Audit Report

# Security Controls Over Confidential HHS Information

**Parkland Community Health Plan, Inc.**

**January 20, 2021**
**OIG Report No. AUD-21-006**

Inspector General

Texas Health and Human Services

Texas Health and Human Services Office of Inspector General Audit and Inspections Division

# SECURITY CONTROLS OVER CONFIDENTIAL HHS INFORMATION

*Parkland Community Health Plan, Inc.*

January 20, 2021

Dear Mr. Wendling:

Overall, Parkland Community Health Plan, Inc. (Parkland) implemented controls to safeguard confidential Health and Human Services (HHS) System information and developed procedures to ensure the continuation of the operations necessary to deliver services to members in the event of an emergency or disaster.

Access to confidential HHS System information must be managed in accordance with HHS Information Security Controls (IS-Controls). Parkland's processes for managing access and authentication to confidential HHS System information in its network and claims management system did not meet all HHS IS-Controls requirements.

The attachment to this letter contains additional details on the issue and associated recommendation. In its management response, Parkland indicated it will take appropriate actions by February 2021 to address the issue identified in this report.

Sincerely,

Audrey O'Neill, CIA, CFE, CGAP
Chief of Audit and Inspections

Attachment

cc: Cecile Erwin Young, HHS Executive Commissioner
Sylvia Hernandez Kauffman, HHS Inspector General

## Background

During state fiscal year 2019, Parkland provided managed care to an average of 183,420 members through the Medicaid State of Texas Access Reform (STAR) and Children's Health Insurance Program (CHIP) programs. During the same period, HHSC made capitation payments totaling $545,030,675 to Parkland.

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

# ATTACHMENT

## Section 1: Summary of Audit Findings and Recommendations

OIG Audit reviewed key security controls protecting confidential HHS System information in the custody of Parkland and its subcontracted third-party administrator, including its claims management application and network directory that contained confidential HHS System information.

Parkland complied with HHS IS-Controls requirements tested for the following control groups: information security oversight, information systems monitoring, risk assessment, workforce training, change control, media protection, and business continuity. HHS IS-Controls defines the control groups and requirements for security control baselines intended to protect confidential HHS System information from unauthorized access, modification, or destruction. Each control group contains multiple control enhancements, which can be layered based on data risks, to provide customized controls for information security.

The HHS Information Security Office has classified the managed care organization systems that process and store HHS system information as requiring the HHS IS-Controls baseline of "moderate" with a Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirement overlay; therefore, audit work performed by OIG Audit applied the moderate HHS IS-Controls requirements.

HHS IS-Controls requires this information system to automatically disable inactive accounts within 90 days;[1] review accounts for compliance with account management requirements at least every 365 days;[2] enforce the limit of consecutive invalid log on attempts;[3] and meet minimum authentication requirements.[4]

Pursuant to Standard 9.61 of *Government Auditing Standards* issued by the Comptroller General of the United States, certain information related to security configurations and vulnerabilities was omitted from this report because the information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code Section 552.139(b), the omitted information is also exempt from the requirements of the Texas Public Information Act.

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

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

[3] HHS Information Security Controls, Appendix B, AC-07, v. 1.0 (Feb. 9, 2018).

[4] HHS Information Security Controls, Appendix B, IA-05, v. 1.0 (Feb. 9, 2018).

Section 3 includes an overview of all control groups and baselines tested in this audit. Table 1 summarizes the issue and recommendation.

**Table 1: Summary of Issue and Recommendation**

| Description of Issue | Recommendation |
|---|---|
| Parkland did not (a) consistently ensure that network and claims management application accounts with access to confidential HHS System information were reviewed and disabled when user access was no longer required, (b) enforce requirements for locking accounts when unsuccessful log on attempts occurred, and (c) enforce all authentication requirements as required by HHS IS-Controls. | Parkland should ensure access and authentication controls for its network and claims management application are managed in accordance with HHS IS-Controls requirements. |

Details of this issue were communicated separately to Parkland management in writing.

## Management Response to Issue (a)

*The plan agrees with the OIG recommendation.*

Action Plan

*Parkland Community Health Plan's (PCHP's) Information Technology Department has implemented a process for periodic review of its third-party administrator's claims application access by PCHP employees. This process is comprised of the following three activities.*

1. *PCHP IT Department has assumed the responsibility for maintenance of system access requests for the third party-administrator's applications. Tracking of all users has been established.*

2. *PCHP IT Department will perform a weekly review of PCHP employees whose employment has ended and will send notification to its third-party administrator to terminate access.*

3. *PCHP IT Department will obtain a list of PCHP employees with active access which will include date of last access and will send notification to its third-party party administrator to terminate access for any employee who has not accessed the system for 90 days. This will occur quarterly.*

