EINS

Data User Stories

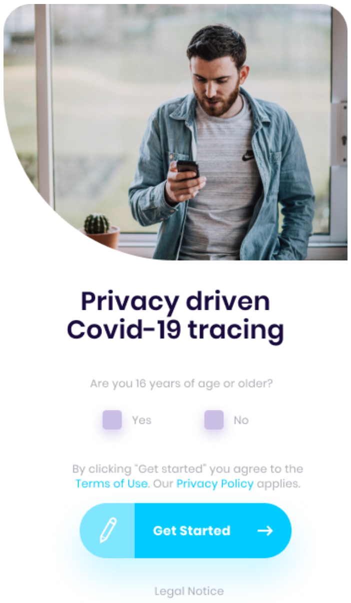
April 20th 2020

Data User Stories

https://www.lucidchart.com/documents/edit/5cdb9be6-d5ed-4ebf-8673-7c6ebe55cbfe/0_0

Registration Process

1. A user downloads the app.
2. The user is required to confirm if they are older/younger than 16 years of age. If a user is younger than 16 years old then they are required to confirm that their legal guardian has provided consent to use the app.

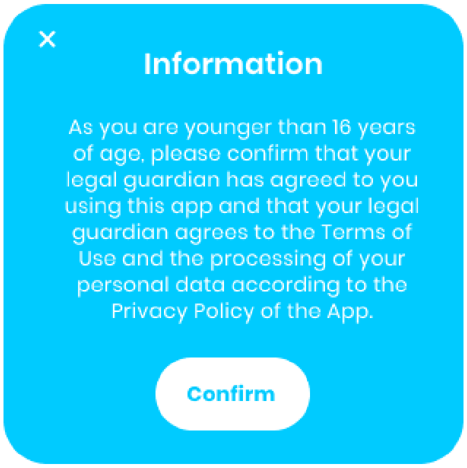


Privacy driven Covid-19 tracing

Are you 16 years of age or older?

□ Yes □ No

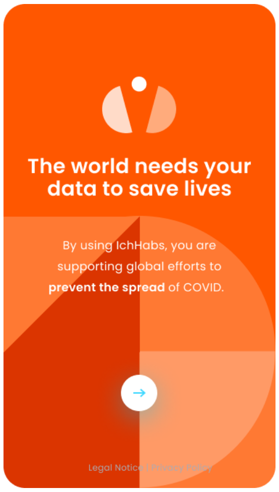
By clicking "Get started" you agree to the Terms of Use. Our Privacy Policy applies.



Information

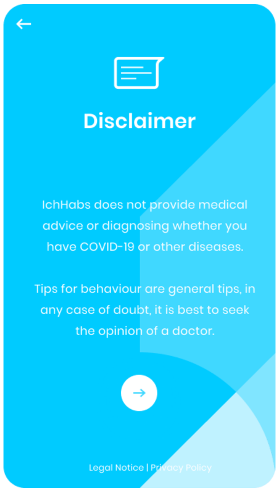
As you are younger than 16 years of age, please confirm that your legal guardian has agreed to you using this app and that your legal guardian agrees to the Terms of Use and the processing of your personal data according to the Privacy Policy of the App.

3. The user completes the following onboarding screens.



The world needs your data to save lives

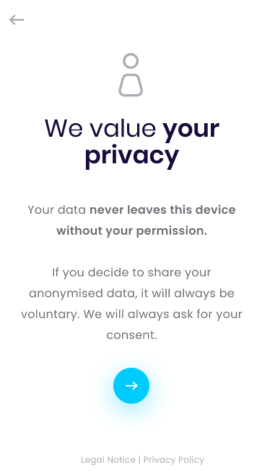
By using IchHabs, you are supporting global efforts to **prevent the spread** of COVID.



Disclaimer

IchHabs does not provide medical advice or diagnosing whether you have COVID-19 or other diseases.

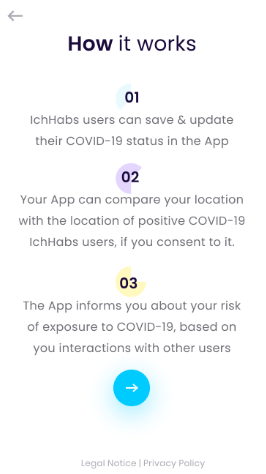
Tips for behaviour are general tips, in any case of doubt, it is best to seek the opinion of a doctor.



