex. Admin. Code, § 202.21 (Mar. 17, 2015) and (Mar. 16, 2016).

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

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

[11] Enterprise 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).

EISSG and requires a description of security controls in place or planned to meet control requirements.

IT management at FirstCare indicated they were not aware of the contractual requirements to comply with the EISSG. Until a complete security plan is submitted, MCSD and HHS IT will not be aware of FirstCare’s control structure designed to comply with the EISSG and will be unable to effectively monitor the security of confidential HHS System information in the custody of FirstCare.

Recommendation 1.1

MCSD, through its contract oversight responsibilities, should require FirstCare to submit a complete security plan for the HealthRules application in accordance with the UMCC.

MCSD should consider tailored contractual remedies to compel FirstCare to submit a complete and compliant security plan for the HealthRules application.

MCSD Management Response

Action Plan

MCSD agrees with the recommendation. HHSC, Chief Information Security Officer, is in the process of updating the EISSG due to multiple changes in federal requirements. Due to the complex nature of the state and federal changes, HHSC, Chief Information Security Officer, is developing a tool to provide the details of selected controls. Both the new EISSG/IS-Controls and tool will be available in October 2017. The EISSG/IS-Controls and tool are required to satisfy the complete submission of the security plan. The Uniform Managed Care Contract will be updated to include the new requirements for the security plans with the March 2018 amendment.

Responsible Manager

Health Plan Management and Director, IT Health Services Systems

Target Implementation Date

August 1, 2018 for FirstCare submission of security plan

FirstCare's Incomplete Security Plan Was Reviewed and Accepted by HHSC IT

HHSC IT Health Services Systems did not provide sufficient oversight or collaborate with the HHS Information Security Officer in reviewing security plans from FirstCare. FirstCare provided its security plans and security plan checklists annually to MCSD, as required.[12] The FirstCare security plans and associated checklists were obtained and reviewed by HHSC IT Health Services Systems.

However, FirstCare (a) submitted security plans that did not contain the content that was required by the EISSG and (b) asserted the plans were complete in the associated security plan checklists. The reviews performed did not identify the missing elements of the security plans, and the security plans were not returned to FirstCare to request revisions or to include detailed descriptions of the FirstCare IT control environment in accordance with contract requirements. Approval of the incomplete security plans creates a false assurance to HHSC that FirstCare's security controls are adequately designed to protect confidential HHS System information and hinders HHSC's ability to hold FirstCare accountable for the incomplete security plans.

Recommendation 1.2

MCSD, in coordination with HHS IT Applications and the Enterprise Information Security Office, should establish formal protocols for review and approval of MCO security plans to ensure that security plans are appropriately reviewed and that any deficiencies are addressed prior to approval.

MCSD Management Response

Action Plan

MCSD agrees with the recommendation. Health Plan Management will work with HHSC IT Health Services Systems and the EISO to develop a process to coordinate the HHSC IT Health Systems Services review of MCO security plans so that security plans are appropriately reviewed and any deficiencies are addressed prior to approval.

Responsible Manager

Director, Health Plan Management and Director, IT Health Services Systems

Target Implementation Date

June 2018

[12] HHSC Uniform Managed Care Manual, Chapter 5: Deliverables, Report Formats, Due Dates, §§ 5.0, Consolidated Deliverables Matrix v. 2.3 (Jan. 5, 2015) through v. 2.4 (Sept. 1, 2016) and 5.2, MIS Deliverables/Formats, v. 2.0 (Feb. 1, 2015).

Issue 2: User Account Management

User account management consists of procedures to request, establish, issue, 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. Privileged 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 (non-unique) or generic privileged accounts.

Many shared or generic privileged accounts are built-in system accounts automatically created when an operating system, application, or database is first installed. Audit results indicated that FirstCare maintained adequate control over these accounts.

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.[13] 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.

FirstCare Granted Excessive Privileged Access Within HealthRules

FirstCare did not limit user access within the HealthRules application and database to only the permissions needed to perform job duties. FirstCare granted privileged access to 14 end users in IT Operations, including one contractor, who did not require these permissions to perform their job duties.