Responsible Managers

*Information Technology Support Manager*
*Senior Director, Information Technology and Reporting*

Target Implementation Date

*February 1, 2021*

## Management Response to Issue (b)

*The plan agrees with the OIG recommendation.*

Action Plan

*Parkland will segregate PCHP employees within its network and apply unique policies to meet the OIG recommendation.*

Responsible Managers

*Manager, Systems Engineering*
*Vice President and Chief Information Security Officer*

Target Implementation Date

*February 26, 2021*

## Management Response to Issue (c)

*The plan agrees with the OIG recommendation.*

Action Plan

*Parkland will segregate PCHP employees within its network and apply unique policies to meet the OIG recommendation.*

Responsible Managers

*Manager, Systems Engineering*
*Vice President and Chief Information Security Officer*

Target Implementation Date

*February 26, 2021*

## Section 2: Objective, Scope, Methodology, Criteria, and Standards

Parkland coordinates health services for members[5] in the Medicaid STAR and CHIP programs and supports Medicaid STAR and CHIP (a) provider claims processing and (b) provider and member benefits administration. To augment its Medicaid and CHIP operations, Parkland subcontracted with a third-party administrator for in-scope activities including provider claims processing, call center services supporting members and providers, and related IT functions.

OIG Audit previously conducted an IT security and business continuity and disaster recovery audit of the subcontracted third-party administrator. The engagement included reviews of the third-party administrator's infrastructure, including networks, applications, databases, web portals, and call centers supporting members and providers. Results of the previous engagement relevant to the scope of this audit of Parkland were relied on where applicable and limited the scope and extent of controls tested at Parkland.

When working remotely, Parkland's workforce accesses the network via a virtual private network (VPN) that authenticates users through a directory service. Authorized individuals in Parkland's workforce, including contracted agents, access the subcontracted third-party administrator's network via a second VPN connection that authenticates the users through a multi-factor sign-on solution[6] and directory service. Once authenticated on the network, authorized users can access the claims management applications and other IT services.

Parkland maintained a single network directory, which stored claims reports and protected health information. Parkland's subcontracted third-party administrator maintained multiple data centers designed to sustain operations in the event of a disruption to the primary data center. Claims data was backed-up daily for storage at an off-site facility.

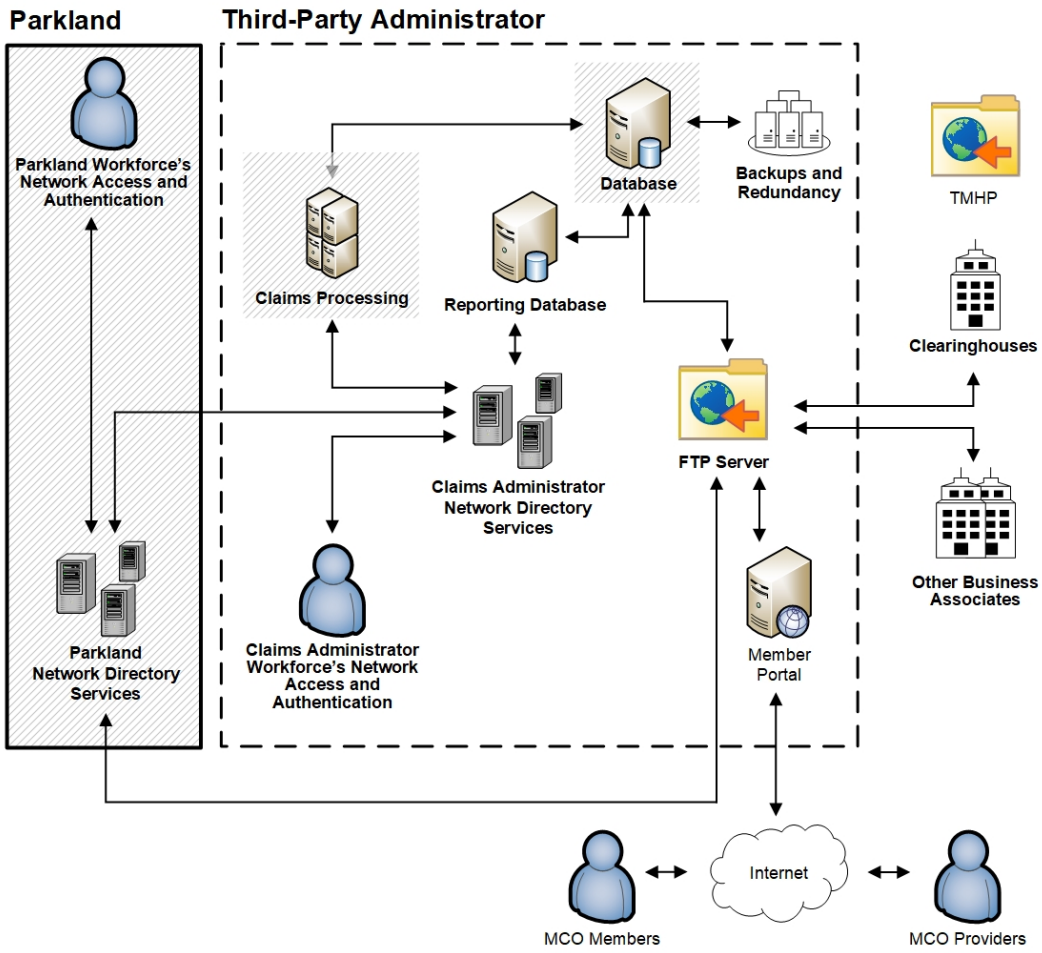
Parkland received and exchanged Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) through clearinghouses, an explanation of benefits portal, and other third parties using secure file transfers through its subcontracted third-party administrator.

