Data Security & Privacy Statement

Updated 25 October 2017

Confidentiality of Data

All data collected by Greenphire is stored securely and confidentially.

Data Information Security

As a matter of policy and commitment to clients and payees, Greenphire takes great strides to protect all data provided. Greenphire has designed its payments and communication platform including all Greenphire's externally facing web tools to actively protect for 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 through a system of unique logins. 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 a secure Web Service (API) or Secure File Transfer (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.

- **Backup and Recovery –** Greenphire performs backups every 4 hours and the entire database is captured and timestamped encrypted. Disaster Recovery testing is conducted annually.

- **Authorized Access –** Greenphire restricts system access to 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 payees. The number of authorized individuals remains limited to protect against internal threats to the data security.

All employees accessing systems or applications will be issued a unique user id and password to allow access to the system or application. A systematic record of user access is maintained for each application or system user, activity captured include: Active user accounts, last logged In time and date, access control lists, access level or privilege level. At a minimum, review of authorization and access grants are completed each quarter.

- **Network Access** - Access to Greenphire resources over internal and external networks is protected through a combination of network security controls:
  - Authentication mechanisms to prevent and detect unauthorized access.
  - Network segmentation
  - Deployment of firewalls and other security appliances.

  Access to any given resource or network service is only granted to users who are specifically authorized to use that resource or service.

- **Proactive Design** - Greenphire's internal technology platform has been intentionally designed to exclude the collection of personal health information. In addition, we have designed the system to protect personal information provided. For example, ClinCard has been specifically patented to blind sponsor from access to site payee information.

- **Software Quality Assurance Process** - Greenphire's Software Quality Assurance (SQA) 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, SQA 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 SQA testing.

- **Customer Service -** Greenphire provides 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 payees. No information related to the protocol, sponsor, structure of the trial, or medical indication is shared with external payee.

- **Audit Procedures –** To ensure compliance, Greenphire has established internal audit procedures, host/support all client audits, and annually has an external company conduct an SOC I, Type II audit. Audit reports are made available to clients upon request, subject to the client entering into a confidentiality agreement.

Reporting an Incident

Greenphire has established internal standard operating procedures that includes steps to follow if there is a need to report a security incident to the [client / sponsor]. This is incorporated as part of Greenphire's Quality Management System and training is required for all Greenphire employees.

Greenphire US-EU and US-Swiss Privacy Shield

Greenphire complies with the EU-US and US-Swiss 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/.

Data Privacy

Greenphire will comply with the requirements of the EU General Data Protection Regulation (GDPR) as they apply to data processors. Greenphire employs appropriate measures to prevent loss, misuse, unauthorized access, disclosure, alteration, or destruction of personal information in accordance with the GDPR.