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

The privileged accounts allowed access to the super-user group, which grants all permissions within HealthRules, and has the ability to add, modify, or delete data involving member benefits, claims processing, and financial billings and receivables. In addition, individuals with access to the super-user group have the ability to disable, circumvent, or alter security configurations and settings. Access to the HealthRules application and database can be controlled through role-based access; however, FirstCare had not designed or implemented role-based access and separation of duties for HealthRules.

FirstCare Did Not Timely Disable User Accounts from the HealthRules Application and the FirstCare Network

FirstCare did not timely terminate 23 former employee accounts from the HealthRules application. Of the 23 accounts, 21 had been disabled in the FirstCare network, preventing network login and prohibiting access to HealthRules and related confidential information. While the removal of the network accounts reduced the risk of unauthorized access to the HealthRules application, the active accounts created weaknesses that could be exploited to inappropriately view, modify, or delete HHS System information.

FirstCare did not disable three network accounts from Active Directory, which is used to control network access. These three accounts retained access to the FirstCare IT network, and two of the three accounts retained access to the HealthRules application. The absence of effective controls to remove access for terminated users increases the risk of unauthorized access to confidential HHS System information. One of the two accounts with access to the HealthRules application remained active for more than a year after the user left employment.

FirstCare had manual processes for disabling terminated user accounts, and completed quarterly user account reviews. The controls processes to detect and remove users with unauthorized access to the FirstCare computer network and HealthRules application were not consistently performed.

Recommendation 2

MCSD, through its contract oversight responsibilities, should require FirstCare to:

- Limit user account permissions to only those activities needed to perform job responsibilities.

- Review access to confidential HHS System information and recertify accounts, at least annually, for appropriateness and to ensure that terminated user accounts are disabled in Active Directory and HealthRules.

MCSD should consider tailored contractual remedies to compel FirstCare to effectively perform account management activities.

MCSD Management Response

Action Plan
MCSD agrees with the recommendation. The Department will allow FirstCare fifteen (15) business days from receipt of the final audit report to submit a corrective action plan (CAP) that identifies the specific steps that FirstCare will take to ensure that FirstCare:

1) Limits user account permissions to only those activities needed to perform job responsibilities; and
2) Reviews access to Confidential HHS System information and recertifies accounts, at least annually, for appropriateness and to ensure that terminated user accounts are disabled in Active Directory and HealthRules.

Health Plan Management will coordinate a review, by HHSC IT Health Services Systems, of FirstCare's corrective actions performed to implement this recommendation.

The Medicaid/CHIP Services Department expects FirstCare to take immediate corrective action under the CAP and will allow FirstCare 90 calendar days to implement all actions within the CAP. The Medicaid/CHIP Services Department will require FirstCare to submit monthly updates detailing the status of each milestone.

Responsible Manager
Director, Health Plan Management and Director, IT Health Services Systems

Target Implementation Date
Ninety days from receipt of the final audit for FirstCare corrective actions

Issue 3: Configuration Settings

The EISSG specifies that documentation and maintenance of current baseline configuration settings for network components is a key control in securing systems.[14] Baseline security configurations include documented standards about information system components' settings and parameters to protect data. Configuration standards include password settings, software installation parameters, and server settings for functions, ports, protocols, services, and remote connections.

FirstCare Password Configurations Did Not Meet UMCC Standards and FirstCare Policy

The HealthRules application password settings were weaker than the EISSG standards for password configurations, which the UMCC requires MCOs to follow. In addition, password configurations implemented for the HealthRules application were not in compliance with FirstCare policy.

Detailed results 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, contractors, and providers, and applicable state officials authorized to receive computer vulnerability information.

Recommendation 3.1

MCSD, through its contract oversight responsibilities, should require FirstCare to address identified password control weaknesses and ensure password requirements are enforced.

See separate document, "Confidential Issues: Audit of Security Controls Over Confidential HHS System Information at FirstCare Health Plans."

MCSD should consider tailored contractual remedies to compel FirstCare to comply with password requirements.

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

MCSD Management Response

Action Plan

MCSD agrees with the recommendation. The Department will allow FirstCare fifteen (15) business days from receipt of the final audit report to submit a corrective action plan (CAP) that identifies the specific steps that FirstCare will take to ensure that FirstCare addresses identified password control weaknesses and ensures password requirements are enforced.

Health Plan Management will coordinate a review by HHSC IT Health Services Systems of FirstCare's corrective actions performed to implement this recommendation.

