

## **PrEP Privacy Policy**

**Last Updated June 4, 2019**

This privacy notice discloses the privacy practices for the prep'd app. This privacy notice applies solely to information collected by prep'd.

### **Information Collection, Use, and Sharing**

We only have access to/collect information that you or your provider enters in the app. This information includes your name, self-reported data to daily check-ins and PrEP readiness questionnaire, messages and documents exchanged between you and your provider, and system activity. Prep'd will use this information to monitor and enhance the user experience and support positive health outcomes. This information is not shared with outside parties.

The prep'd mobile platform requires a password to access and has other security features to protect my information in prep'd. The password is unique for each member and members will only be able to change it by calling a prep'd staff member. Members have access to a documents feature that will allow me to upload images to providers at your participating PrEP clinic. During the image capture process, images will not be stored to the member's phone and will only store within the prep'd app.

Prep'd members, study staff, and provider participants will have access to the community board. The community board content is monitored by study staff.

The user can revoke consent to this information being collected at any time. Your consent does not end unless you cancel it. To revoke consent, the user must contact the prep'd team right away. The prep'd team will still use information about you that was collected before you revoked your consent. When consent is revoked, the user's account will be deactivated.

### **Security**

We take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline.

Wherever we collect sensitive information, that information is encrypted and transmitted securely. All communications/transactions between the prep'd servers and apps are encrypted — not just sensitive information. Specifically, the data is transmitted with HTTPS/SSL TLSv1.1, TLSv1.2

While we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, your PrEP navigator or study staff) are granted access to personally identifiable information. The servers in which we store personally identifiable information are kept in a secure environment. Physical access to these servers are prohibited and the data is stored on encrypted hard drives with AWS KMS.