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

[6] "Single sign-on" is an authentication process that allows a user to present two pieces of evidence when logging into an account.

Figure A is an illustration of Parkland's systems and processes. The information presented in the solid line box represents Parkland's network, while the information in the dashed line box represents the network of Parkland's subcontracted third-party administrator. The shaded areas designate the applications and processes in the scope of the audit, including access to Parkland's network, claims management application, and associated databases.

## Figure A: Parkland's Systems




*Source: OIG Audit and Inspections Division*

## Objective and Scope

The audit objectives were to assess the design and effectiveness of:

- Selected logical security controls over confidential HHS System information stored and processed by Parkland.

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

The audit scope covered, for September 1, 2019, through August 31, 2020, the Medicaid contracts between Parkland and the Texas Health and Human Services Commission (HHSC) and included a review of significant controls and control components including:

- IT controls for logical security implemented to protect access to confidential HHS System information processed and stored within (a) Parkland's network and (b) its third-party administrator's claims management application and related databases.

- Information system security planning, risk management, incident monitoring, and response management.

- Information systems security policy, media destruction procedures, and workforce security awareness training.

- General controls supporting systems backup, contingency planning, and disaster recovery activities.

## Methodology

OIG Audit reviewed key security controls protecting confidential HHS System information in the custody of Parkland, primarily the claims management application. Control groups are the HHS IS-Controls defined groupings of baseline security controls. Each control group contains multiple control baselines, which can be layered based on data risks, to provide customized controls for information security.

Section 3 presents an overview of all control groups and baselines tested in this audit.

OIG Audit examined key IT security controls and relevant activities supporting data confidentiality, integrity, and availability at Parkland by (a) reviewing policies and procedures in detail to gain an understanding of the design of controls,

(b) conducting WebEx sessions to interview key personnel and observe security procedures and processes, and (c) testing the effectiveness of the controls designed to protect or recover information processed and stored by Parkland.

Parkland subcontracted claims processing, member and provider servicing, and related IT functions to a third-party administrator. Results of the recently completed OIG audit over IT Security and Business Continuity and Disaster Recovery at the third-party administrator indicated it complied with HHS IS-Controls requirements for the following groups: information security oversight, information systems monitoring, risk assessment, workforce training, change control, media protection, and business continuity.

OIG Audit assessed the reliability of data used to evaluate access to Parkland's network and its third-party administrator's claims management application by (a) performing electronic and other testing of relevant data elements associated with system access, (b) reviewing information about the data and the system that produced the data, and (c) interviewing responsible Parkland personnel knowledgeable about the data. In addition, OIG Audit traced a random sample of the data to source documents and information from other relevant systems. OIG Audit determined that the data were sufficiently reliable for the purposes of this report.

## Criteria

OIG Audit used the following criteria, which were in effect during the scope of the audit, to evaluate the information provided:

- 1 Tex. Admin. Code, § 202.1, § 202.3, and Subchapter B (2015) and (2016)
- Uniform Managed Care Contract, v. 2.29 (2019) through v. 2.30 (2020)
- HHS Information Security Controls (IS-Controls), v. 1.0 (2018)

## Auditing Standards

Generally Accepted Government Auditing Standards

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

ISACA (formerly known as the Information Systems Audit and Control Association)

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

## Section 3: Controls Tested

Italicized controls were tested solely in OIG Audit's engagement of Parkland's third-party claims administrator.