The Medicaid/CHIP Services Department expects FirstCare to take immediate corrective action under the CAP and will allow FirstCare 90 calendar days to implement all actions within the CAP. The Medicaid/CHIP Services Department will require FirstCare to submit monthly updates detailing the status of each milestone.

Responsible Manager

Director, Health Plan Management and Director, IT Health Systems Services

Target Implementation Date

Ninety days from receipt of the final audit for FirstCare corrective actions

FirstCare Baseline Server Configurations Were Not Documented

FirstCare did not have documented baseline configuration settings for servers. While a process for maintaining configurations was verbally communicated to the IG Audit Division, evidence was not provided to support the asserted control design. Documented server configurations are an essential component to harden system security, develop repeatable builds, implement efficient change management, and assist in troubleshooting security events or incidents. Baseline configuration settings for new server installations and server rebuilds help ensure that services, ports, and default accounts are appropriately implemented and maintained.

Recommendation 3.2

MCSD, through its contract oversight responsibilities, should require FirstCare to document baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

MCSD should consider tailored contractual remedies to compel FirstCare to adequately document the configuration of servers.

MCSD Management Response

Action Plan

MCSD agrees with the recommendation. The Department will allow FirstCare fifteen (15) business days from receipt of the final audit report to submit a corrective action plan (CAP) that identifies the specific steps that FirstCare will take to ensure that FirstCare documents baseline configurations for servers and any other network devices that store and process confidential HHS System information.

Health Plan Management will coordinate a review by HHSC IT Health Systems Services of FirstCare's corrective actions performed to implement this recommendation.

The Medicaid/CHIP Services Department expects FirstCare to take immediate corrective action under the CAP and will allow FirstCare 90 calendar days to implement all actions within the CAP. The Medicaid/CHIP Services Department will require FirstCare to submit monthly updates detailing the status of each milestone.

Responsible Manager

Director, Health Plan Management and Director, Health Systems Services

Target Implementation Date

Ninety days from receipt of the final audit for FirstCare corrective actions

Issue 4: Information Systems Monitoring

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 the EISSG.[15] 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.

FirstCare Did Not Have an Effective Process for Responding to Incidents

FirstCare utilized a variety of software and devices to prevent and detect security events over its network. However, FirstCare did not have a detailed and tested process for responding to security incidents and did not train its workforce on how to properly respond to security events. The EISSG requires documented controls for incident response, which include having a defined process for responding to security incidents, minimizing impact, and reducing the likelihood of a reportable privacy breach involving confidential HHS System information.[16]

Security incidents may involve exploited vulnerabilities, such as allowing a computer virus to infect the network. Effective incident response procedures can minimize the loss and destruction of data and address the exploited weaknesses to prevent recurrence. The absence of a documented incident response process increases the possibility of a security event escalating to a privacy breach.

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

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

Recommendation 4

MCSD, through its contract oversight responsibilities, should require FirstCare to:

- Develop and document incident response policies and processes that define the type of incidents and the roles and responsibilities for responding to each.

- Annually train its workforce on incident response procedures, and conduct annual incident response tests and exercises.

MCSD should consider tailored contractual remedies to compel FirstCare to develop and maintain an incident response plan, and provide annual training to its workforce.

MCSD Management Response

Action Plan

MCSD agrees with the recommendation. The Department will allow FirstCare fifteen (15) business days from receipt of the final audit report to submit a corrective action plan (CAP) that identifies the specific steps that FirstCare will take to ensure that FirstCare:

1) Develops and documents incident response policies and processes that define the type of incidents and the roles and responsibilities for responding to each; and

2) Annually trains its workforce on incident response procedures, and conduct annual incident response tests and exercises.

Health Plan Management will coordinate a review by HHSC IT Health Systems Services of FirstCare's corrective actions performed to implement this recommendation.

The Medicaid/CHIP Services Department expects FirstCare to take immediate corrective action under the CAP and will allow FirstCare 90 calendar days to implement all actions within the CAP. The Medicaid/CHIP Services Department will require FirstCare to submit monthly updates detailing the status of each milestone.

