## Compliance and Security Overview

Palalinq Social Purpose Corporation (dba WEconnect) recognizes the necessity of secure, responsible custodianship of your data. More than that, we recognize that our relationship with our partners requires us to be compliant with federal privacy laws, such as HIPAA. We take these relationships seriously, and as an illustration of our commitment we have created this statement of compliance to provide an overview of how we protect your privacy.

Federal regulations demand a basic standard of data protection. The following processes have been implemented to meet and exceed these standards:

- Support for encryption for all reports
- No PHI is persisted on employee mobile phone applications
- Restricted access to PHI on a need to know basis (via passwords and company policy)
- Periodic review of passwords for all production accounts; any transition or potential breach requires immediate review and renewal or revocation of privileges.
- Restricted access to all servers and production workstations
- Automated data backups
- Secure data storage in trustworthy data centers
- Automated virus checking
- Email address verification
- Due Diligence, including official Background Checks for all new hires
- Secure password guidelines

In addition, WEconnect has instituted policies to ensure the following:

- We report any unauthorized access, unauthorized behavior, violation of policies or failure to comply with relevant laws or regulations immediately.
- We recognize the right of the Secretary of the United States Department of Health and Human Services to audit our records and practices related to the use and disclosure of PHI to ensure compliance.
- WEconnect employees must sign a confidentiality statement as a term of their employment.
- WEconnect has appointed a Privacy and Compliance Officer, and a Security Officer, who are in charge of developing and instituting policies and practices.
- WEconnect's Privacy and Compliance officer is in charge of training each employee on the appropriate handling and management of ePHI.
- All WEconnect employees receive training on policies and procedures surrounding the protection of PHI, HIPAA requirements, and security protocols.

- WEconnect employees with access to ePHI receive additional personalized role-based training on the appropriate handling and custodianship of ePHI.

## Authorized Access to your Data

Consistent with Federal and State records laws, and with HIPAA, you have the right to request a copy of your data at any time. Your treatment center, if applicable, may request a copy of your data if authorized. We will not share these data with any unauthorized third party.

## Unauthorized Access to your Data

Access to our databases is restricted to those who are required to access it in the lawful course of their duties. WEconnect has strict policies about employee passwords, workstations, and unnecessary access that prohibit behaviors that could put your privacy at risk. Access to your account is restricted to your unique user ID, and requires your password. We perform regular vulnerability assessments to ensure that we are employing the most current protections and the most relevant policies.

## Your Password

Each login session is given and managed by its associated access token, which is generated at the time of login. Once an access token expires, the user must login with their credentials again in order to receive a new access token to access and manage their data. In the event of a password reset, all previous & existing access tokens are invalidated immediately.

Your password is never stored anywhere by us, and so cannot be obtained if our security is compromised. When you set your password, it is encrypted, salted, and stored as hash values as soon as it is created. There is no way for us to retrieve or access them. We do offer a way to reset passwords, which can be found in the login screen of our app.

## Disposal of Data

When your account is deactivated, we provide both you and your treatment center (if applicable) the opportunity to request a copy of any information we may have stored on your behalf. At the expiration of that period, or as the end result of a negative or affirmative response, all identifiable data will be destroyed. We do not retain paper copies of any ePHI beyond that required by law, and then only for the specified period. When records are no longer required or relevant, they are destroyed.

Audit logs for our servers and data are archived indefinitely. All interactions with our data (CRUD: create/read/update/delete) are communicated via our in-house APIs, and every API call is monitored and logged.

V 1.4 November 2017
6/7/2017

## Technical Infrastructure

All of our current technical infrastructure resides within AWS. More specifically, we use Heroku (PaaS) as our platform provider, and Heroku uses AWS (IaaS) for their infrastructure. Because we are using a platform like Heroku, we do not build or maintain our own infrastructure. Heroku's statement on Data Protection and encryption can be found here (https://www.heroku.com/policy/security).

All of our resources are hosted in secure networks, protected by multiple layers of security. AWS has a commitment to HIPAA compliance, and their security policies and protocols are outlined here (https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/). All sensitive data are encrypted both at rest and in transmission.

Any access to these data must go through a dedicated and certified Heroku endpoint, a layer that provides multiple layers of protection such as encryption, authentication, isolation, throttling, logging, load balancing, etc. This layer is also secured by Firewalls, DDoS mitigation, and other protections from spoofing, sniffing and other known vulnerabilities.

We are committed to the responsible use and stewardship of your data. For more information on how we use, store and share your information, please request our aggregated policies or ask us a question by emailing privacy@weconnectrecovery.com.

Our Best,
The WEconnect Privacy and Security Team