Audit Report

Security Controls Over Confidential HHS Information

Driscoll Health Plan

August 15, 2023
OIG Report No. AUD-23-024

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

Driscoll Health Plan

August 15, 2023

Dear Craig Smith:

Driscoll Health Plan (Driscoll) complied with most of the information security requirements tested; however, Driscoll did not comply with certain information security requirements applicable to confidential Texas Health and Human Services (HHS) System information. HHS System information must be managed in accordance with HHS Information Security Controls (IS-Controls) as required by the Uniform Managed Care Contract and the STAR Kids Managed Care Contract.

The attachment to this letter summarizes audit results and details on the objectives, scope, methodology, criteria, and standards. Details of audit results were communicated separately in writing.

The HHS Office of Inspector General Audit and Inspections Division (OIG Audit) made recommendations which, if implemented by Driscoll, will further protect confidential HHS System information.

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

During state fiscal year 2022, which included the period from September 1, 2021, through August 31, 2022, Driscoll provided services to Texas members through the Medicaid STAR program, the Medicaid STAR Kids program, and the Children's Health Insurance Program (CHIP). For these services, Driscoll received capitation payments totaling $1.25 billion.

OIG Audit conducted this audit to determine whether Driscoll had select controls that effectively protected confidential HHS System information.

Attachment

Section 1: Summary of Audit Results and Recommendations

The Texas Health and Human Services (HHS) Office of Inspector General (OIG) Audit and Inspections Division (OIG Audit) reviewed key security controls protecting confidential HHS System information stored and processed by Driscoll Health Plan (Driscoll) and exchanged with other external entities. Driscoll complied with select components of the HHS Information Security Controls (IS-Controls) requirements tested for the following control groups:

- Identification and authentication
- System and communications protection
- Configuration management
- Incident response

HHS IS-Controls defines the control groups and requirements for security control baselines intended to protect confidential HHS System information. 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, OIG Audit applied the moderate HHS IS-Controls requirements for testing on this audit.

HHS IS-Controls requires the managed care organization to (a) disable system access prior to or during the termination process,[1] (b) disable inactive accounts within 90 days,[2] (c) review and confirm ongoing operational need for current

[1] HHS Information Security Controls (IS-Controls), Appendix B, PS-04(a) and Std.1 (Moderate, High), v. 1.1 (Sept. 28, 2020) through v. 1.2.2 (Dec. 20, 2021).

[2] HHS Information Security Controls (IS-Controls), Appendix B, AC-02(03), v. 1.1 (Sept. 28, 2020) through v. 1.2.2 (Dec. 20, 2021).

access authorizations to information systems when individuals transfer to other positions within the organization, (d) initiate a review of required system access immediately upon transfer, (e) modify access authorization as needed to correspond with any changes in operational need due to the transfer,[3] and (f) provide security and awareness training to workforce members with access to its information systems.[4]

Pursuant to Standard 9.61 of *Government Auditing Standards* issued by the Comptroller General of the United States, certain information 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, the omitted information is also exempt from the requirements of the Texas Public Information Act.

The following sections of this report present additional information about the audit results and are considered written education in accordance with Texas Administrative Code.[5] In addition, other audit issues identified in this report may be subject to liquidated damages or OIG administrative enforcement measures,[6] including administrative penalties.[7]

OIG Audit made recommendations to Driscoll which, if implemented, will further protect confidential HHS System information.

[3] HHS Information Security Controls (IS-Controls), Appendix B, PS-05, v. 1.1 (Sept. 28, 2020) through v. 1.2.2 (Dec. 20, 2021).

[4] HHS Information Security Controls (IS-Controls), Appendix B, AT-02(a) and (c), v. 1.1 (Sept. 28, 2020) through v. 1.2.2 (Dec. 20, 2021).

[5] 1 Tex. Admin. Code § 371.1701 (May 1, 2016).

[6] 1 Tex. Admin. Code § 371.1603 (May 20, 2020).

[7] Tex. Hum. Res. Code § 32.039 (Apr. 2, 2015).

Table 1 summarizes the issues and recommendations.

Table 1: Summary of Issues and Recommendations

Description of Issues	Recommendations
Driscoll did not: • Timely disable user accounts, which had access to confidential HHS System information, when access was no longer required. • Manage user access for transferring employees. • Require consultants to complete security and awareness training as required.	Driscoll should verify and demonstrate that it manages user accounts, access requests, and workforce training in accordance with HHS IS-Controls requirements.