We value **your privacy**

Your data **never leaves this device without your permission.**

If you decide to share your anonymised data, it will always be voluntary. We will always ask for your consent.



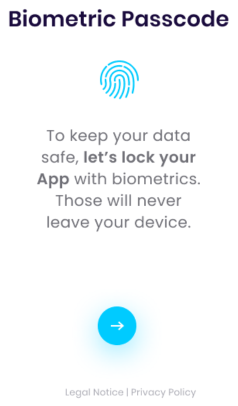
How it works

01 IchHabs users can save & update their COVID-19 status in the App

02 Your App can compare your location with the location of positive COVID-19 IchHabs users, if you consent to it.

03 The App informs you about your risk of exposure to COVID-19, based on you interactions with other users

4. The user locks the app with their biometrics or device password.



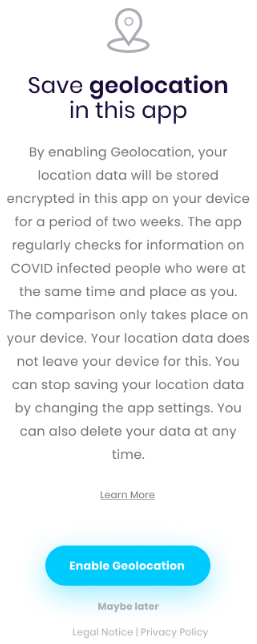
Biometric Passcode

To keep your data safe, **let's lock your App** with biometrics. Those will never leave your device.

→

Legal Notice | Privacy Policy

5. The app connects to the VIA servers:
   a. End-to-end asymmetric encryption is achieved.
   b. The app stores hashed AppID on the server.
6. If the user agrees to have their future locations stored in the app:
   a. Get the user to allow app tracking via prompt.
   b. The app takes a sample of geolocation points at n-minute intervals and adds this to a list of location-date time points in the local device storage via encryption.



Save **geolocation** in this app

By enabling Geolocation, your location data will be stored encrypted in this app on your device for a period of two weeks. The app regularly checks for information on COVID infected people who were at the same time and place as you. The comparison only takes place on your device. Your location data does not leave your device for this. You can stop saving your location data by changing the app settings. You can also delete your data at any time.

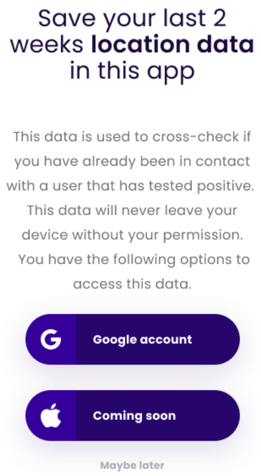
Learn More

Enable Geolocation

Maybe later

Legal Notice | Privacy Policy

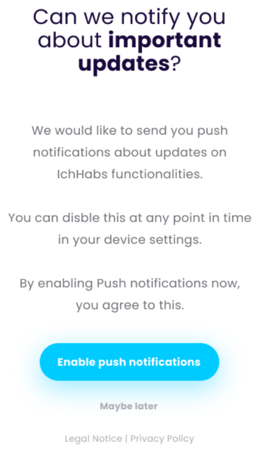
7. If the user agrees to download past geolocation data into the app:
    a. The user selects either Apple (note: Apple will not be available with first release) or Google account.
    b. The user authenticates into their Google or Apple account via the app
    c. The user is prompted to download location data to their cloud drive from Google or Apple.
    d. The user is prompted to access cloud drive.
    e. The app fetches 2 weeks of data from the user's cloud drive.
    f. The app deletes the data from the user's cloud drive.
    g. The app then terminates the connection to the account and cloud drive then discards the access tokens.
    h. The app takes the location history data and thins it by taking N-minute samples of geolocation.
    i. The app discards the original location data download.
    j. The app saves the list of DateTime-Location points into encrypted local device storage.



Save your last 2 weeks **location data** in this app

This data is used to cross-check if you have already been in contact with a user that has tested positive. This data will never leave your device without your permission. You have the following options to access this data.

8. Users are asked to enable push notifications. If agreed:
    a. The app requests push token from the apple or android servers.
    b. The app receives the push token.
    c. The app sends the push token, along with hashed AppID, to the server for storage.