Responsible Manager

Director, Health Plan Management and Director, Health Systems Services

Target Implementation Date

Ninety days from receipt of the final audit for FirstCare corrective actions

Issue 5: Physical Security

The EISSG requires FirstCare to limit physical access to information systems, equipment, and operating environments to authorized individuals.[17] Physical security controls include maintaining physical access audit logs for entry into data centers, escorting visitors, and securing access keys, combinations, and other physical access devices such as badges. Restricting data center access helps to prevent (a) interruptions in computer services due to physical damage, (b) unauthorized disclosure of confidential information, (c) loss of control over system integrity, and (d) theft of equipment or confidential information.

FirstCare Data Center Access was Not Sufficiently Controlled

From September 2015 to December 2016, there were 89 entries to the data center in which the specific individual who accessed the data center could not be identified as required by the EISSG.[18] For 25 entries, a temporary badge was utilized to access the data center without proper logging of the individual issued the badge or the retention of sign-in logs to the data center. By not maintaining accurate audit logs for access to the data center using the temporary badges, FirstCare (a) places confidential HHS System information at risk for unauthorized viewing or loss of integrity and (b) is unable to identify and hold individuals accountable for inappropriate access.

For the other 64 entries, FirstCare's badge access system initially recorded the appropriate badge holder's identity, but overwrote historical entries of badge holders when associated badge access cards were assigned to different individuals. In addition, FirstCare did not have a manual process for tracking historical badge assignments. Consequently, FirstCare was unable to (a) identify individuals who accessed the data center using a badge that was later reassigned to a different workforce member or (b) reconcile badge issuance to a specific individual at a point in time. Responsible IT management at FirstCare indicated they were working to implement control processes to address the logging, tracking, and identification of historical badge assignments.

[17] Enterprise Information Security Standards and Guidelines Controls Catalog, § 7.11, Physical and Environmental Protection v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[18] Enterprise Information Security Standards and Guidelines Controls Catalog, § 7.11, Physical and Environmental Protection, PE-2, Physical Access Authorizations and PE-3, Physical Access Control v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Recommendation 5

MCSD, through its contract oversight responsibilities, should require FirstCare to secure and track custody of badges that provide access to the data center and maintain accurate records of all authorized access and entry.
MCSD should consider tailored contractual remedies to compel FirstCare to maintain accurate records of authorized access and entry to the data center.

MCSD Management Response

Action Plan
MCSD agrees with the recommendation. The Department will allow FirstCare fifteen (15) business days from receipt of the final audit report to submit a corrective action plan (CAP) that identifies the specific steps that FirstCare will take to ensure that FirstCare secures and tracks custody of badges that provide access to the data center and maintain accurate records of all authorized access and entry.

Health Plan Management will coordinate a review by Health Systems Services of FirstCare's corrective actions performed to implement this recommendation.

The Medicaid/CHIP Services Department expects FirstCare to take immediate corrective action under the CAP and will allow FirstCare 90 calendar days to implement all actions within the CAP. The Medicaid/CHIP Services Department will require FirstCare to submit monthly updates detailing the status of each milestone.

Responsible Manager
Director, Health Plan Management and Director, Health Systems Services

Target Implementation Date
Ninety days from receipt of the final audit for FirstCare corrective actions

CONCLUSION

The IG Audit Division completed an audit of selected security controls over confidential HHS System information in the custody of FirstCare. The audit included an evaluation of IT security controls over the FirstCare HealthRules application. The IG Audit Division conducted site visits at FirstCare in April and May 2017.

The IG Audit Division concluded:

- Security plans submitted by FirstCare were not sufficient to meet UMCC requirements.

- HHSC IT Health Services Systems approved FirstCare’s security plans, but did not identify incomplete elements in FirstCare’s security plans or require FirstCare to bring its plans into compliance with the EISSG, as required by UMCC.

- User access to information systems that contained confidential HHS System information was not effectively managed.

- Password configurations were not in compliance with the EISSG, as required by UMCC.

- Server baseline configuration settings were not documented.

- Incident response procedures were not documented or tested, and staff were not trained on incident response.

- Data center badge custody was not tracked to provide an accurate history of entries by workforce or visitors.

The IG Audit Division offered recommendations which, when implemented, will result in FirstCare having:

- A complete and reliable security plan.
- Stronger account management practices and password configurations.
- Documented baseline server configurations.
- Documented, tested security incident response procedures and workforce trained for effective response.
- Accurate logging of current and historical data center access.