Details of these issues were communicated to authorized personnel in a separate report.

Management Response

Action Plan

Driscoll shall update procedures as necessary and more thoroughly document relevant processes associated with user account management. Additionally, Driscoll shall require security and awareness training to be completed by consultants as required by HHS IS Controls.

Responsible Manager

Chief Information Security Officer

Target Implementation Date

December 31, 2023

Section 2: Background

Driscoll:

- Coordinates health services for members[8] in the STAR program, the STAR Kids program, and the Children's Health Insurance Program (CHIP).
- Facilitates Medicaid and CHIP (a) provider claims processing and (b) provider and member benefits administration.

Driscoll supports its Medicaid and CHIP operations through its information technology (IT) infrastructure, including networks, applications, databases, web portals, and call centers supporting members and providers.

When working remotely, Driscoll's workforce accesses the network via a portal application that authenticates the users through Active Directory[9] and a multifactor authentication solution.[10] Once authenticated on the network, authorized users can access the claims management application and other resources through a single sign-on[11] solution.

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

[9] Active Directory is a tool developed by Microsoft that provides centralized management for administrators to manage user permissions.

[10] "Multifactor authentication" is an authentication system that requires more than one distinct authentication factor for successful authentication.

[11] "Single sign-on" is an authentication process that allows a user to access multiple applications with one set of login credentials.

Section 3: Objective, Scope, Methodology, Criteria, and Standards

Objective and Scope

The audit objective was to determine whether Driscoll had select information security controls that effectively protected confidential HHS System information.

The audit scope (a) covered, for the period from September 1, 2021, through August 31, 2022, the Medicaid and CHIP contracts between Driscoll and the Texas Health and Human Services Commission (HHSC) and (b) included a review of Driscoll's internal controls through the end of fieldwork on June 16, 2023, as well as testing of controls that were significant within the context of the audit objectives.[12]

Methodology

OIG Audit reviewed select key information security controls protecting confidential HHS System information in the custody of Driscoll. OIG Audit also reviewed Driscoll's system of internal controls, including components of internal control,[13] within the context of the audit objectives.

Auditors reviewed information technology (IT) security controls and relevant activities supporting data confidentiality at Driscoll by (a) reviewing policies and procedures to gain an understanding of the design of controls and (b) testing the effectiveness of the controls designed to protect information processed and stored by Driscoll.

Data Reliability

OIG Audit assessed the reliability of user account data provided by Driscoll by tracing user information to Driscoll human resources reports and interviewing

[12] For more thorough coverage, OIG Audit expanded the audit scope for testing user access of transferring employees to include September 1, 2021, though October 31, 2022.

[13] For more information on the components of internal control, see the United States Government Accountability Office's *Standards for Internal Control in the Federal Government*, (Sept. 2014), https://www.gao.gov/assets/gao-14-704g.pdf (accessed Apr. 16, 2021).

relevant Driscoll personnel knowledgeable about the systems and data. OIG Audit determined that the data was sufficiently reliable for the purpose of this audit.

Testing Methodology

OIG Audit collected information for this audit through interviews and electronic communications with Driscoll management and staff. Auditors examined key IT security controls and relevant activities supporting data confidentiality at Driscoll by:

- Reviewing policies and procedures to understand the design of controls.
- Conducting Microsoft Teams sessions to interview key personnel and observe security procedures and processes.
- Testing the effectiveness of the controls designed to safeguard information processed and stored by Driscoll.

Sampling Methodology

Auditors collected, reviewed, and analyzed complete populations of user data to perform selected tests. Auditors used risk-based, nonstatistical samples of user populations to perform checks on Driscoll's processes and procedures over access controls and training. These sample designs were chosen to address specific factors identified in the populations. The sample items were generally not representative of the populations for the entities; therefore, it would not be appropriate to project the test results to those populations.