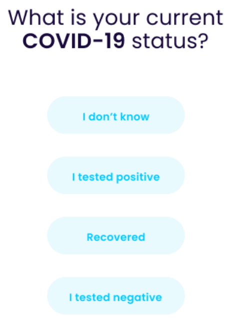
Can we notify you about **important updates**?

We would like to send you push notifications about updates on IchHabs functionalities.

You can disble this at any point in time in your device settings.

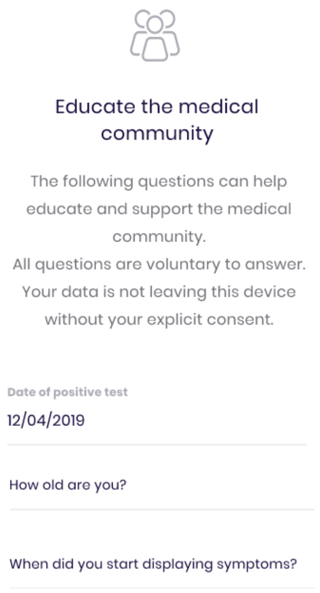
By enabling Push notifications now, you agree to this.

9. The user enters their COVID-19 status and subsequent questions.
    a. The app stores the answers into an encrypted local device.



What is your current **COVID-19** status?

10. The user enters basic survey data based on the status answer.



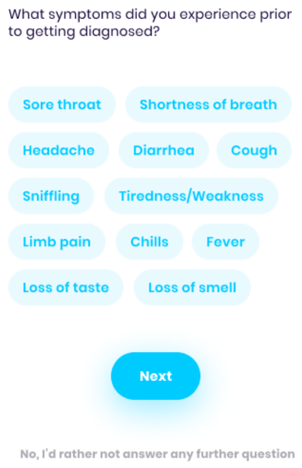
Educate the medical community

The following questions can help educate and support the medical community.
All questions are voluntary to answer.
Your data is not leaving this device without your explicit consent.

Date of positive test
12/04/2019

How old are you?

When did you start displaying symptoms?

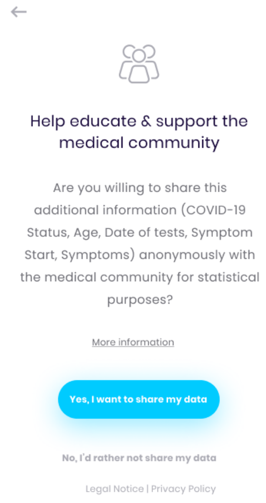


What symptoms did you experience prior to getting diagnosed?

11. Users are then asked if they are happy to donate and share the survey data anonymously. If agreed:

  a. User age is masked by adding a random factor of +-2 years to the date. This anonymizes the data, without statistically damaging the set.

  b. The data is uploaded along with the hashed AppID (ensures no double submissions).



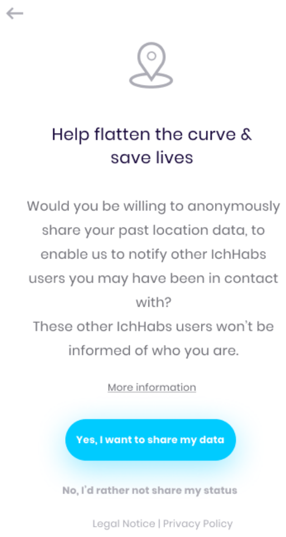
Help educate & support the medical community

Are you willing to share this additional information (COVID-19 Status, Age, Date of tests, Symptom Start, Symptoms) anonymously with the medical community for statistical purposes?

More information
Yes, I want to share my data
No, I'd rather not share my data
Legal Notice | Privacy Policy

User Updates COVID-19 Status

1. The user updates their COVID-19 status.

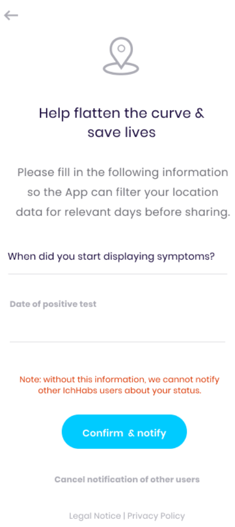


Help flatten the curve & save lives

Would you be willing to anonymously share your past location data, to enable us to notify other IchHabs users you may have been in contact with?
These other IchHabs users won't be informed of who you are.