The IG Audit Division thanks the management and staff of MCSD, HHSC IT Health Services Systems, HHS Information Systems Security, and FirstCare 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 FirstCare.

Scope

The scope of the IT security assessment of FirstCare included:

- Logical and physical security controls, including network access and authentication, designed to safeguard the HealthRules application and associated database, which process and store confidential HHS System information.
- Security plans and associated HHSC security plan review processes for fiscal years 2016 and 2017.
- Controls for user account management, information system monitoring, and physical access to the data center in effect from September 2015 through April 2017.

Methodology

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

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

The IG Audit Division issued an engagement letter to FirstCare on April 7, 2017, providing information about the upcoming audit, and conducted fieldwork at FirstCare’s facility in Austin, Texas, on April 10 and 11, 2017, and conducted a physical security review of FirstCare’s data center on May 8, 2017. While on site, the IG Audit Division interviewed responsible personnel, observed and tested configuration settings, and reviewed documentation relevant to support the control environment.

Criteria

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

- Enterprise Information Security Standards and Guidelines Controls Catalog v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015)
- 1 Tex. Admin. Code, §§ 202.1 and 202.3 and Subchapter B (Mar. 17, 2015) and (Mar. 16, 2016)
- 45 C.F.R. Part 160 and Subparts A and C of Part 164 (Feb. 20, 2013)
- Uniform Managed Care Contract, Attachment A, v. 2.16 (Sept. 1, 2015) through v. 2.22 (Feb. 1, 2017)
- HHSC Uniform Managed Care Manual Chapter 5: Deliverables, Report Formats, Due Dates, §§ 5.0, Consolidated Deliverables Matrix v. 2.3 (Jan. 5, 2015) through v. 2.4 (Sept. 1, 2016) and 5.2, MIS Deliverables/Formats, v. 2.0 (Feb. 1, 2015)
- HHS Information Security Plan Template v. 1.3 (July 2015) through v. 1.6 (May 2016)
- HITECH Act, Pub. L. No. 111–5 (Feb. 17, 2009)

Auditing Standards

The IG Audit Division analyzed information and documentation it collected to determine whether selected logical controls over confidential HHS System information stored and processed by FirstCare were well designed and operating effectively.

The IG 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 IG Audit Division believes the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

Appendix B: Testing Methodology

The IG Audit Division examined FirstCare IT security controls that were in effect during the period from September 2015 to April 2017. After performing a risk and controls assessment of FirstCare's documented IT security control structure, the IG Audit Division performed testing of selected security controls over the HealthRules production environment and supporting infrastructure.

Information Security Oversight

The IG Audit Division examined processes over HHSC's review and acceptance of annual FirstCare security plans to determine whether the plans were complete, accurate, and approved.

User Account Management

The IG 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 IG Audit Division tested all user accounts for HealthRules and the FirstCare network environment.

Configuration Settings

The IG Audit Division interviewed FirstCare IT staff and examined applicable IT policies and system configurations.

Information Systems Monitoring

The IG Audit Division interviewed FirstCare 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 FirstCare network.

Vulnerability Assessment and Remediation

The IG Audit Division reviewed the results of the most recent vulnerability assessments and penetration tests conducted on behalf of FirstCare by a third-party vendor and examined FirstCare'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

