Flo Anonymous Mode overview

Protecting reproductive health data

September 2022

Table of contents

Protecting reproductive health data post-Roe

The needs of our global community of users are the driving force behind the Flo app. We understand that when you use our product, you expect your personal information to be private and secure. That's why when the US Supreme Court overturned Roe v. Wade, which had previously guaranteed a constitutional right to abortion in the United States, we used our technology to develop and offer a new feature: Anonymous Mode.

Multiple studies establish that women and people who menstruate who are denied abortions suffer significantly adverse health outcomes. Banning abortion increases the number of unsafe abortions and cases of maternal death and leads to a sixfold increase in the chance of developing a life-threatening condition. That's why Flo is aligned with the World Health Organization: Being able to obtain a safe abortion is a crucial aspect of health care.

At the same time, evidence-based information on effective contraceptive methods and reproductive health plays a big role in preventing the need for an abortion and countering the growing volume of online misinformation. This is why Flo supports female health literacy by giving our global, 257-million-strong community access to medically credible information to make informed decisions about their health.

Every day, all over the world, millions of women and people who menstruate trust Flo with their most personal information. We believe that now more than ever, everyone deserves to access, track, and gain insight into their personal health information without having to worry about privacy or medical misinformation.

Flo will always stand up for the health of women and people who menstruate, and we will do everything in our power to protect the data and privacy of our users. Flo encrypts all data, engages in independent privacy audits, and recently received ISO 27001 certification, making Flo the first period and ovulation tracker to achieve this milestone. Together with our robust privacy and security best practices, Flo's Anonymous Mode is a significant step in protecting the privacy of reproductive health data, allowing our users to access medically credible information without anxiety or concern.

The Flo team

Introduction to Flo Anonymous Mode

Flo’s Anonymous Mode introduces an even deeper layer of privacy for reproductive health data.

The new feature is based on decoupling health data from personal information and creating a new Anonymous Mode account that does not contain any unique user identifiers, such as email address and Google/Apple account ID; payment identifiers; or technical identifiers, such as IP address, ID for advertisers (IDFA), or other IDs. The data that is transferred from “ancestor” (original) accounts includes health data (such as logged cycle dates and symptoms), reminders, and the user’s aim for using Flo.

This new approach allows Flo to keep the benefits of client–server architecture, such as providing more accurate cycle and symptom predictions, insight personalization, and chatbots on all devices, while ensuring that the data stays private throughout its lifecycle.

To introduce a deeper layer of protection, Flo has partnered with Cloudflare to implement an Oblivious HTTP standard, which ensures, that no single party processing user data in Anonymous Mode has complete information on both who the user is and what they are trying to access.

The Anonymous Mode feature is localized into 20 languages and can be enabled via the app’s settings in iOS and Android (to be released in October 2022).

