15301 Dallas Parkway, Suite 960, Addison, TX 75001
MAIN 214 545 3965 | FAX 214 545 3966 | www.bkmsh.com

Service Organization Control (SOC 3) Report

Report on the Artemetrx's Specialty Monitor™ System Relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy

For the Period:

July 1, 2016 through October 31, 2016

BKM SOWAN HORAN
ACCOUNTANTS CONSULTANTS

15301 Dallas Parkway
Suite 960
Addison, Texas 75001
MAIN 214 545 3965
FAX 214 545 3966
www.bkmsh.com

Independent Service Auditors' Report

To the Owners and Management of Artemetrx, LLC

We have examined management's assertion that during the period from July 1, 2016 to October 31, 2016, Artemetrx, LLC ("Artemetrx" or the "Company") maintained effective controls over its Artemetrx's Specialty Monitor™ System to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical);
- the system was available for operation and use to meet the entity's commitments and system requirements;
- information designated as confidential was protected as committed or agreed;
- the system's processing was complete, valid, accurate, timely, and authorized; and
- the system's collection, use, retention, disclosure, and disposal of personal information is in conformity with commitments in Artemetrx's privacy notice set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA,

based on the criteria for the Security, Availability, Confidentiality, Processing Integrity, availability and Privacy principles set forth in the AICPA's Trust Service Principles (TSP) section 100A, *Trust Services Principles, Criteria and Illustrations Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*. This assertion is the responsibility of Artemetrx's management. Our responsibility is to express an opinion of such assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included: (1) obtaining an understanding of Artemetrx's relevant Security, Availability, Confidentiality, Processing Integrity and Privacy controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and go undetected. Furthermore, the projection of any conclusions contained within this report to future periods is subject to the risk that the validity of such conclusions may be weakened as a result of changes made in, or a failure to

make needed changes to, the system or controls utilized, as well as deterioration in the degree of effectiveness of such controls.

In our opinion, Artemetrx's management assertion referred to above is fairly stated, in all material respects, based on the AICPA Trust Services Principles and Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy.

BKM Sowan Horan, LLP

BKM Sowan Horan, LLP
Addison, Texas
December 14, 2016

Management's Assertion

Artemetrx maintained effective controls over the Security, Availability, Confidentiality, Processing Integrity, and Privacy of its Artemetrx's Specialty Monitor™ to provide reasonable assurance that, for the period from July 1, 2016 to October 31, 2016, and based on the AICPA Trust Services Principles and Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy located at www.aicpa.org:

- the system was protected against unauthorized access (both physical and logical);
- the system was available for operation and use to meet the entity's commitments and system requirements;
- information designated as confidential was protected as committed or agreed;
- the system's processing was complete, valid, accurate, timely, and authorized; and
- the system's collection, use, retention, disclosure, and disposal of personal information is in conformity with commitments in Artemetrx's privacy notice set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA.

Our attached system description summarizes those aspects of the system covered by our assertion.

/s/ Drue Pounds Chief Financial and Compliance Officer
Artemetrx, LLC
December 14, 2016

Background

Artemetrx, LLC ("Artemetrx" or the Company) is a subsidiary of Pharmaceutical Strategies Group LLC ("PSG") based in Plano, Texas. Artemetrx is a pharmacy drug management company focused on providing benefits analysis and consulting. Its flagship product, Artemetrx Specialty Monitor™ System ("Specialty Monitor"), provides analytics, benchmarking and cost management solutions to plan sponsors by identifying the high cost specialty drug spending directly from the sponsor's pharmacy and medical claims data.

The Specialty Monitor system is comprised of the following five components:

- Infrastructure (facilities, equipment, and networks);
- Software (systems and applications);
- People (management, software developers, and operators);
- Procedures (automated and manual); and
- Data (transaction streams, files, and databases).

The remainder of this section defines each of the five components listed above.

System Boundaries

As outlined in TSP Section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy, a system is designed, implemented, and operated to achieve specific business objectives (for example, the delivery of services, production of goods) in accordance with management-specific requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above in the five components described below: infrastructure, software, people, procedures and data.

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures and data necessary to provide services relevant to the Specialty Monitor application to the client. The system refers to the system of internal controls as it relates to the scope of the report which is Specialty Monitor. The term "system" is used throughout the report as a reference to the Specialty Monitor application, unless otherwise specified as an actual software application or computer system. System boundaries, pertaining to collection, use, retention, disclosure, and disposal of private, personal, confidential or Personal Healthcare Information (PHI) is governed by contract provisions for particular service engagements.

