**Privacy statement**

**About Us**

The App has been co-designed by the HIV community and UK university researchers.

We aim to:

1. Develop and evaluate new tools that empower people to use their personal data for self-managing HIV, in order to live and age well;

2. Understand what it means to share this personal data with others, including people living with HIV and health care professionals;

3. Identify ethical issues associated with Trust, Identity, Privacy and Security related to sharing information and managing stigma and well-being. This will help to develop responsible processes for conducting technology research and developing applications.

Whilst our work plan focuses on people living with HIV, it ensures that insights from the research can be of value for understanding barriers to sharing personal information when living with other potentially stigmatised long-term conditions, such as mental health conditions.

For more information about the INTUIT project or to get in touch with the team, please contact us by email: [info@intuitproject.org](mailto:info@intuitproject.org" \t "_blank).

**Consent and data collection**

**Our approach**

The App enables you to track personal data and the My Journey functionality helps you reflect on the data you have collected and spot patterns. When you use these features of the App none of your personal data leaves your phone and none of it is visible to anybody else. The app also provides an optional Community forum where you can ask questions and have discussions with other people living with HIV. In order to use this forum we have to securely store in the cloud the data that you share on the forum with your peers, such as posts and questions. We refer to these as ‘community data’. We will only do this if you give your consent. We also ask for your consent to collect anonymous data about how you use the App, known as ‘analytics data’, in order to improve user experience.

If you consent to us collecting either analytics data or to store community data then we will only process these data in ways that you would reasonably expect:

a. anonymous analytics data will be processed to investigate how different users use the App in order to help us improve its design.

b. community posts and other data will not be analysed and only stored in the cloud in order to facilitate community data sharing

We do not mislead or deceive people when we collect these personal data.

We are open and honest and comply with the transparency obligations of App users’ right to be informed about which personal data we collect if users give their consent.

**How it works**

When the App is initially downloaded it uses three default privacy settings that are designed to protect the privacy of your personal data. You can choose to relax some of the default settings and share some of your personal data.

Before using the App, you will be asked if you give consent for:

a. Data about how you use the app being stored and processed in the cloud using Amplitude services

b. Community content to be stored in the cloud using SendBird service. You can use the app to track and annotate personal data without giving consent for either option (a) or (b).

**Your data rights**

At any point you can update your consent options (see our approach). If consent for the storage of community data is not given or withdrawn then you will not be able to use the community functionality. Consent settings can be found in the Profile section of the application.

A full account of your data rights can be found here

LEARN MORE button

**Learn more**

**1. Right of Access**

You have the right to access any personal data which we collect with your consent. You can contact us via email [myData@intuitproject.org](mailto:myData@intuitproject.org) or verbally via telephone (the phone number can be found in the in-app privacy statement) and ask for all the personal data that we have collected.

We will email all of the collected information within one month of receiving the request, but aim to do it without undue delay. We will not charge a fee for providing this information.

**2. Right of Rectification**

You have the right to ask for any inaccurate personal data to be rectified. Data is inaccurate if it is incorrect or misleading as to any matter of fact. You can contact the research team via email [myData@intuitproject.org](mailto:myData@intuitproject.org) or by telephone (the phone number can be found in the in-app privacy statement).

**3. Right of Erasure**

You can delete any personal data that has been collected by the App:

a. Analytics data on how you use the App;

b. Posts and other community content.

These personal data can be erased in the Profile section of the App. Alternatively, you can contact us via the App, via email myData@intuitproject.org or verbally via telephone (the phone number can be found in the in-app privacy statement) and ask for the analytics data or community content to be erased. Once erased these data cannot be restored.

**4. Right of Portability**

You have the right to request a copy of all the personal data we have collected with your consent. You can contact us via email myData@intuitproject.org or verbally via telephone (the phone number can be found in the in-app privacy statement) and ask for a copy of all the personal data that we have collected with your consent.

More information from the Information Commissioners Office (ICO) about your right to be informed as a data subject can be found at this link: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>.

**How your data is stored**

All of your tracked personal data is only stored on your mobile device. We store only the minimum amount of other data required for the App to work properly outside of this.

A full list of the stored data items can be found here:

LEARN MORE button

**Learn more**

**What is stored**

**Username**

The name you use to sign up for the application. You will be provided with a Study Email that we would like you to use as the username. If you do not use this email then password recovery options will be limited which prevents the personal data you have tracked and the data you have shared on the Community forum from being available if you lose your password.

