Audit Report

Security Controls Over Confidential HHS Information

Aetna Better Health of Texas

August 24, 2020
OIG Report No. AUD-20-017

Inspector General

Texas Health and Human Services

SECURITY CONTROLS OVER CONFIDENTIAL HHS INFORMATION

Aetna Better Health of Texas

August 24, 2020

Dear Ms. Harding:

Overall, Aetna Better Health of Texas (Aetna) 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). Aetna's processes for managing certain accounts with access to confidential HHS System information in its 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, Aetna indicated it will take appropriate actions by December 2020 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

Background

Aetna provides managed care to its members through the Medicaid State of Texas Access Reform (STAR), STAR Kids, and Children's Health Insurance Program (CHIP) programs.

The HHS Office of Inspector General (OIG) Audit and Inspections Division conducted the audit to determine whether (a) confidential HHS System information in the custody of Aetna was protected from unauthorized access, loss, or disclosure and (b) plans were developed and tested and Aetna'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.

Section 1: Summary of Audit Findings and Recommendations

The OIG Audit and Inspections Division reviewed key security controls protecting confidential HHS System information in the custody of Aetna, including its claims management application. Aetna 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 the OIG Audit and Inspections Division applied the moderate HHS IS-Controls requirements.

HHS IS-Controls requires the 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] and disable information system access prior to or during the employee termination process.[3]

Pursuant to Standard 7.61 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, PS-04a, 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
Aetna did not ensure that claims management application user accounts with access to confidential HHS System information were reviewed and disabled when user access was no longer required. Aetna had compensating controls in place that reduced the risk of unauthorized access to the claims management application from outside the Aetna network.	Aetna should ensure access to confidential HHS System information in its claims management application is managed in accordance with HHS IS-Controls requirements.

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

Management Response

Action Plan

Aetna's policy for access management is role-based with controls in place for an annual recertification by user's supervisor. Recertification is required in order to maintain continued access for applications containing confidential HHS system information. Additionally, access to systems is conditional on user not being terminated from Aetna's network.

For Business Continuity and load-balancing reasons, Aetna allows users to have access to systems beyond 90 days of user inactivity. This access is still dependent on employee meeting the criteria mentioned above – role based, active user and access recertified by manager.

Aetna's action plan will be focused on ensuring that recertification process is exhaustive, robust and complete. Specifically, action plan will address – 100% onboarding of active users with system access for annual recertification review.

Responsible Manager

Director, Management Information Systems

Target Implementation Date

December 2020

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

Aetna coordinates health services for members[4] in the Medicaid STAR, STAR Kids, and CHIP programs and supports Medicaid and CHIP (a) provider claims processing and (b) provider and member benefits administration. Aetna supports its Medicaid and CHIP operations through its IT infrastructure, including networks, applications, databases, web portals, and call centers supporting members and providers.

When working remotely, Aetna's workforce accesses the network via a virtual private network (VPN) connection that authenticates the users through a directory service. Once authenticated on the network, authorized users can access the claims management applications through a single sign-on[5] solution. Aetna utilized a two-factor authentication solution for accessing networked applications.

Aetna maintains multiple data centers designed to sustain operations in the event of a disruption to the primary data center. Claims data is backed-up daily for storage at an off-site facility.

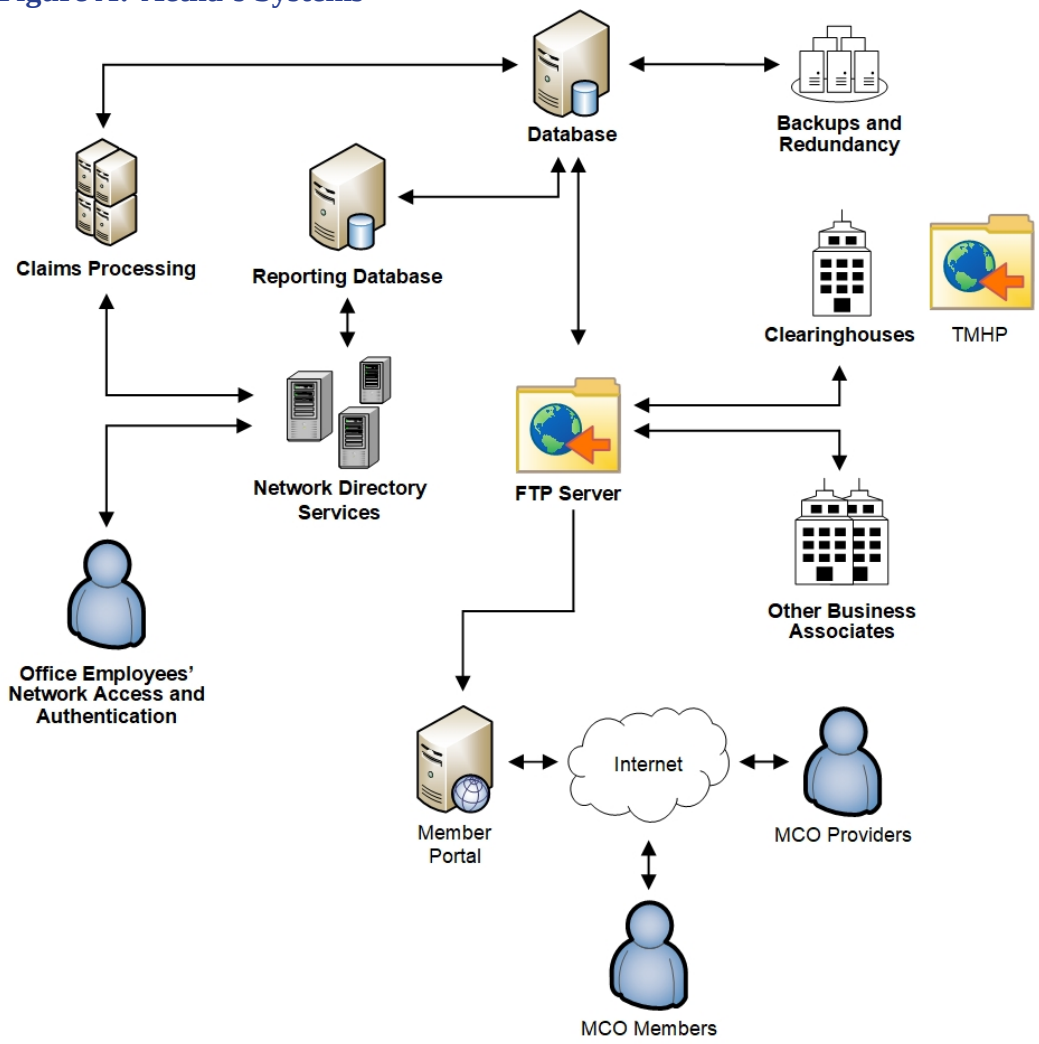
Aetna receives and exchanges Medicaid and CHIP information from and with the Texas Medicaid and Healthcare Partnership (TMHP) through clearinghouses, an explanation of benefits portal, and other third parties using secure file transfers.