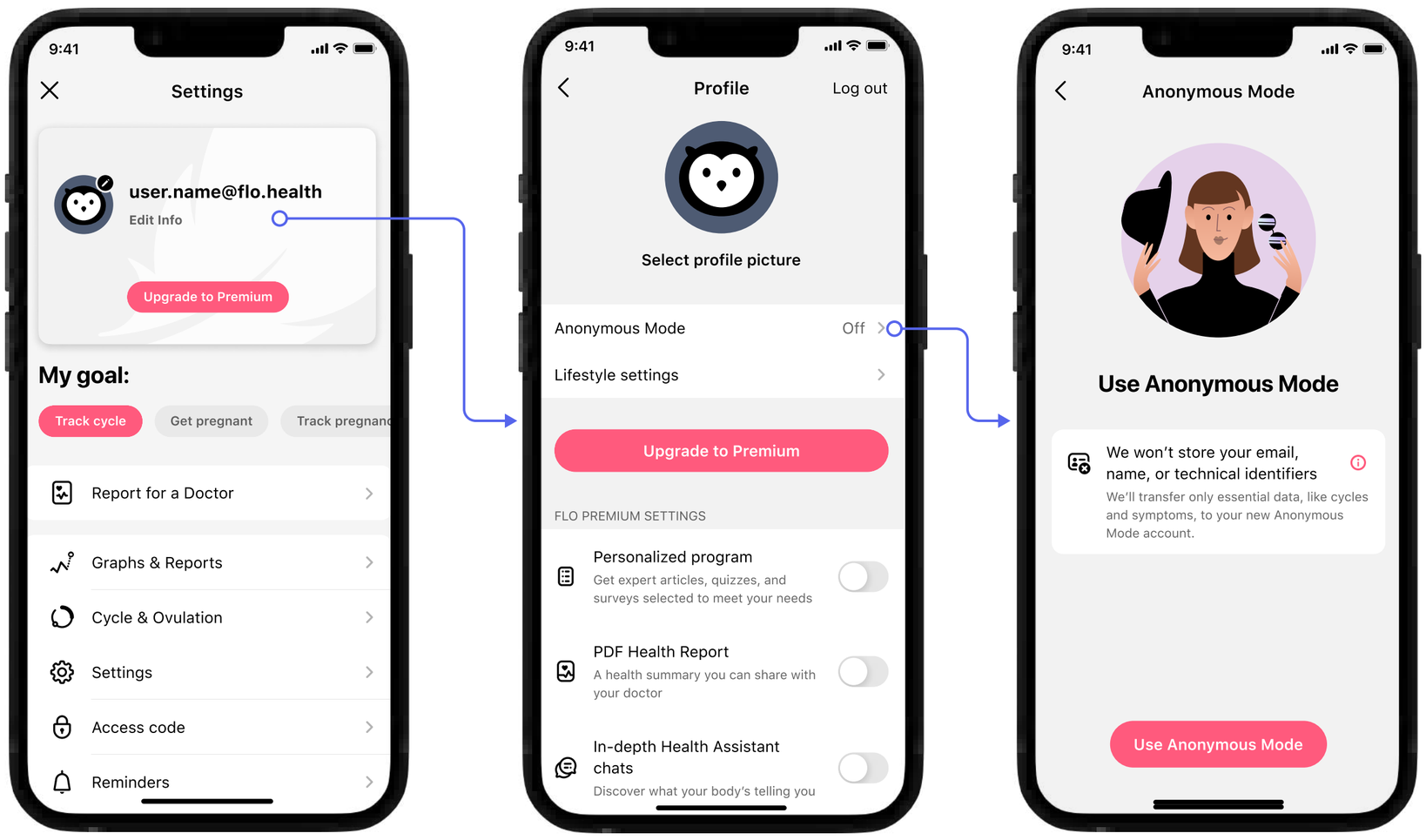
Using Flo Anonymous Mode

Enabling Anonymous Mode

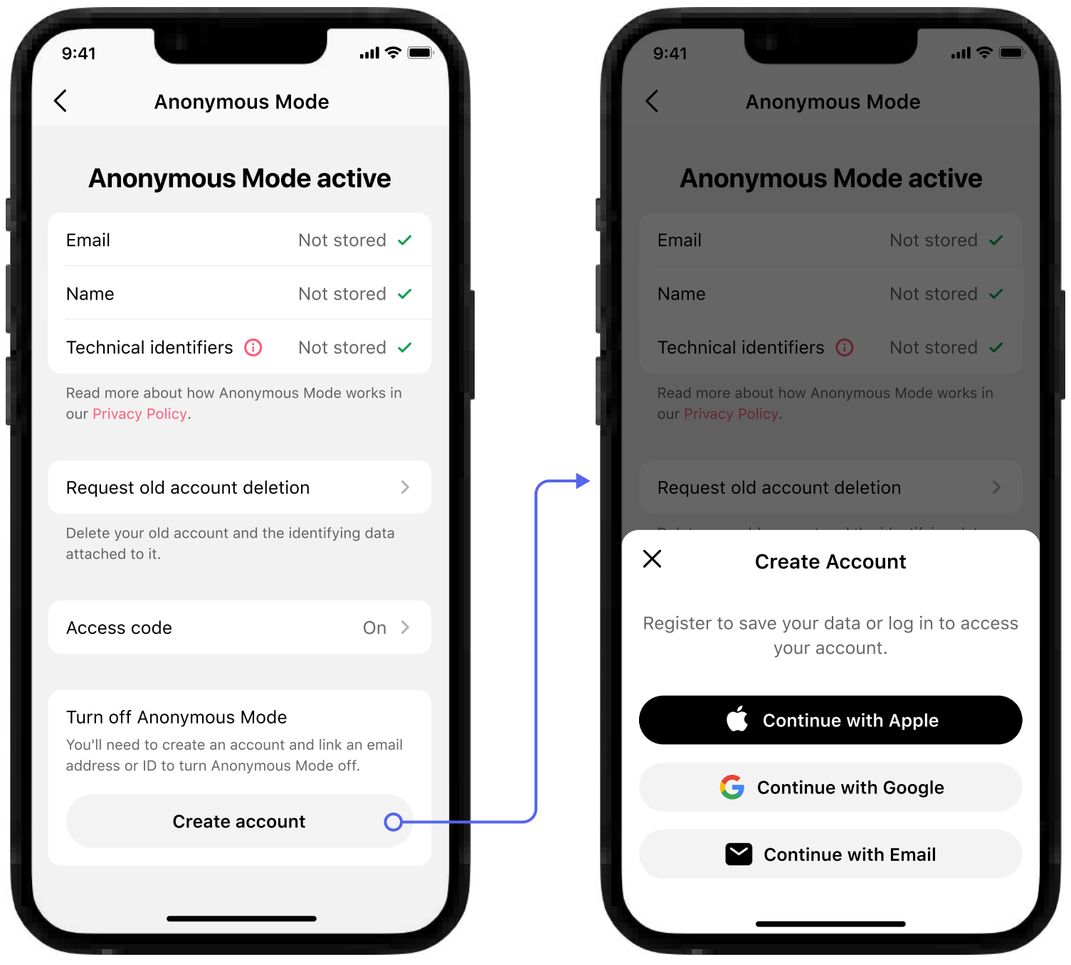
Switching to Anonymous Mode is optional. Flo provides a user interface for switching from an ancestor account to an Anonymous Mode account, instructions, a “how to,” and a link to chat with a Support team member. Anonymous Mode can be disabled at any time if a user decides they no longer need the additional layer of data protection or need some features that are unavailable in Anonymous Mode, such as transferring their Flo data to a new device.

As illustrated below, current users can create an Anonymous Mode account by going to Settings > Profile picture > Anonymous Mode.

New users need to install the Flo app > Set up an account > Settings > Profile picture > Anonymous Mode.



