MMS Analytics, Inc. DBA TALON

Report on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, and Processing Integrity

SOC 3®

For the Period April 1, 2023 to March 31, 2024

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

Independent Service Auditor's Report

To the Management of MMS Analytics, Inc. DBA TALON:

Scope

We have examined TALON's accompanying assertion titled "Assertion of TALON Management" (assertion) that the controls within TALON's MyMedicalShopper application (system) were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that TALON's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

TALON is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TALON's service commitments and system requirements were achieved. TALON has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TALON is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent of TALON and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve TALON's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve TALON's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within TALON's MyMedicalShopper Application were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that TALON's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

May 15, 2024

Assertion of TALON Management

We are responsible for designing, implementing, operating, and maintaining effective controls within TALON's MyMedicalShopper application (system) throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that TALON's service commitments and system requirements relevant to security, availability, confidentiality, and processing integrity were achieved. Our attached system description of the MyMedicalShopper application identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that TALON's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). TALON's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that TALON's service commitments and system requirements were achieved based on the applicable trust services criteria.

MMS Analytics, Inc. DBA TALON

May 15, 2024

TALON's Description of the Boundaries of Its MyMedicalShopper Application

Description of Services Provided

TALON (the "company") was founded in 2014 and focuses on healthcare price transparency by providing cost-containment tools, services, and strategies to enable a market-driven healthcare system. The MyMedicalShopper Software as a Service (SaaS) application provides medical procedure pricing transparency to end users and healthcare analytics to third-party administrators and employers (as appropriate). MyMedicalShopper is a web and mobile application running in the Amazon Web Services (AWS) infrastructure.

TALON's core products/solutions are built on the TALON MyMedicalShopper application (the "system"). The TALON MyMedicalShopper application is a collection of custom software solutions and services that includes, but is not limited to, the following products/services:

- MyMedicalShopper™
    - MyMedicalRewards™
    - Claims Hindsight™
    - Consumer Interest Calculator™
    - SPARC™ Plan Analysis
    - MyPlanGuide™
    - MyMedicalMetrics™

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which include the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The system is hosted in AWS in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs).

User requests to TALON web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote access is done through a bastion host with a virtual private network (VPN). The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS. AWS Lambda is also used for REST services, portal processing, and PDF processing. Production servers at AWS maintain failover capabilities in the event of physical hardware or logical software failures. The system is also hosted partially in MongoDB. MongoDB is used to host databases in support of the MyMedicalShopper application. The system is encrypted at rest and in transit to backend systems in AWS. This infrastructure is hosted in high-availability data centers with multiple availability zones.

The MyMedicalShopper application is also partially hosted in Meteor Galaxy, which provides automatic load balancing and scaling, distribution of Meteor Galaxy Servers, and application and performance monitoring services to TALON.

Meteor Galaxy is included in TALON's data sub processors listing and reviewed annually for security concerns in accordance with the company's Risk Management Policy and Third-party Management Policy. TALON is responsible for managing the development and operation of the TALON MyMedicalShopper application including infrastructure components such as servers, databases, and storage systems.

Talon is not responsible for hosting any infrastructure on premises that supports the delivery of the MyMedicalShopper application.

People

TALON is organized in the following functional areas:

- **Board of Directors:** Responsible for the oversight of internal controls and includes members independent of control operators.
- **Executive Management:** Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives. Exercises oversight of the development and performance of internal control.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality.
- **Security, Compliance, and Risk Committee:** Responsible for identifying, assessing, and addressing as warranted, issues relating to information security, applicable regulatory and compliance requirements including, but not limited to HIPAA, SOC, and overall risk management.
- **Technical Incident Management:** Responsible for assessing the technical and operational status of the IT infrastructure immediately following an incident, determining the need for countermeasures, reviewing the situation with the management team, and actively mitigating the effects of the incident.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Accounting:** Responsible for maintaining the accounting systems and ensuring their accuracy and timeliness.
- **Information Technology (IT):** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Customer Success:** Responsible for sales, account management, customer success, and customer support activities.
- **HIPAA Security Officer:** Responsible for oversight of TALON's HIPAA compliance program. Also responsible for reviewing, approving (or disapproving) proposed projects, services, or contracts that may require TALON to handle ePHI; and determining whether a proposed project includes business associate activities and, where necessary, implementing a business associate agreement and monitoring compliance with its terms.

Data

Data, as defined by TALON, constitutes any information collected from employees, candidates, users, customers, vendors, or other parties that provide information to TALON.

Information assets are assigned a sensitivity level based on the audience for the information. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Classification Levels	Description	Examples of Data
TALON Protected	Data that contains PHI and ePHI and/or personally identifiable information (PII) concerning any individual.	• PII • ePHI • Financial information
TALON Sensitive	Data that is not classified as TALON protected data, but is information that TALON would not distribute to the general public.	• Financial and budget data • Customer lists • Proprietary technology roadmaps
TALON Public	Data that TALON is comfortable distributing to the general public.	• TALON website • Press releases • Newsletters • Whitepapers

The MyMedicalShopper application processes the information types as described in the table above. To assist with the data handling procedures, TALON has a documented Data Retention Policy that defines the system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policies are reviewed and updated accordingly on at least an annual basis by the security, compliance, and risk committee. Customer data is disposed of per request by customers. For disposal requests, a confirmation is sent back to the customer to notify them that the disposal is complete. Processes for the disposal of data and ePHI are defined within the Data Retention Policy.

Processes and Procedures

TALON has developed and communicated policies and procedures to manage the information security of the system. Policies are reviewed on an annual basis and changes are made to the policies when necessary. Policies are approved by the security, compliance, and risk committee when edited and at least annually. The following policies and procedures are in place:

- Employee handbook
    - Standard of conduct
    - Conflict of interest
    - Confidential information
    - Anti-harassment and anti-discrimination
    - HIPAA training and compliance
    - Information security
    - Acceptable use of company equipment and software
- Asset management
- Background checks
- Backups
- Business continuity and disaster recovery
- Change management
- Cryptography
- Data retention
- Employee termination
- General user access
- Incident response
- Information classification and handling
- Network management
- Password management
- Patching
- Privacy
- Physical security
- Risk assessment and management
- Vendor risk management
- Threat and vulnerability management

Principal Service Commitments and System Requirements

TALON designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that TALON makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that TALON has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the MyMedicalShopper application. Service commitments are set forth in standardized contracts, service-level agreements, and in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of security monitoring to prevent and identify potential security attacks from users outside the boundaries of the system;
- Provide training to employees during onboarding;
- Secure and maintain insurance at all times;
- Engage with customers to address any deficiencies applicable to the TALON solution and provide a mutually agreeable action plan;
- Monthly vulnerability scans on externally facing endpoints and production environment; and,
- Operational procedures for managing security incidents, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality or non-disclosure agreements with employees and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between TALON and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans and periodic testing;
- Redundant connectivity and storage location; and,
- Operational procedures supporting the achievement of availability commitments (99.9% uptime) to user entities.

Processing integrity commitments are standardized and include, but are not limited to, the following:

- Procedures to ensure definition of data processed and product and services specifications are documented and communicated to users of the system; and,
- Policies and procedures are in place to store inputs, data in process, and outputs completely, accurately, and timely.

TALON establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system;
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures; and,
- Business processing rules, standards, and regulations, including:
    - Data security measures as required by the General Data Protection Regulation (GDPR); and,
    - The NIST Cybersecurity Framework.

TALON establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in TALON's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools accessible to all personnel with access to the company systems.