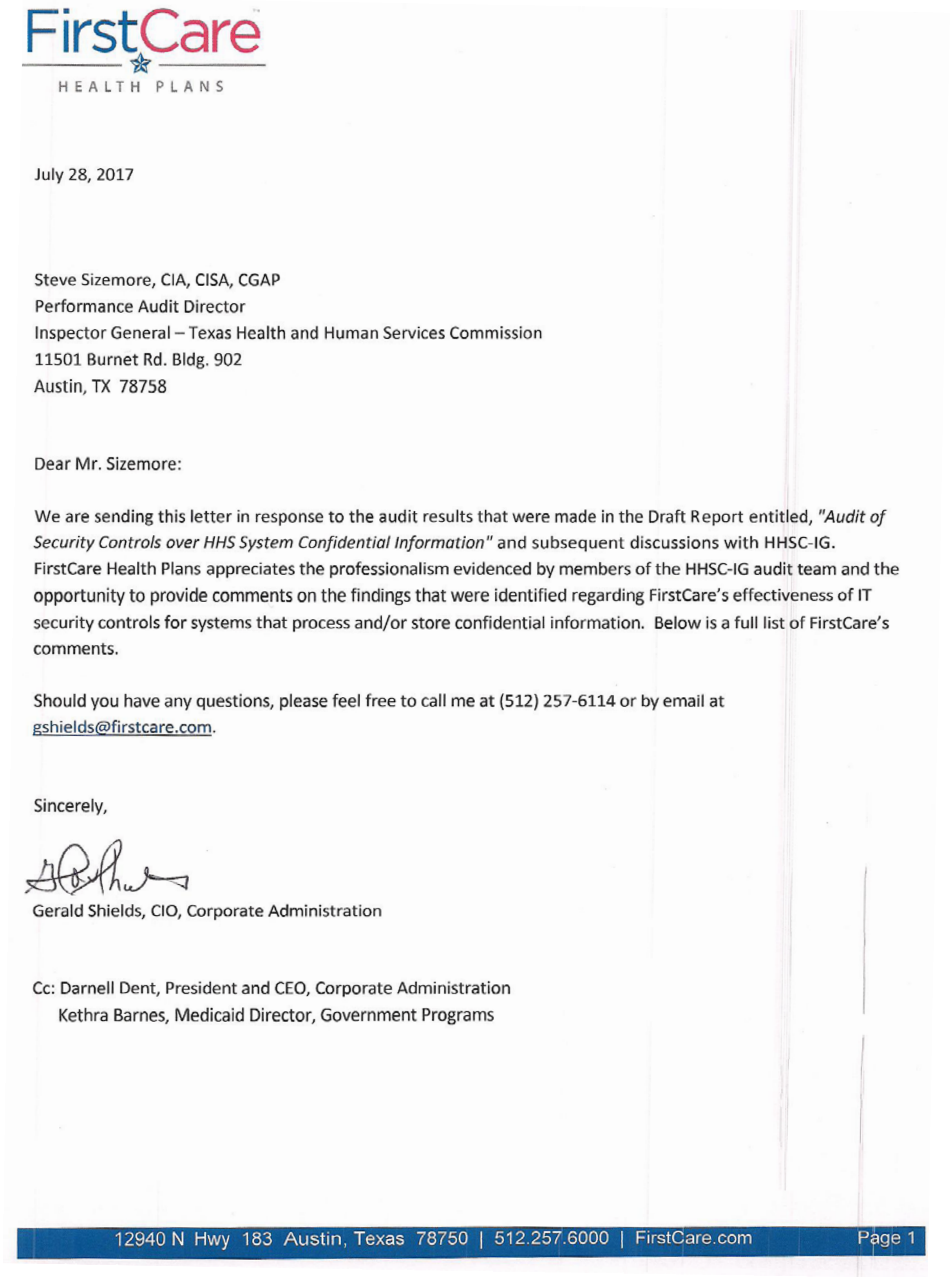
The IG Audit Division performed a physical security inspection of the FirstCare data center and evaluated badge access logs to determine whether access was limited to authorized workforce and visitors.

Appendix C: Controls Tested

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

Control Group	Control Description	Control Issue - Control Design (CD) or Control Effectiveness (CE)	Report Issue
Incident Response (IR)			
IR-1	Incident Response Policy and Procedures		N/A
IR-3	Incident Response Testing	CD	4
IR-4	Incident Handling	CD	4
IR-5	Incident Monitoring	CD	N/A
IR-6	Incident Reporting	CD	4
IR-8	Incident Response Plan	CD	4
Physical and Environmental Protection Controls (PE)			
PE-3	Physical Access Control	CE	5
PE-6	Monitoring Physical Access	CE	5
PE-8	Visitor Access Records	CE	5
Planning Controls (PL)			
PL-1	Security Planning Policy and Procedures		N/A
PL-2	System Security Plan	CE	1
PL-8	Information Security Architecture		N/A
Risk Assessment Control			
RA-1	Risk Assessment Policy and Procedures		N/A
RA-2	Security Categorization		N/A
RA-3	Risk Assessment		N/A
RA-5	Vulnerability Scanning		N/A

Appendix D: FirstCare Management Comment



FirstCare
HEALTH PLANS

July 28, 2017

Steve Sizemore, CIA, CISA, CGAP
Performance Audit Director
Inspector General – Texas Health and Human Services Commission
11501 Burnet Rd. Bldg. 902
Austin, TX 78758

Dear Mr. Sizemore:

We are sending this letter in response to the audit results that were made in the Draft Report entitled, "*Audit of Security Controls over HHS System Confidential Information*" and subsequent discussions with HHSC-IG. FirstCare Health Plans appreciates the professionalism evidenced by members of the HHSC-IG audit team and the opportunity to provide comments on the findings that were identified regarding FirstCare's effectiveness of IT security controls for systems that process and/or store confidential information. Below is a full list of FirstCare's comments.

