Patient Privacy & Data Security Compliance Statement
McCreadie Group Software LLC

McCreadie Group Software LLC offers Vestigo®, an investigational drug accountability software solution.

In providing customers with access to and use of Vestigo:

- McCreadie Group is not classified as a Business Associate;
- The company does not perform HIPAA-covered functions on behalf of its customers;
- Information uploaded and processed in Vestigo does not constitute Protected Health Information (PHI).

Clinical research activities conducted by Vestigo users fall outside the scope of standard medical care and treatment services regulated by HIPAA. Other than end-user credentials for Vestigo users, identifiable information created, received, or accessed through the platform is limited to data regarding research subjects who have provided informed consent and have been enrolled in a research study. As such, McCreadie Group's role as the provider of Vestigo does not meet the definition of a Business Associate, and a Business Associate Agreement (BAA) is not applicable. Executing a BAA in this context would impose unnecessary HIPAA compliance obligations on both parties for activities not governed by HIPAA regulations. Furthermore, if the information were considered PHI, customers would face restrictions on its use and disclosure that are incompatible with research purposes. Vestigo does contain Patient Identifiable Information (PII).

While a BAA is not required, McCreadie Group remains committed to data security and maintains physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and availability of all data within Vestigo. We are SOC 2 certified and conduct regular third-party penetration testing, among other ongoing security measures.

We have instituted policies and standard operating procedures to ensure this is done, including, but not limited to, the following:

- All employees have been trained on patient and data privacy rules and procedures and are required to retake this training every year
- All employees are required to sign a confidentiality agreement as a condition of employment
- All policies and procedures related to information and physical security are frequently reviewed to ensure they are up to date and follow any new or revised regulations.
- We have implemented Information Security procedures such as:
    - Automatic expiration of passwords.
    - Account lockouts upon numerous failed login attempts.

- Prohibitions on sending PII and sensitive information content via unsecured channels.
- Mandatory data encryption at rest and in transit.
- Automatic virus scans.
- Secure data backups.
- Any potential or actual breaches are logged, investigated, and reported.

We are committed to keeping all PII (Patient Identifiable Information) and sensitive information secure and to keeping our systems and procedures up to date and in compliance with all related regulations. As the key provider of Investigation Drug Service software, protecting our client's data is of the utmost importance and we have the policies and standard operating procedures in place to ensure that principle is never broken.