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

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

Figure A is an illustration of Aetna's systems and processes. The information systems in bold designate the applications and processes in the scope of the audit, including (a) access to Aetna's network, claims management application, and associated databases, (b) sharing of data with external business associates, and (c) storage and backup activities.

Figure A: Aetna'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 Aetna.

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

The audit scope covered, for September 1, 2018, through February 29, 2020, the Medicaid contracts between Aetna Better Health of Texas 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 Aetna's claims management application and related databases.

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

- Security of data in transit and stored, and media destruction procedures.

- Information systems security policy and workforce security awareness training.

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

Methodology

The OIG Audit and Inspections Division reviewed key security controls protecting confidential HHS System information in the custody of Aetna, 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.

The OIG Audit and Inspections Division examined key IT security controls and relevant activities supporting data confidentiality, integrity, and availability at

Aetna 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 Aetna.

The OIG Audit and Inspections Division assessed the reliability of data used to evaluate access to Aetna'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 Aetna personnel knowledgeable about the data. In addition, the OIG Audit and Inspections Division traced a random sample of the data to source documents and information from other relevant systems. The OIG Audit and Inspections Division determined that the data were sufficiently reliable for the purposes of this report.

Criteria

The OIG Audit and Inspections Division 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. 2.26 (2018) through v. 2.29 (2019)
- HHS Information Security Controls (IS-Controls), v. 1.0 (2018)

Auditing Standards

Generally Accepted Government Auditing Standards

The OIG Audit and Inspections Division 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. The OIG Audit and Inspections Division 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)

The OIG Audit and Inspections Division 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

Access Control
- AC-01: Access Control Policy and Procedures
- AC-02: Account Management
- AC-03: Access Enforcement
- AC-04: Information Flow 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 Control

Contingency Planning
- CP-01: Contingency Planning Policy and Procedures
- CP-02: Contingency Plan
- 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-03: Incident Response Testing
- IR-04: Incident Handling
- IR-08: Incident Response Plan

Maintenance
- MA-01: System Maintenance Policy and Procedures

Media protection
- MP-01: Media Protection Policy and Procedures
- MP-06: Media Sanitization

Physical and Environmental Protection Controls
- PE-01: Physical and Environmental Protection Policy and Procedure
- 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-07: Third-Party Personnel Screening
- 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 Confidentiality 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
- Melissa Larson, CIA, CISA, CFE, Senior Managing Auditor
- Daniel Graf, CISA, Audit Project Manager
- Ashley Malone, CISA, Senior Auditor
- Jay Florian, Staff Auditor
- Julia Youssefnia, CPA, Quality Assurance Reviewer
- Ashley Rains, CFE, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Cecile Erwin Young, Executive Commissioner
- 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, State Medicaid Director, Medicaid and CHIP Services
- Camisha Banks, Interim Director, Managed Care Compliance and Operations, Medicaid and CHIP Services
- Ricardo Blanco, Deputy Executive Commissioner, Information Technology and Chief Information Officer
- Thuy Cao, HHS Chief Information Security Officer

Aetna Better Health of Texas

- Cheryl Harding, Chief Executive Officer
- Brian Wheeler, Chief Operations Officer
- David Hall, Director of Compliance
- Aniket Jain, Director, Management Information Systems

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