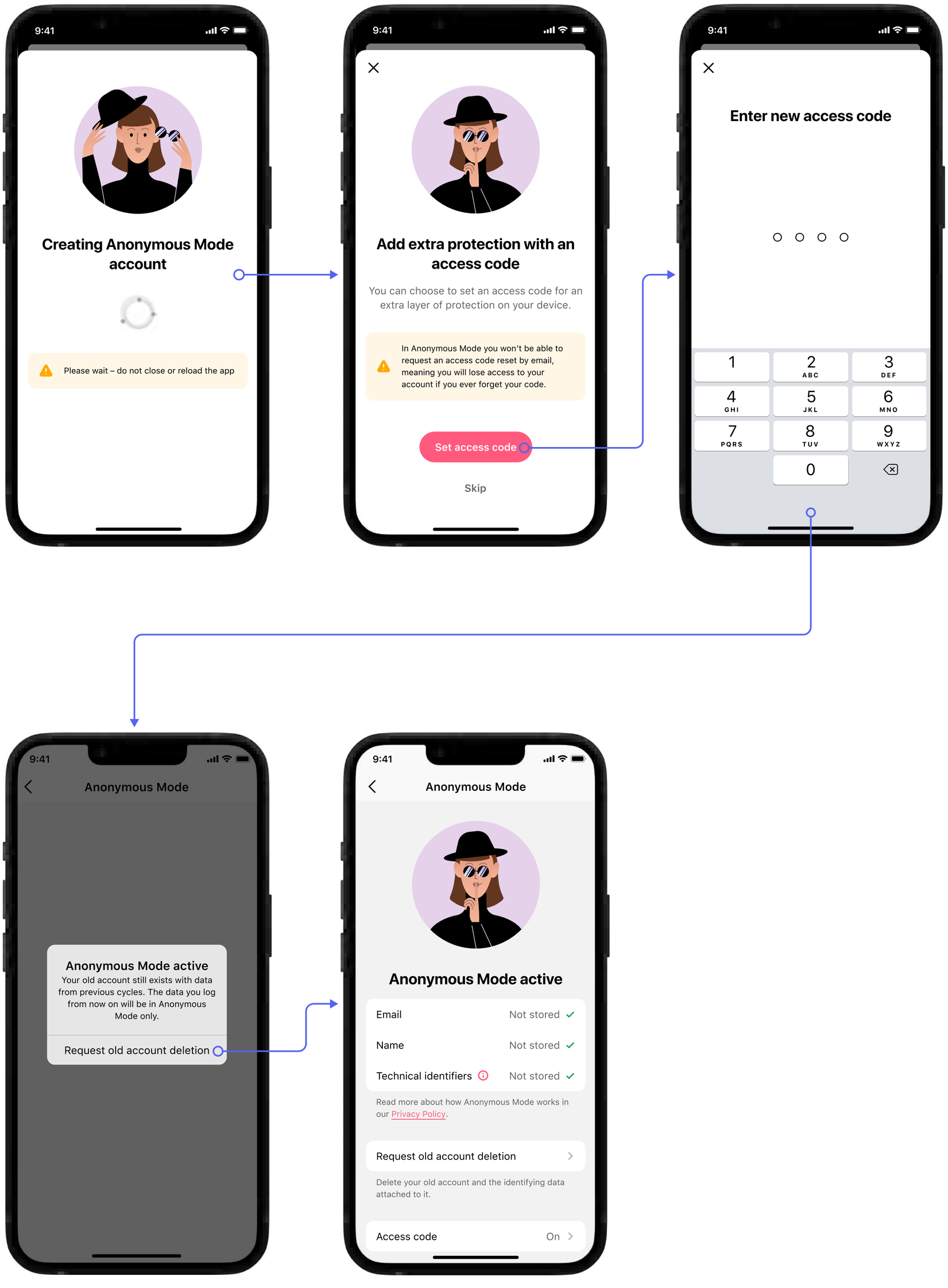
If a user wants to disable Anonymous Mode, they enter the sign-up flow. The number of transitions to and from Anonymous Mode is not limited.



Onboarding

If the user chooses to create an Anonymous Mode account, they are guided through a UI wizard that does the following:

- Explains which data will be kept and which forgotten
- Details which features will be unavailable in Anonymous Mode
- Indicates the transition progress and status
- Asks the user to request that their old account be deleted
- Encourages the user to create an access code to secure data access on their device



