artemetrx™
SPECIALTY DRUG SOLUTIONS

PRIVACY POLICY

PSG

PRIVACY POLICY
MAY 2017

GENERAL

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

Artemetrx, LLC 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, LLC also complies with all state laws and regulations.

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

SECURITY

Artemetrx, LLC 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, LLC collects data from clients, pharmacies, hospitals and various other sources mainly through secure file transfer protocol ("SFTP"), but Artemetrx, LLC 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, LLC employees to access and process such data solely for the purposes of customer fulfillment, business administration, business reporting, statistical analysis and marketing of Artemetrx, LLC 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, LLC. 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, LLC 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, LLC ends, Artemetrx, LLC will return or destroy all client/client member and proprietary information received during the course of the working relationship/project. In most cases, Artemetrx, LLC 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, LLC 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.