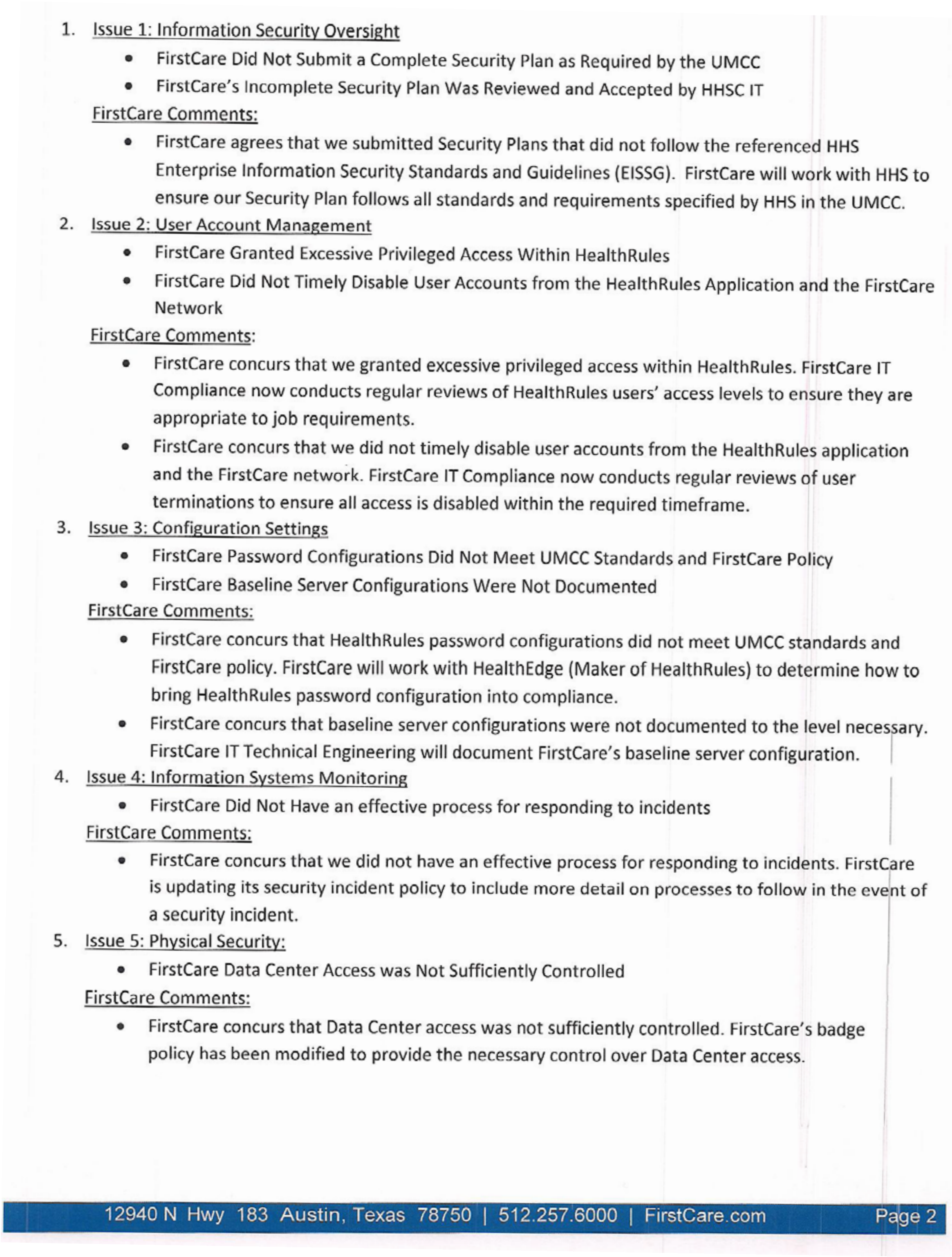
Should you have any questions, please feel free to call me at (512) 257-6114 or by email at gshields@firstcare.com.