Storage location: Firebase authentication

**Password**

The password you use to sign up/log in to the application. To increase the security of your account, ensure the password is strong. The application will provide guidelines to ensure a strong password: A length greater than eight characters, at least one symbol, at least one upper case character, at least one number, the password is not used for other services.

Firebase does not store the password itself but stores a salted hash of the password. If Firebase had a data breach the usernames and passwords would be protected.

Storage location: Firebase authentication.

**Database of tracked personal data, including the diary**

The categories people are tracking. e.g. Mood, Sleep, if Medication has been taken, and the associated data that is recorded using the App.

Storage location: Mobile device persistent storage.

**Confirmed HIV status**

Whether the user has been verified by an authorised third party. This will be stored when the status authorisation is implemented. It’s not intended to build this for the evaluation.

Storage location: Mobile device persistent storage.

**Data sharing nickname and profile picture**

The name you select which is how you appear to the other members when using the P2P functionality.

Storage location: SendBird,

**Data sharing posts, tips and comments**

Encrypted questions asked by users regarding their PHI. Also associated tracker data if they choose to attach it to posts and tips

Storage location: SendBird

**Post likes and communities followed**

Users’ Firebase ID, which is also used for Sendbird

Storage location: Firebase

**Direct messages to peers**

Encrypted private communications between users regarding their personal data.

Storage location: SendBird

**App usage data (for data analytics)**

We track how people use the App e.g. which features they use, in order to improve the App design.

Storage location: Amplitude.

**Why is it stored**

**Username**

The sername must be stored for the user to have an account that enables them to track data and interact with peers.

**Password**

The password is stored to authenticate the user when logging in to the application.

**Database of tracked personal data, including the diary**

So that the user has a record of the personal data they have tracked.

**Confirmed HIV status**

To access the P2P data sharing this needs to be checked.

**Data sharing nickname and profile picture**

Such that the user can save their nickname when communicating in the P2P sharing component.

**Data sharing posts, tips and comments**

These need to be stored so that users can view and respond to them. There should also be a record of these so that if people have similar questions in the future, they can search to find existing answers.

**Direct messages to peers**

A user should be able to retrieve their chat history with a given user.

**How data is stored/Who can access it**

**Username**

This is visible to the application maintenance team from the Firebase console. Stored alongside it is the user’s randomly generated unique identifier.

**Password**

The application maintenance team cannot access this as it is encrypted using keys the team does not have access to. Only the user knows their own password.

**Database of tracked personal data, including the diary**

This is stored within the user’s persistent storage on their phone. For an adversary to access this information, they would need to unlock and gain access to the phone.

**Confirmed HIV status**

If a user is on the Peer-to-Peer (P2P) sharing component, their status is confirmed. This means that the other P2P users will know their confirmed status. The application maintenance team would not be able to associate this information with the user’s identity if implemented and may not have access to it at all.

**App usage data (for data analytics)**

We track how people use the App e.g. which features they use, in order to improve the design.

**Security**

**Accessing the App**

**Tracking features**

Access to the application requires an account which can be created through the sign up page. To sign up you must provide a username and password. You must create a new email address which does not include any personally identifiable information to improve your privacy. Once you have signed up, you can log in. The application ensures that the password is suitable with a minimum length requirement. Your email and password are stored securely in Firebase.

**Where your data is stored**

**Me and My Journey data**

All data collected in the Me and My Journey sections are encrypted and stored locally on your mobile phone.

**Community data**

Data shared in the community section of the app is stored by the Firebase and SendBird cloud services, whose security implementations are explained on the next slides.

**Cloud services**

**Google cloud functions**

All communications between the app and cloud services is done with a secure communication method via google cloud functions, ensuring your personal data is protected whilst data is in transit.

**Firebase**

What is stored:

Email, encrypted password, community metadata such as URLs of posts made, liked and commented on, user ID.

How it’s stored:

All data is encrypted.

**SendBird**

What is stored:

User nickname, comments, posts, direct messages, user ID.

How it’s stored:

All data is encrypted.

**Amplitude**

What is stored:

User ID, usage data, accompanying user data determined by user;

How it’s stored:

All data is encrypted.