The boundaries of the system include the creation and configuration of the application environment that directly support the Specialty Monitor product. All infrastructure that supports the services provided to Artemetrx's customers is not included within the boundaries

of the system as it is operated by subservice organizations. For purposes of this report, "customers" or "user entity" refers to any organization using the Specialty Monitor product.

The scope and objective described in the report are specific to the Specialty Monitor. Additional products or services that may be provided by Artemetrx are not addressed within the scope of this report.

Certain Trust Service Principle criteria are not applicable to the system as they are provided by subservice organizations. We obtain SOC 1 (SSAE 16) and SOC 2 Type 2 reports which these controls.

Subservice Organizations

Artemetrx uses subservice organizations to provide data center hosting and management services for the infrastructure as a service (IaaS) environment utilized in Specialty Monitor's system development and production environments. A subservice organization is also used to provide encrypted email if sensitive information is required to be sent through email. Artemetrx periodically reviews the quality of the outsourced operations by various methods including the review of Service Organization Control reports and evaluation of service level agreements (SLAs).

Infrastructure

The key infrastructure for Specialty Monitor is provided by a subservice organization. Artemetrx maintains a contract with Armor Defense, Inc. (Armor) located in Richardson, Texas to provide managed support and virtualized hosting services for an Infrastructure as a Service (IaaS) platform. Artemetrx relies on Armor's formal internal control policies and procedures to manage change requests to these infrastructure components.

Armor's server network is managed up to the application layer of the Open Systems Interconnect (OSI) model. Armor owns manages and administers: all computing and storage, networks, security infrastructure and firewalls devices necessary to manage and administer the operating system virtual machines (VM) provided by their hosting partners.

Developers and technical support professionals use a VPN client to access Specialty Monitor. All login information is secured using 265-bit SSL encryption. Two factor authentication is required to authenticate users through encrypted email or phone. Encrypted email is provided by a subservice organization. Password policies require a minimum length, mixed case and letters/numbers for complexity. Passwords are also required to be changed on first longin and every ninety days.

Armor manages the procurement and security compliance of commercial data centers as part of their value added services. Production databases are backed up timely via an automated system with media being secured offsite at our subservice organization's disaster recovery data center.

Software

Specialty Monitor is an online reporting platform, software-as-a-service (SaaS) that provides analysis of healthcare records pertaining to our client's employee: eligibility, medical and pharmacy claims. Source data is provided by customers through encrypted email or secure file transfer protocol (SFTP) on a one-time or recurring monthly basis. The records are then imported, validated and mapped into standard Artemetrx formats for processing. Once complete, analytical routines are performed and available for reporting.

Specialty Monitor is written using current commercial programming languages and operated on modern technology platforms. The application source code is also version controlled at application and database level. Application webservers maintain RSA SHA-256 V3 Certificate valid from January of 2016 through January of 2019.

People

The following functional groups within Artemetrx are responsible for supporting Specialty Monitor.

- **Executive Management –** This group is responsible for developing and establishing organizational goals, strategic vision, organization direction, client strategy, client acquisition, market positioning, internal control and regulatory compliance, and company growth.
- **Operations –** This group provides divisional leadership and is responsible for all aspects of running the business unit.
- **Product Engineering –** This group designs, implements, tests and delivers software features and service releases.
- **Analytics –** This group provides reporting leadership by identifying, analyzing, and interpreting trends in industry specific data sets.
- **Sales –** This group is responsible for sales and marketing initiatives of the organization.
- **Information Technology & Client Support –** This group is responsible for initial client onboarding, assistance with implementation, usage and technical support.

Procedures

The Company has documented standard operating policies and procedures for the operation of Specialty Monitor that includes:

- System Development Lifecycle ;
- System Change Management ;
- System Security & Security Incident Management;
- Enterprise Risk Assessments (Internal & External) ;
- Data Classification, Privacy and Retention ; and
- Client Onboarding and Implementation.

Control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities, and are part of the process by which Artemetrx strives to achieve its business objectives. Artemetrx has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Change management of Artemetrx's IaaS hosted by Armor requires the submission of a service request ticket. A service request ticket is required to track all infrastructure, network, and administrative security requests. Only authorized Artemetrx employees may open a service request with Armor. Artemetrx is also responsible for reviewing changes to services for completeness and accuracy of all infrastructure changes.

Artemetrx's system development lifecycle (SDLC) policies are applied to all software platforms, infrastructure, networking and operating systems application. It ensures that security is built into our developed applications and supporting infrastructure. Change control is strictly enforced for operational and application code changes.