Sincerely,

Gerald Shields, CIO, Corporate Administration

Cc: Darnell Dent, President and CEO, Corporate Administration
Kethra Barnes, Medicaid Director, Government Programs

12940 N Hwy 183 Austin, Texas 78750 | 512.257.6000 | FirstCare.com Page 1



1. Issue 1: Information Security Oversight
   - FirstCare Did Not Submit a Complete Security Plan as Required by the UMCC
   - FirstCare's Incomplete Security Plan Was Reviewed and Accepted by HHSC IT

   FirstCare Comments:
   - FirstCare agrees that we submitted Security Plans that did not follow the referenced HHS Enterprise Information Security Standards and Guidelines (EISSG). FirstCare will work with HHS to ensure our Security Plan follows all standards and requirements specified by HHS in the UMCC.
2. Issue 2: User Account Management
   - FirstCare Granted Excessive Privileged Access Within HealthRules
   - FirstCare Did Not Timely Disable User Accounts from the HealthRules Application and the FirstCare Network

   FirstCare Comments:
   - FirstCare concurs that we granted excessive privileged access within HealthRules. FirstCare IT Compliance now conducts regular reviews of HealthRules users' access levels to ensure they are appropriate to job requirements.
   - FirstCare concurs that we did not timely disable user accounts from the HealthRules application and the FirstCare network. FirstCare IT Compliance now conducts regular reviews of user terminations to ensure all access is disabled within the required timeframe.
3. Issue 3: Configuration Settings
   - FirstCare Password Configurations Did Not Meet UMCC Standards and FirstCare Policy
   - FirstCare Baseline Server Configurations Were Not Documented

   FirstCare Comments:
   - FirstCare concurs that HealthRules password configurations did not meet UMCC standards and FirstCare policy. FirstCare will work with HealthEdge (Maker of HealthRules) to determine how to bring HealthRules password configuration into compliance.
   - FirstCare concurs that baseline server configurations were not documented to the level necessary. FirstCare IT Technical Engineering will document FirstCare's baseline server configuration.
4. Issue 4: Information Systems Monitoring
   - FirstCare Did Not Have an effective process for responding to incidents

   FirstCare Comments:
   - FirstCare concurs that we did not have an effective process for responding to incidents. FirstCare is updating its security incident policy to include more detail on processes to follow in the event of a security incident.
5. Issue 5: Physical Security:
   - FirstCare Data Center Access was Not Sufficiently Controlled

   FirstCare Comments:
   - FirstCare concurs that Data Center access was not sufficiently controlled. FirstCare's badge policy has been modified to provide the necessary control over Data Center access.

Appendix E: Report Team and 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
- Jim Hicks, CISA, IT Audit Project Manager
- Amy Behrnes, CIA, IT Audit Project Manager
- Corrine Warfel, IT Staff Auditor
- Brian Baker, Staff Auditor
- Kathryn Messina, 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, Information Technology
- Karen Ray, Chief Counsel
- Karin Hill, Director of Internal Audit
- Jami Snyder, Associate Commissioner, Medicaid and CHIP Services Department
- Tony Owens, Deputy Associate Commissioner, Health Plan Monitoring and Contract Services, Medicaid and CHIP Services Department
- Grace Windbigler, Director, Health Plan Management, Medicaid and CHIP Services Department
- Ying Chan, Chief Information Technology Officer
- Ivan Hovey, Director, HHSC IT Applications

- Shirley Erp, HHS Chief Information Security Officer

FirstCare Health Plans

- Darnell Dent, Chief Executive Officer
- Gerald Shields, Chief Information Officer
- Kethra Barnes, Director of Medicaid
- Jenny Garza, Manager of Compliance

Appendix F: IG Mission and Contact Information

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:

- Sylvia Hernandez Kauffman, Principal Deputy Inspector General
- 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
- Alan Scantlen, Deputy IG for Data and Technology
- Judy Knobloch, Interim Deputy IG for Medical Services
- Anita D'Souza, Chief Counsel

To Obtain Copies of IG Reports

- IG 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 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