Technical deep dive

Anonymous Mode key design decisions

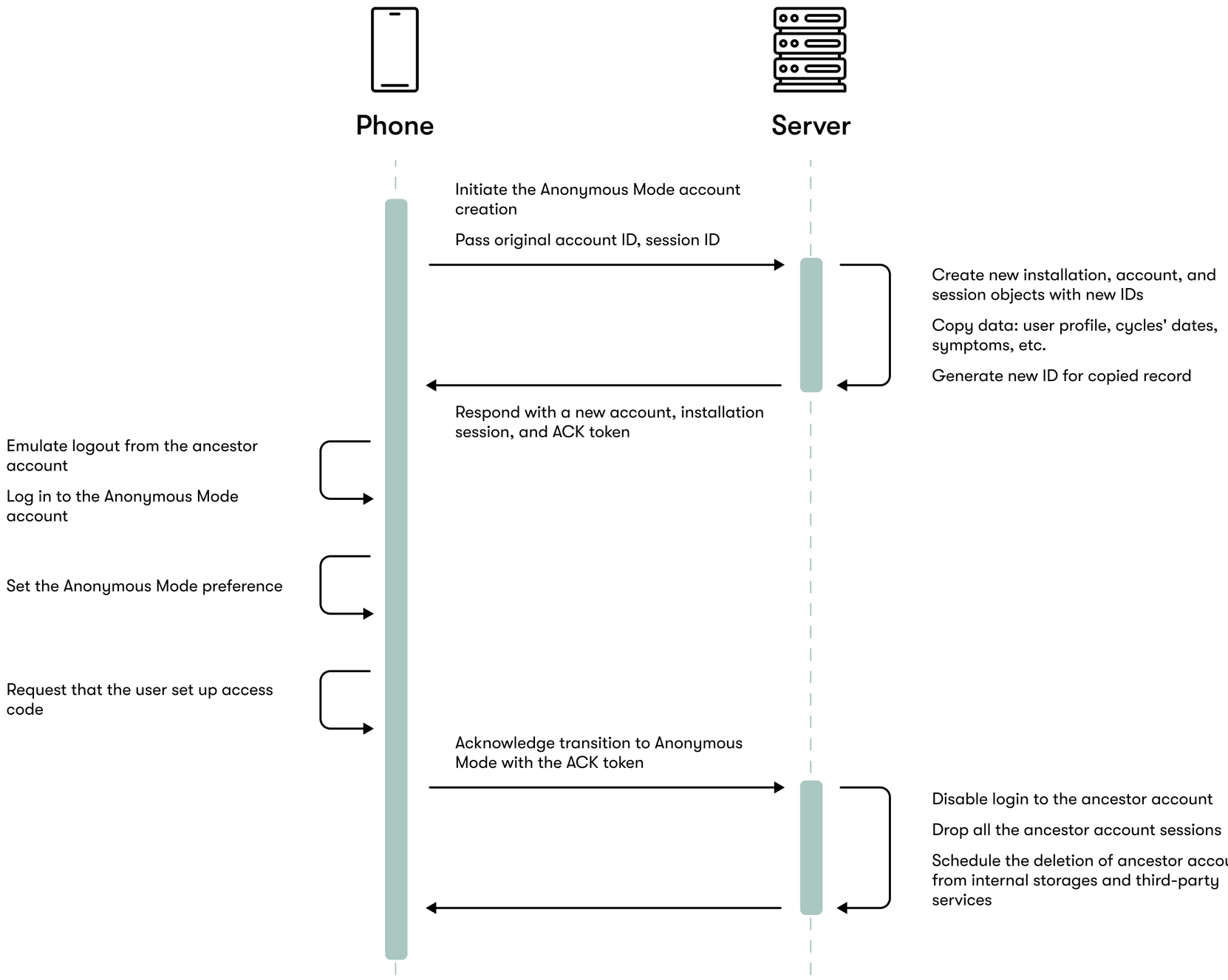


Image 1. Flow of transition to Anonymous Mode

1. When a user chooses to create an Anonymous Mode account, Flo creates a new, separate account that does not contain personal information. Flo transfers the application usage aim, cycle data, and marked symptoms from the ancestor account but does not transfer previously collected email, IP address, or other identifiers. By creating a new Anonymous Mode account and copying data to it instead of changing something in the ancestor account, Flo can control what data is transferred and ensure that only nonidentifiable data required for functionality is copied (e.g., users' notes are not copied because they may contain unique information that may identify or be associated with a user).

   At the same time, a new Flo user ID is created, and the application session and all the transferred records get new internal identifiers. This way, data will be separated from any past technical reference.

   This operation is performed on the backend side. During the process, the server knows which ancestor account is linked to the new Anonymous Mode one, but that knowledge is transient and lost after the server completes the data transfer. Note that if the user wants to come back to a non-Anonymous Mode account, it is not possible to restore it, but only to create a new one.

2. On a device, creating an Anonymous Mode account emulates logging out from the ancestor account and logging in to the new Anonymous Mode one. During the process, it resets the client-side storage for the Flo app and removes all personal information stored on the device within the Flo app.

3. Then, Flo sets a special preference on the device reflecting that the user is in Anonymous Mode, which:
   - Prevents the device from collecting some data from the operating system (e.g., advertising ID) despite the given permissions
   - Blocks the display of sign-up pop-ups
   - Upgrades the HTTP client used to communicate with the Flo backend via Oblivious HTTP relay (see Transport chapter)
   - Disables AppsFlyer and Sentry SDKs on the device

4. Anonymous Mode encourages users to enable an access code to improve the security of their Flo account.

5. At the end of the process, the client sends confirmation to the server, and the original account is deactivated immediately. This means that all existing sessions of that user are terminated, and a new one cannot be established through the login flow.
   In addition, the ancestor account deletion is scheduled in accordance with Flo's Privacy Policy.

If a user decides to leave Anonymous Mode, Flo extends their account with an identity (e.g., email or Google/Apple account ID) and resets the preference described in point 3 of the list above.

Three levels of Anonymous Mode architecture

There are three levels where changes had to be implemented to create the Anonymous Mode architecture: server, transport, and client.

SERVER

There are several categories of personal information that are normally collected by Flo and stored on the server side. The basis for this data collection is described in Flo's Privacy Policy and dedicated Privacy Portal. The following data collection must be stopped for users who switch to Anonymous Mode accounts:

- General information:
  - Email address (asked during sign-up)
  - Google or Apple account ID (asked during sign-up via Google/Apple)
  - Real-world name (may be asked during onboarding)
  - Billing address (when subscription is bought on Flo website)

- Technical identifiers collected automatically with appropriate user consent or operating system-level permission:
  - IDFA or another advertising ID (IFA, IFV, Android advertising ID)
  - IP address
  - Device ID
  - Device name
  - Payment transaction ID (see Subscriptions chapter)
  - Push notification token
  - Third-party-generated identifiers such as AppsFlyer ID, HealthKit event ID, or Auth0 account ID (Flo's vendor for authorization and authentication)
  - Credit card or PayPal payment information

Subscriptions

The subscription domain has integrations with the App Store, Google Play, Stripe, and PayPal, which are reflected by relevant IDs related to subscriptions. If Flo stores such connections in its database, these third-party IDs (e.g., in the case of an App Store subscription, original_transaction_id) may be used to identify Flo users. On the other hand, these third-party identifiers are connected to credit card data or Apple/Google accounts, which in turn, could have users' personal information. To break this end-to-end connection, Flo doesn't maintain a connection between external purchase ID and Flo user ID in the database and instead processes subscription status confirmation and/or renewal transiently when the user opens the app. The solution makes it impossible to link Flo user IDs with IDs from any of the external marketplaces Flo works with.