More information
Yes, I want to share my data
No, I'd rather not share my status
Legal Notice | Privacy Policy

2. If the user tests positive, he/she is asked to share their Location-DateTime history.
3. If the user agrees, he/she is then asked for the date of symptom start and date of the positive test result
    a. The app crops the Location-DateTime history to 2 weeks (note: this will be refined later on in the development process).
    b. The app uploads the data to the server along with the hashed AppId.
    c. The hashed AppID is stored in a submission table to prevent abuse and multi submission protection.
    d. The submission for the dataset is stored separately and anonymously.



Help flatten the curve & save lives

Please fill in the following information so the App can filter your location data for relevant days before sharing.

When did you start displaying symptoms?

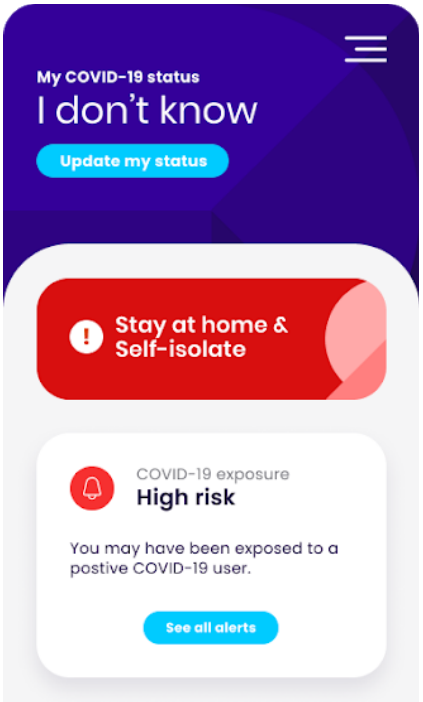
Date of positive test

Note: without this information, we cannot notify other IchHabs users about your status.

Confirm & notify
Cancel notification of other users
Legal Notice | Privacy Policy

User Tests Path for COVID-19 Contact

1. A check is carried out on 3 events:
   a. The user opens the app.
   b. The app is set to check daily.
   c. App receives a push notification.
2. App prepares geolocation parameters to request relevant data set:
   a. App checks geolocation data for maximum and minimum latitude and longitude of their locally stored geolocation data points.
   b. The app adds some randomized buffers/padding to the boundaries which mask the identity, reducing correlation capabilities further.
3. App submits bounds to the server when downloading heatmap chunk.
4. App receives the heatmap data in question.
5. The app runs a local matching process to determine contact with risk areas and people.
6. The app reports any contact to the app user, via the UI/UX for warning and suggestion.
7. The app discards the local heatmap data.



My COVID-19 status

I don't know

Stay at home & Self-isolate

COVID-19 exposure

High risk

You may have been exposed to a postive COVID-19 user.

Geolocation and Statistics Server

The EINS server's main task is to securely store the geolocation-timestamp points of donated and shared data from patients who tested positive for the virus. The geolocation server needs the ability to store, as well as quickly access a point cloud of the geolocation-timestamp heat map. This data does NOT have any links between the data points (therefore no paths, just points). There are various ways in which EINS can anonymise this data in the future, using 'gaussian blur functions' to add noise. This is so that there is less chance of de-anonymising the data.

Registration Process

1. The server receives the AppID of a newly installed app on a new device.
2. If agreed to by the app user, the server stores the push token of each app install with the AppID.
3. If the user agrees to submit their survey data, the server accepts the survey data along with the AppID.
    a. The AppID is hashed and checked against a list of hashed IDs saved. If the hash is already present, then the submission is discarded as a duplicate or a malicious submission.

b. If the AppID was not found, the survey data is saved and the AppID is added to the list and then discarded. The AppID is not saved alongside the survey response.

User Updates COVID-19 Status

1. If a user that tests positive agrees to share the data, their app sends the server a set of geolocation-timestamp points:
2. The server must insert the data points into the mapping, not preserving the consecutive nature (not a path, just dots with location and time).

User Tests Path for COVID-19 Contact

1. When the server gets a request to allow a user to get part of the heatmap to do local collision/risk checking.
2. The server accepts the latitude and longitude bounds (which contain randomization from the user to obscure/anonymize the data further), fetches the heatmap points between those areas and returns that to the user.