Criteria

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

- 1 Tex. Admin. Code § 202.1, § 202.3, and Subchapter B (2015 through 2021)
- Uniform Managed Care Contract, v. 2.34 (2021) through v. 2.36 (2022)
- STAR Kids Managed Care Contract, v. 1.15 (2021) through v. 1.17 (2022)
- HHS Information Security Controls (IS-Controls), v. 1.1 (2020) through v. 1.2.2 (2021)

Auditing Standards

Generally Accepted Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Section 4: Related Reports

- Security Controls Over Confidential HHS Information: Community Health Choice, AUD-22-015, July 22, 2022
- Security Controls Over Confidential HHS Information: Scott and White Health Plan, AUD-21-017, July 30, 2021
- Security Controls Over Confidential HHS Information: Parkland Community Health Plan, Inc., AUD-21-006, January 20, 2021
- Security Controls Over Confidential HHS Information: Aetna Better Health of Texas, AUD-20-017, August 24, 2020
- Security Controls Over Confidential HHS System Information: El Paso Health, AUD-20-009, April 24, 2020
- Security Controls Over Confidential HHS System Information: Children's Medical Center Health Plan, AUD-20-002, December 20, 2019
- Security Controls Over Confidential HHS System Information and Business Continuity and Disaster Recovery Plans: Texas Children's Health Plan, AUD-19-025, July 31, 2019
- Audit of Security Controls Over Confidential HHS System Information: Amerigroup Texas, Inc., AUD-19-006, November 30, 2018
- Audit of Security Controls Over Confidential HHS System Information: Community First Health Plans, AUD-18-031, August 2, 2018
- Security Controls Over Confidential HHS System Information: MAXIMUS Enrollment Broker, AUD-18-011, February 23, 2018
- Audit of Security Controls Over Confidential HHS Information System: FirstCare Health Plans, AUD-17-017, August 22, 2017

Section 5: Resources for Additional Information

The following resources provide additional information about the topics covered in this report.

For more information on the STAR program:

"STAR Medicaid Managed Care Program," HHS, https://www.hhs.texas.gov/services/health/medicaid-chip/medicaid-chip-members/star-medicaid-managed-care-program (accessed July 19, 2023)

For more information on the STAR Kids program:

"STAR Kids," HHS, https://www.hhs.texas.gov/services/health/medicaid-chip/medicaid-chip-members/star-kids (accessed July 19, 2023)

For more information on CHIP:

"Medicaid & CHIP," HHS, https://www.hhs.texas.gov/services/health/medicaid-chip/medicaid-chip-members/chip (accessed July 19, 2023)

For more information on Driscoll:

Homepage, Driscoll Health Plan, https://driscollhealthplan.com/ (accessed July 19, 2023)

Section 6: Report Team and Distribution

Report Team

OIG staff members who contributed to this audit report include:

- Anton Dutchover, CPA, Deputy Inspector General of Audit and Inspections
- Jennifer Wu, CISA, Audit Project Manager
- John Poynor, Staff Auditor
- Annalisa Adams, Staff Auditor
- Kimberly Howell, Associate Auditor
- James Hicks, CISA, Quality Assurance Reviewer
- Ashley Rains, CPE, 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
- Jordan Dixon, Chief Policy and Regulatory Officer
- Karen Ray, Chief Counsel
- Michelle Alletto, Chief Program and Services Officer
- Nicole Guerrero, Chief Audit Executive
- Emily Zalkovsky, Chief Medicaid and CHIP Services Officer, Medicaid and CHIP Services
- Shannon Kelley, Deputy Executive Commissioner for Managed Care
- Dana L. Collins, Deputy Executive Commissioner for Operations, Medicaid and CHIP Services

- Ricardo Blanco, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Vikram Muralidharan, Chief Information Security Officer

Driscoll Health Plan

- Craig Smith, President and Chief Executive Officer
- Jennifer Brooks, Vice President of Claims Administration

Driscoll Health System

- Justin Box, Chief Information Officer
- Ian Samples, Chief Information Security Officer
- Maurice Afram, Senior Director of Information Systems and Telecom
- Allan Tinana, Senior Director of Audit and Corporate Compliance

Section 7: 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
- Kacy J. VerColen, Chief of Audit and Inspections
- Diane Salisbury, Chief of Data Reviews
- Susan Biles, Chief of Staff, Chief of Policy and Performance
- Erik Cary, Chief Counsel
- Matt Chaplin, Chief of Operations
- Steve Johnson, Chief of Investigations and Utilization Reviews

To Obtain Copies of OIG Reports

- OIG website: ReportTexasFraud.com

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

- Online: https://oig.hhs.texas.gov/report-fraud-waste-or-abuse
- Phone: 1-800-436-6184

To Contact OIG

- Email: oig.generalinquiries@hhs.texas.gov
- Mail: Texas Health and Human Services
  Office of Inspector General
  P.O. Box 85200
  Austin, Texas 78708-5200
- Phone: 512-491-2000