



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

Follow-Up Assessment on Previously Issued Audit Recommendations

Security Controls Over Confidential HHS Information at Parkland Community Health Plan, Inc.

AUD-23-019

August 7, 2023

Dear Victoria Mora:

The Texas Health and Human Services (HHS) Office of Inspector General Audit and Inspections Division (OIG Audit) conducted a follow-up assessment of the previously issued audit report titled "Security Controls Over Confidential HHS Information: Parkland Community Health Plan, Inc." to determine the implementation status of audit recommendations previously issued by OIG Audit.

Based on the results of our assessment, OIG Audit determined that Parkland Community Health Plan, Inc. (Parkland) fully implemented all reported audit recommendations. As a result, OIG Audit did not reissue any recommendations from the previous audit. OIG Audit communicated less-significant observations to Parkland in a separate written communication.

OIG Audit thanks management at Parkland for their responsiveness, cooperation, and assistance during this assessment. The attachment to this letter contains additional details on the assessment.

Sincerely,

Kacy J. VerColen, CPA, CIGA
Chief of Audit and Inspections

Attachment

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

Background

The previously issued audit report was published on January 20, 2021. The objectives of the original audit were to assess the design and effectiveness of (a) selected logical security controls over confidential HHS System information stored and processed by Parkland and (b) the business continuity and disaster recovery planning for selected activities related to the delivery of managed care services to Medicaid and Children's Health Insurance Program (CHIP) members enrolled with Parkland.

The scope of the original audit covered the period from September 1, 2019, through August 31, 2020.


Attachment

Pursuant to Standard 9.61 of *Government Audit Standards* issued by the Comptroller General of the United States, certain information related to security configurations and vulnerabilities was omitted from the original 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, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Figure 1 summarizes the implementation status of the recommendation included in the previously issued audit report, "Security Controls Over Confidential HHS Information: Parkland Community Health Plan, Inc.," [AUD-21-006](#), issued January 20, 2021.

A fully implemented recommendation was successfully implemented by Parkland using a process, system, or policy.

Figure 1: Implementation Status of the Audit Recommendation to Parkland

Implementation Status	Recommendation
 Fully Implemented	1 Parkland should ensure access and authentication controls for its network and claims management application are managed in accordance with HHS Information Security Controls (IS-Controls) requirements.

Source: OIG Audit

Through its implementation of the audit recommendation, Parkland more effectively (a) protected confidential HHS information and (b) reduced its risk of noncompliance.

Objective, Scope, Methodology, Criteria, and Standards

Objective and Scope

The objective of this follow-up assessment was to determine the implementation status of OIG Audit's previously issued recommendation to Parkland, which included testing the effectiveness of management activities designed to remediate the identified recommendation.

The scope of the assessment was limited to reviewing the implementation status of the recommendation identified in the previously issued audit report.

Methodology

OIG Audit issued an engagement letter to Parkland on April 19, 2023, providing information about the upcoming assessment, and conducted testing from April 19, 2023, through July 21, 2023.

OIG Audit reviewed the previously issued audit report and performed a follow-up assessment of the reported finding, recommendation, and management response.

Data Reliability

OIG Audit assessed the reliability of Parkland's user account data by reviewing parameters of reports Parkland provided and interviewing relevant Parkland personnel knowledgeable about the systems and data. OIG Audit determined that the data was sufficiently reliable for the purposes of this assessment.

Testing Methodology

To determine the effectiveness of the implemented audit recommendation, OIG Audit:

- Examined user account access to Parkland's internal network and claims management system.
- Determined whether access to Parkland's systems was limited to active users.

- Examined documentation of Parkland’s reviews of user accounts, which Parkland conducted at least annually.
- Reviewed Parkland’s security parameters to determine whether Parkland met password control requirements.

OIG Audit collected information for this assessment through interviews and electronic communications with Parkland management. Auditors assessed the effectiveness of management activities designed to remediate the findings from the original report and conducted testing for the recommendation Parkland management asserted had been fully implemented.

Criteria

OIG Audit used the following criteria to evaluate the information provided:

- HHS Information Security Controls (IS-Controls), v. 1.0 (2018) through v. 1.2.2 (2021)

Auditing Standards

Generally Accepted Government Auditing Standards

OIG Audit conducted the original audit in accordance with generally accepted government auditing standards (GAGAS) and performed the work in accordance with the IT Standards, Guidelines, and Tools as well as the Techniques for Audit and Assurance and Control Professionals published by ISACA (formerly known as the Information Systems Audit and Control Association).

In accordance with GAGAS, providing audit, investigative, and oversight-related services—such as periodic audit recommendation follow-up engagements and reports—does not involve a GAGAS engagement. OIG Audit planned and performed this follow-up assessment to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions included in this report based on the assessment objectives.