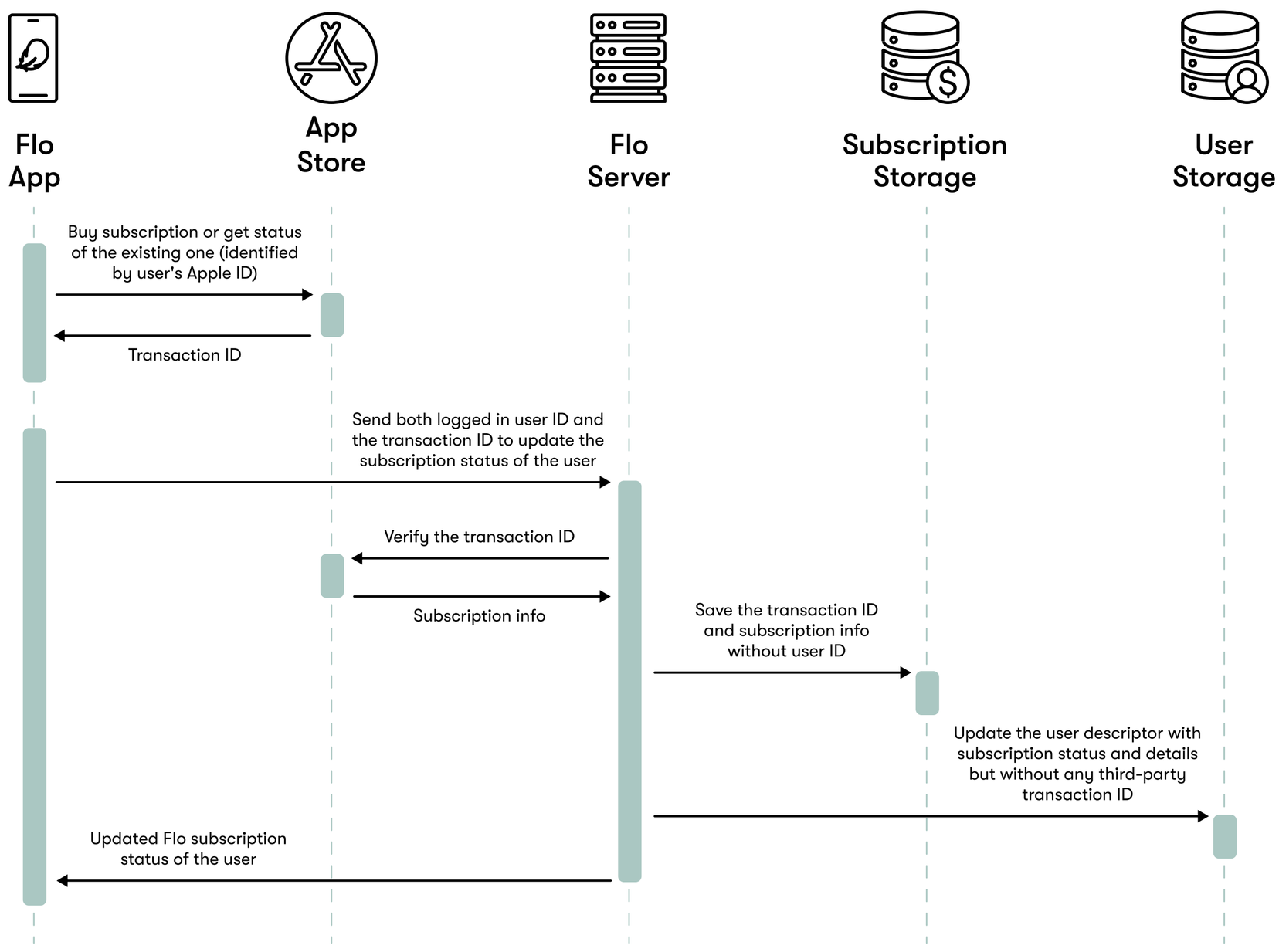


Image 2. Subscription flow for Flo Anonymous Mode

This technical solution has several pros and cons.

+ The user can transfer the subscription between Flo accounts as long as they continue using the same App Store or Google Play account.

+ There is no database storing mappings between third-party marketplace IDs and Flo user IDs, which can be used to look up users.

− Cross-platform subscriptions; it is not possible to buy a subscription in Google Play and use Flo Premium on iOS using Anonymous Mode.

− We can not update users' subscription statuses in the background and keep our database up to date for accurate analytics and reporting.

TRANSPORT

API and content resources

User traffic from any device, including mobile, could contain identifiable data and reveal very sensitive information about the user:

- Data inside an HTTP request
    - Headers: cookies, user agent, authentication tokens, and path, to name a few
    - Body: JSON bodies in HTTP API requests could contain sensitive health data
- Content delivery network requests, e.g., image paths like “/pregnancy_third_week.png,” especially connected to other personal information (like IP address)

Normally, this traffic is accompanied by the user’s IP address, which resides in a transport level of internet protocol and, generally speaking, can be used to identify a user.

Sample API request that we are securing (IDs have been replaced):

```
PUT https://api.owhealth.com/call/v1/userdata HTTP/2
Accept-Language: en
X-Api-Key: de69b65c-12db-4edb-ba53-99c2965ddaf
X-Application-Key: 3dcd1d99-1bb6-4c6e-a809-b607d9a04f3c
X-Screen-Scale: 2.17
X-Screen-Pixels: 1080x2340
User-Agent: Mozilla/5.0 (Linux; Android 12; SM-S906N
Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/80.0.3987.119 Mobile
Safari/537.36
Content-Type: application/json; charset=utf-8
Content-Length: 431
Host: api.owhealth.com
Connection: Keep-Alive
Accept-Encoding: gzip
{“update”:{“cycles”:[{“additional_fields”:
{},“pregnant”:false,“id”:“0f2472df-08d9-4bf9-
b467-9596302e5839",“period_end_date”:“2022-08-26T21:00:00+
0000",“period_intensity”:
{“4":-1,“3”:-1},“period_start_date”:“2022-08-20T21:00:00+0
000”,“pregnancy_end_reason”:0,“pregnant_due_date”:null,“pr
egnant_end_date”:null,“pregnant_start_date”:null,“source”:
null,“source_id”:null,“source_client”:2,“source_client_ver
sion”:“9.6.0"}]},“delete”:{}} END PUT (431-byte body)
```

Oblivious HTTP overview

To hide sensitive application and device data from Cloudflare and IP addresses from Flo, Anonymous Mode uses Oblivious HTTP (OHTTP), the emerging standard from the Internet Engineering Task Force co-developed by Cloudflare and Mozilla, with input from teams from Google, Apple, Brave, Akamai, and Fastly.