Data

Customer data is held in accordance with applicable protection and other regulations set out in customer contracts and limits access to electronically held customer data on a need-to-know basis. When the arrangement between a client and our Company ends, the Company returns or destroys all client/client member and proprietary information received during the course of the working relationship/project after maintaining the records for a minimum of six years as required by HIPAA. In most cases, the Company will not retain any copies of the information longer than legally required, unless otherwise noted or agreed to with the client.

Artemetrx has also established data classification in our policies, specifically identifying and classifying confidential, private and non-private data. The Company differentiates between types of client data, and each type is held to the specific standards, policies, and procedures relevant to the given data classification. Customer data is held in SQL databases and is managed by the Information Technology Department. Data in transmission is encrypted by Virtual Private Networks (VPNs) or a RSA SHA-256 V3 certificate. Data-at-rest is encrypted and protected using Vormetric Transparent Encryption software.

Artemetrx's method of data exchange with its customers is accomplished through the Secure File Transfer Protocol (SFTP). SFTP locations and credentials are provided separately to each customer via encrypted/secure message using encrypted email during the onboarding process.

Block-level backups of the Specialty Monitor environment are performed daily and replicated offsite each night. Daily backups are retained for thirty days, weekly backups are retained for three weeks and monthly backups are retained for sixty months. Backup restoration procedures are tested annually to ensure the processing integrity of the backup files and the availability of the records retained. Backups are AES-256 disk safe encrypted at the time of backup.

Artemetrx Privacy Notice

General

This privacy policy outlines how Artemetrx, LLC (Artemetrx), uses and protects client information and data when doing business with Artemetrx. Artemetrx is committed to ensuring that our clients' privacy and data is secure and protected.

Artemetrx complies with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a federal law designed to ensure the privacy of personal and health information. In addition to all federal laws, Artemetrx also complies with all state laws and regulations.

All Artemetrx employees, contractors, and applicable third-party associates are required to read, understand, and abide by this policy.

Security

Artemetrx has implemented a security policy that further ensures that our clients' information and data is secure. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic, and managerial procedures to safeguard and secure the information we collect for business purposes.

Method of Data Collection

Artemetrx collects data from clients, pharmacies, hospitals and various other sources mainly through secure file transfer protocol ("SFTP"), but Artemetrx also is provided information via encrypted, password protected CDs, encrypted USB drives and/or encrypted files via email.

Types of Protected Information

The types of information protected by this policy are: confidential information (CI), such as individually identifiable health information and protected health information ("PHI"), financial information, non-public personal information, and all data exchanged during the course of business to complete the tasks associated with an agreement, consultation, audit, or project.

Additional data and information may include company/client contact names, addresses, email addresses, demographic data, etc. This information may be stored in internal systems, such as sales management applications. These systems permit Artemetrx employees to access and process such data solely for the purposes of customer fulfillment, business administration, business reporting, statistical analysis and marketing of Artemetrx products and services.

Incident Management and Reporting

Employees, contractors, and applicable third-party associates are required to report any suspected breach or policy violation immediately, without unreasonable delay and in no case later than five (5) business days, to their immediate manager. The manager will evaluate the suspected breach or violation and, if validated, will report it to the Chief Financial Officer of Artemetrx. If the breach or violation is validated, the affected client(s) will be notified within a reasonable amount of time. In addition, the notification will include a description of any investigatory steps taken, list of individuals impacted by the incident, the type of information involved in the incident, the date of the potential incident, and the date of discovery.

All incidents, breaches, or violations should be confidentially and immediately reported to:

Pharmaceutical Strategies Group, LLC
5360 Legacy Drive, Building 3, Suite 230
Plano, TX 75024
Attention: Drue Pounds, CCO
(972) 943-7154
DPounds@psgconsults.com

Confidentiality and Non-Disclosure Agreements

Artemetrx executes Confidentiality and/or Nondisclosure Agreement with employees, third parties, contracted individuals, and/or contracted organizations performing services that involve the use or disclosure of CI.

Return/Destruction of Information Procedure

When the arrangement between a client and Artemetrx ends, Artemetrx will return or destroy all client/client member and proprietary information received during the course of the working relationship/project.

In most cases, Artemetrx will not retain any copies of the information, unless otherwise noted or agreed.

If the return or destruction of this information is not feasible, Artemetrx will continue to extend the protections of the BAA and/or NDA and limit further use of such information to those purposes that make the return or destruction of such information infeasible.