Audit Report

Security Controls Over Confidential HHS Information

Scott and White Health Plan

July 30, 2021
OIG Report No. AUD-21-017

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

Scott and White Health Plan

July 30, 2021

Dear Mr. Ingrum:

Scott and White Health Plan (Scott and White) did not comply with certain information security requirements applicable to confidential Health and Human Services (HHS) System information. However, Scott and White complied with most of the information security requirements tested and established procedures to ensure continuation of the operations necessary to deliver services to Medicaid members in the event of an emergency or disaster.

HHS System information must be managed in accordance with HHS Information Security Controls (IS-Controls) as required by the Uniform Managed Care Contract.

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

OIG Audit made recommendations which, if implemented by Scott and White, will further protect confidential HHS information. Scott and White agreed with the audit recommendations and indicated corrective actions would be implemented.

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 2020, Scott and White provided managed care to an average of 44,456 members through the Medicaid State of Texas Access Reform (STAR) program. During the same period, HHSC made capitation payments totaling $139,804,414 to Scott and White.

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 Scott and White was protected as required and (b) plans were developed and tested, and Scott and White's workforce was trained to support 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 Results and Recommendations

The HHS OIG Audit and Inspections Division (OIG Audit) reviewed key security controls protecting confidential HHS System information stored and processed by Scott and White and exchanged with other external entities. 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, audit work performed by OIG Audit applied the moderate HHS IS-Controls requirements.

Scott and White Health Plan (Scott and White) did not comply with all requirements for managing information security of Health and Human Services (HHS) System information.

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.

Details related to noncompliance were communicated to Scott and White management separately in writing.

OIG Audit made recommendations which, if implemented by Scott and White, will further protect confidential HHS information. Scott and White agreed with the audit recommendations and indicated corrective actions would be implemented.

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

Scott and White coordinates health services for members[1] in the Medicaid State of Texas Access Reform (STAR) program and facilitates Medicaid (a) provider claims processing and (b) provider and member benefits administration. Scott and White supports its Medicaid operations through its IT infrastructure, including networks, applications, databases, web portals, and call centers supporting members and providers.

Scott and White received and exchanged Medicaid 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.

Objective and Scope

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

- Selected information security controls over confidential HHS System information in the custody of Scott and White.

- Business continuity and disaster recovery planning for selected activities related to the delivery of managed care services to Medicaid members enrolled with Scott and White.

The audit scope covered, for September 1, 2019, through January 31, 2021, the Medicaid contracts between Scott and White and the Texas Health and Human Services Commission (HHSC) and included a review of Scott and White's internal controls through the end of fieldwork in June 2021 as well as testing of controls that were significant within the context of the audit objectives.

Methodology

OIG Audit reviewed key information security controls protecting confidential HHS System information in the custody of Scott and White. OIG Audit also reviewed Scott and White's system of internal controls, including components of internal control,[2] within the context of the audit objectives.

OIG Audit examined key IT security controls and relevant activities supporting data confidentiality, integrity, and availability at Scott and White by (a) reviewing

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

[2] 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).

policies and procedures in detail to gain an understanding of the design of controls, (b) conducting fieldwork procedures remotely, including interviews of key personnel and observations of security procedures and processes, and (c) testing the effectiveness of the controls designed to protect or recover information processed and stored by Scott and White.

OIG Audit assessed the reliability of data used to evaluate access to Scott and White'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 Scott and White 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. 2.31 (2020)
- HHS Information Security Controls (IS-Controls), v. 1.0 (2018) through v. 1.1 (2020)

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.

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: 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 J. VerColen, CPA, Deputy Inspector General of Audit and Inspections
- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Daniel Graf, CISA, Audit Project Manager
- Jim Hicks, CISA, Staff Auditor
- Bennie Hookfin, 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
- Emily Zalkovsky, Deputy State Medicaid Director, 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

Scott and White Health Plan

- Jeffrey Ingrum, Senior Vice President, Baylor Scott and White Health, and Chief Executive Officer, Scott and White Health Plan
- Vic Richey, Senior Vice President, Baylor Scott and White Health, and Chief Operating Officer, Scott and White Health Plan
- Barbara Guerin, Interim Chief Information Security Officer, Baylor Scott and White Health
- Rick G Martin, System Director Information Security, Baylor Scott and White Health
- Ovidio Trevino, Director of Infrastructure, Baylor Scott and White Health
- Rob Fort, Director of Health Plan Information System Operations, Scott and White Health Plan
- Amy Cornett, Director of Compliance, Scott and White Health Plans

Section 4: 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.hhs.texas.gov/report-fraud-waste-or-abuse
- Phone: 1-800-436-6184

To Contact OIG

- Email: OIGCommunications@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