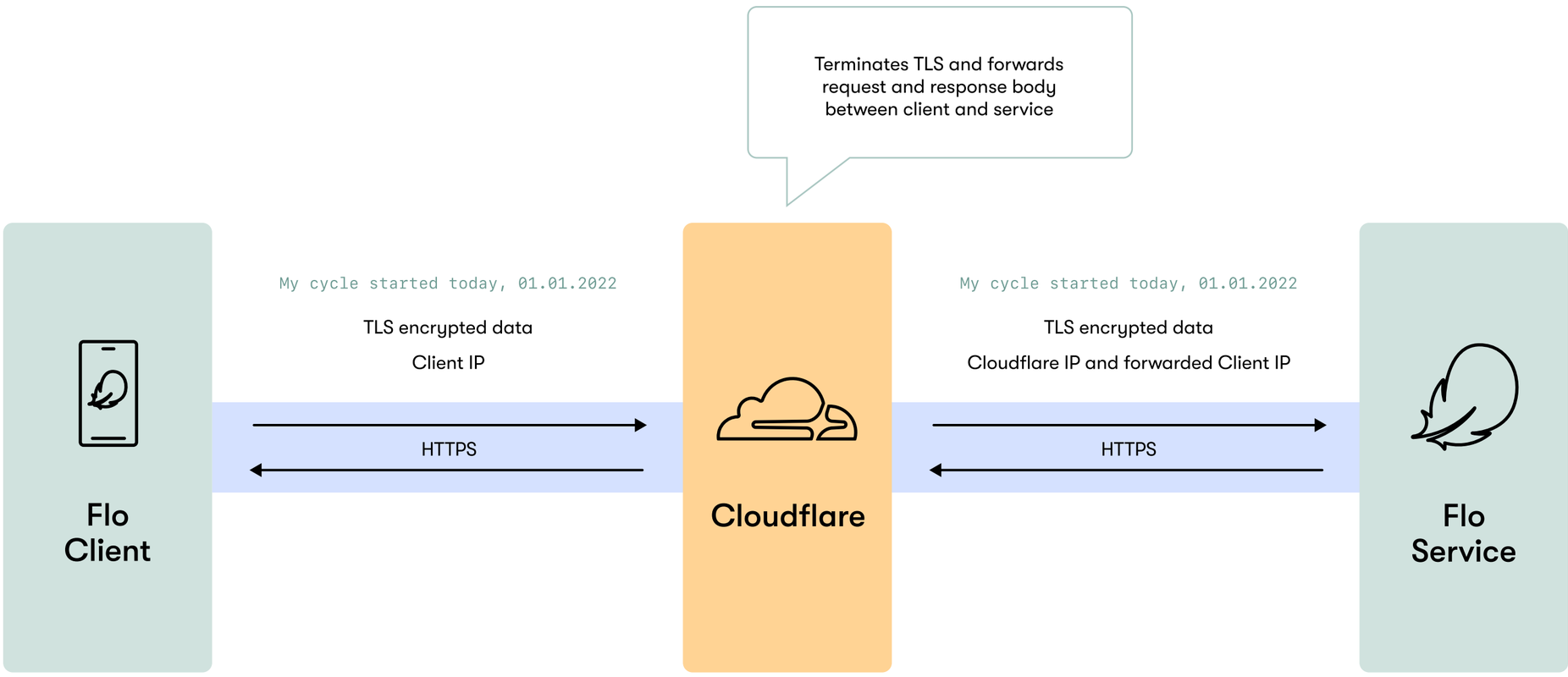


Image 3. Data transport infrastructure for non-Anonymous Mode accounts

For non-Anonymous Mode accounts, both Flo and Cloudflare may see the user's IP address and health data. This is because Cloudflare terminates TLS connections from the Flo app and, in processing a request from the application, forwards the user's IP address to Flo servers in an HTTP header. Improving user privacy further requires an architectural change.

In particular, this change consisted of two fundamental parts (see Image 4):

1. Flo end-to-end encrypts all application data between the client and Flo servers.
2. Cloudflare serves as a relay for requests between the Flo app and its servers, which does not reveal the user IP address to Flo servers.

This means that the Cloudflare relay sees user IP addresses but not user data, whereas the Flo service sees user data but not user IP addresses. This is elaborated on below.

