ClinCard Program: Data Security & Privacy Statement

Updated 14 March 2017

Confidentiality of Protected Health Information (PHI)

All clinical trial participant information is stored securely. Greenphire does not sell, use or distribute clinical trial participant information for any purpose other than those needed to execute, service and maintain the ClinCard program (including ClinCard Direct Deposit and Travel Reimbursement methods).

Data Information Security

As a matter of policy and commitment to clients and clinical trial participants, Greenphire takes great strides to protect all information relating to cardholders. Greenphire has designed its payments and communication platform including all Greenphire's externally facing web tools to actively protect all data transfers and data stored with Greenphire's infrastructure:

- **Database and Encryption**– All passwords within our database are protected using the one-way PBKDF2 algorithm to encrypt passwords with a SHA256 hash, a password stretching mechanism recommended by NIST. Where necessary, Greenphire's platform makes use of encryption using the 256-bit Advanced Encryption Standard (AES), which is one of the most popular algorithms used in symmetric key cryptography. AES is approved by the US National Intelligence Agency (NSA) for top secret information.

- **Web Tools –** All Greenphire's web tools that are involved in transferring data between an end-user's web browser and Greenphire's platform (and vice versa) are secured by Secured Socket Layer (SSL) with TLS 1.2 encryption. Greenphire is able to track the activities performed on accounts by site administrators through a system of unique logins which allow users access to the clincard.com web tool. In addition, all user activities in the Greenphire Platform are auditable.

- **Financial Data Transfer -** Communications between the Greenphire platform and financial networks are executed via Web Service (API) or sFTP transport.

- **Physical Protection –** Greenphire houses its internal database on servers that are located in a highly secure, off-site facility. Access to the physical servers at the facility is limited to Network Operations Center (NOC) Engineers and Technicians. The facility is secured with a bio-metric security system that can track access to the facility and is monitored by digital security video surveillance, includes multiple suppliers for network connectivity and redundant power supplies including on-site power generation in the event of emergency.

- **Authorized Access –** Greenphire restricts access to sensitive data to only a limited number of essential internal personnel. Authorized individuals are only permitted to access data if it is required to service our client, their authorized users or the clinical trial participant. The number of authorized individuals remains limited to protect against internal threats to the security of sensitive data.

- **Proactive Design** - Greenphire's internal technology platform has been intentionally designed to exclude the requirement of certain sensitive information that other similar companies require to be stored in their systems, such as PIN numbers. If new types of sensitive data must be introduced and stored, per the design of a specific protocol, Greenphire will protect the data using the encryption methods described previously.

- **Customer Service -** Greenphire provides all of its cardholders with 24/7/365 customer service. Customer service is handled by both an automated IVR system and a call center where live customer service representatives may provide financial assistance to cardholders. No information related to the protocol, sponsor, structure of the trial, or medical indication is shared with external cardholder customer service functionality.

- **Quality Control Process** - Greenphire's Quality Control (QC) Department performs system testing in an isolated environment to test and ensure that the software is functioning properly. Each new piece of functionality is thoroughly tested individually. In addition, QC conducts integration and regression testing before new code is approved for movement into production. When a change to the system necessitates a change to the database, the required changes and process to make the changes are documented and tested prior to being performed on production. No code is pushed to production until it has passed QC testing. Data used in QC is test data and does not include data that is, or ever was, production data.

Greenphire US-EU Privacy Shield

Greenphire complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. Greenphire has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.