**Access Control**
- AC-01: Access Control Policy and Procedures
- AC-02: Account Management
- AC-03: Access Enforcement
- AC-06: Least Privilege

**Awareness Training**
- AT-01: Security Awareness and Training Policy and Procedures
- AT-02: Security Awareness Training

**Security Assessment and Authorization Control**
- CA-01: Security Assessment and Authorization Policy and Procedures
- CA-02: Security Assessments

***Configuration Management***
- *CM-01: Configuration Management Policy and Procedures*
- *CM-03: Configuration Change Controls*

***Contingency Planning***
- *CP-01: Contingency Planning Policy and Procedures*
- *CP-02: Contingency Planning*
- *CP-03: Contingency Training*
- *CP-04: Contingency Plan Testing*
- *CP-06: Alternate Storage Site*
- *CP-07: Alternate Processing Site*
- *CP-08: Telecommunications Services*
- *CP-09: Information System Backup*

**Identification and Authorization**
- IA-01: Identification and Authentication Policy and Procedures
- IA-02: Identification and Authentication [Organization Users]
- IA-05: Authenticator Management
- IA-08: Identification and Authentication [Non-organizational Users]

**Incidence Response**
- IR-01: Incident Response Policy and Procedures
- IR-02: Incident Response Training
- IR-03: Incident Response Testing
- IR-04: Incident Handling
- IR-08: Incident Response Plan

***Maintenance***
- *MA-01: System Maintenance Policy and Procedure*

**Media Protection**
- MP-01: Media Protection Policy and Procedures
- MP-06: Media Sanitization
- MP-07: Media Use

***Physical and Environmental Protection Controls***
- *PE-01: Physical and Environmental Protection Policy and Procedures*
- *PE-02: Physical Access Authorization*
- *PE-03: Physical Access Control*

**Planning Controls**
- PL-01: Security Planning Policy and Procedures
- PL-02: System Security Plan

**Information Security Program Plan**
- PM-02: Senior Information Security Officer

**Personnel Security**
- PS-01: Personnel Security Policy and Procedures
- PS-03: Personnel Screening
- PS-04: Personnel Termination
- PS-05: Personnel Transfer
- PS-08: Personnel Sanctions

**Risk Assessment Control**
- RA-01: Risk Assessment Policy and Procedures
- RA-02: Security Categorization
- RA-03: Risk Assessment
- RA-05: Vulnerability Scanning

***Systems and Communication Protection***
- *SC-01: System and Communications Protection Policy and Procedures*
- *SC-08: Transmission Confidential and Integrity*
- *SC-28: Protection of Information at Rest*

***System and Information Integrity***
- *SI-01: System and Information Integrity Policy and Procedures*
- *SI-04: Information System Monitoring*

## Section 4: Report Team

### Report Team

OIG staff members who contributed to this audit report include:

- Audrey O'Neill, CIA, CFE, CGAP, Chief of Audit and Inspections
- Kacy VerColen, CPA, Assistant Deputy Inspector General of Audit and Inspections
- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Daniel Graf, CISA, Audit Project Manager
- Bennie Hookfin, Staff Auditor
- Jay Florian, Staff Auditor
- Erin Powell, Quality Assurance Reviewer
- Ashley Rains, CFE, Senior Audit Operations Analyst

### Report Distribution

Health and Human Services

- Cecile Erwin Young, Executive Commissioner
- Kate Hendrix, Chief of Staff
- Maurice McCreary, Jr., Chief Operating Officer
- Victoria Ford, Chief Policy and Regulatory Officer
- Karen Ray, Chief Counsel
- Michelle Alletto, Chief Program and Services Officer
- Nicole Guerrero, Director of Internal Audit
- Stephanie Stephens, Deputy Executive Commissioner, Medicaid and CHIP Services
- Shannon Kelley, Associate Commissioner for Managed Care, Medicaid and CHIP Services
- Ricardo Blanco, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Thuy Cao, Chief Information Security Officer

Parkland Community Health Plan, Inc.

- John Wendling, Chief Executive Officer
- Andrew Shapiro, Chief Operating Officer
- Patricia Ryan, Senior Director, Information Technology and Reporting
- Nakia Smith, Vice President, Compliance
- Bruce McDaniels, Vice President and Chief Information Security Officer
- Darren Clark, Manager, Systems Engineering
- John Scott, Information Technology Support Manager

## Section 5: OIG Mission, Leadership, and Contact Information

The mission of OIG is to prevent, detect, and deter fraud, waste, and abuse through the audit, investigation, and inspection of federal and state taxpayer dollars used in the provision and delivery of health and human services in Texas. The senior leadership guiding the fulfillment of OIG's mission and statutory responsibility includes:

- Sylvia Hernandez Kauffman, Inspector General
- Susan Biles, Chief of Staff
- Dirk Johnson, Chief Counsel
- Christine Maldonado, Chief of Operations and Workforce Leadership
- Juliet Charron, Chief of Strategy
- Steve Johnson, Chief of Investigations and Reviews

### To Obtain Copies of OIG Reports

- OIG website: ReportTexasFraud.com

### To Report Fraud, Waste, and Abuse in Texas HHS Programs

- Online: https://oig.hhsc.texas.gov/report-fraud
- Phone: 1-800-436-6184

### To Contact OIG

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