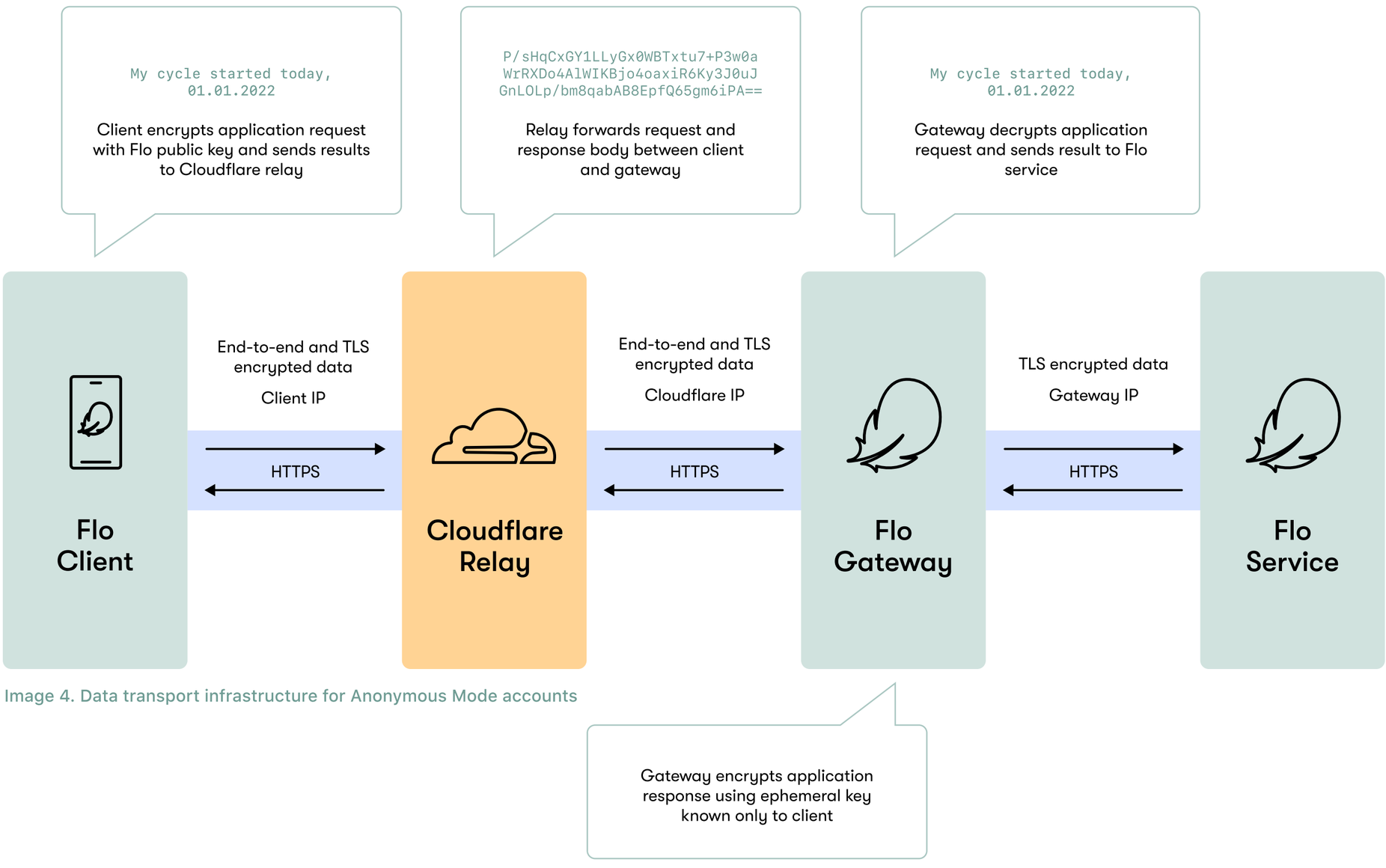


Image 4. Data transport infrastructure for Anonymous Mode accounts

OHTTP introduces two new entities that help process HTTP requests: a *relay*, operated by Cloudflare, and a *gateway*, operated by Flo. Application requests are end-to-end encrypted between the client and gateway. These requests pass through the relay from client to gateway. In effect, the relay sees the user IP address (and other request metadata) but not the application data, and the gateway sees the application data but not the user IP address. This is summarized in the image above.

In this architecture, every Flo client application request is first binary encoded and then encapsulated using a fresh, one-time-use ephemeral key (which is combined with the gateway's public key; see Hybrid Public Key Encryption). The Flo client sends this encapsulated request to the Cloudflare relay – *https://flo.app-relay.cloudflare.com*. The relay then forwards this data to the Flo gateway. The gateway uses its private key along with the client's ephemeral key to decapsulate each request. Thus, it decrypts it to recover the original application request, which it then sends to the Flo service as usual for processing. The response from the Flo service is then again encapsulated, encrypted, and passed back to the relay.

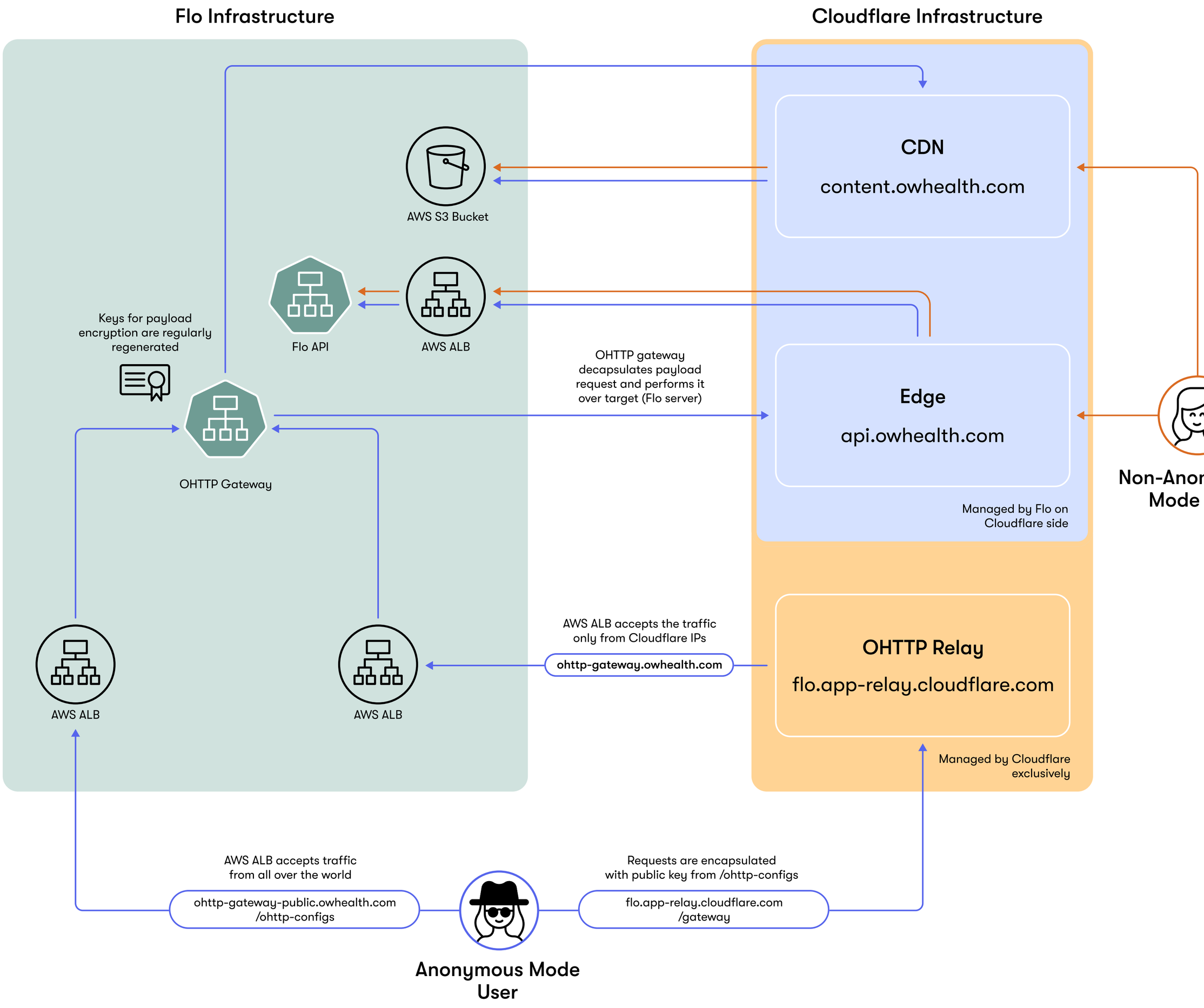


Image 5. OHTTP architecture at Flo

Oblivious HTTP architecture

To implement the OHTTP standard, Anonymous Mode uses an open-source solution developed by the Cloudflare team with Flo's contribution. It encompasses App Relay, a service run on Cloudflare Workers, and Flo Gateway. On the client side, Flo uses the open-source Rust library compiled for iOS and Android. Flo uses Protocol Buffers to encode application requests instead of Binary HTTP. This allows code to be reused more easily across Android and iOS platforms without reimplementing a new serialization format. Details about how OHTTP can be used with different application serialization formats can be found in the specification.

Public key configuration
The gateway public key used for request encapsulation is regularly rotated to mitigate the risk of private key compromise. Therefore, clients must regularly fetch it directly from Flo's gateway (*https://ohttp-gateway-public.owhealth.com/ohttp-configs*) rather than from Cloudflare's relay. This is done to ensure that Flo is the only entity capable of providing this key, and another party (a relay) has no way to substitute the key (and thus get decryption possibilities). This means that Flo has access to the IP address of the client sending the request but only for a single particular request for the public key configuration.

To mitigate the risk of this IP address being used or correlated with logs or other data and therefore identifying a user, the Flo app makes requests to retrieve the gateway public key for all users — not just those who are using Anonymous Mode. As a result, the IP address does not reveal anything about a specific Anonymous Mode user. Moreover, these requests are performed independently of user actions, so the timing of each request does not reveal information about individual user behavior.

Stripping out all unnecessary headers from the encapsulating OHTTP request
An OHTTP request itself is an HTTP POST, so while the client device sends the data through the gateway, it also adds HTTP headers like user-agent and language. User-agent differs from device to device and can be exploited in probabilistic matching algorithms along with time and other data. Anonymous Mode additionally anonymizes these OHTTP requests, making user-agent and language the same for everyone, regardless of the device or platform on which the request is generated.

Third-party requests from client
All requests that are not allowed by Flo are blocked. This means that only OHTTP-protected requests to Flo's API and content delivery network servers are allowed. All requests to third parties are blocked.

Restrictions and limitations of OHTTP

- Video streaming is not protected in the same way as HTTP API and content requests.
    - Video streaming is not suitable for OHTTP protocol as it is designed to secure HTTP request-response rather than streams of data. It is generally possible to secure streams too but requires much more complicated and resource-hungry application services.

    - Instead of using specific titles for videos (like the aforementioned “pregnancy_third_week.avi,” for example), random file identifiers are implemented. Also, this data is stored for a very limited period of time in correspondence with Cloudflare’s Privacy Policy.
    - This topic will be reiterated during the next feature upgrades since there are emerging services or features that could be utilized in the future.

- There is added latency for the extra hops for each request as data passes from source to destination through additional layers. Some measures have already been taken toward minimizing network hops with the intention to go even further in the future if there are noticeable user experience lags. This is one reason why OHTTP is not offered as a default option, since it is still not clear if this added security will be adequate for all users, keeping in mind a generally accepted security/convenience ratio.

- OHTTP architecture does invalidate some features provided by the L7 proxy, including caching, but it’s not necessary to use OHTTP for all requests between client and server. In the current implementation, Flo chose to load images/PDFs through OHTTP, too, in order to address the aforementioned security considerations. But some features of AWS WAF based on IP addresses are also lost. For example, the lack of an IP address may limit Flo’s capabilities to detect malicious traffic from bots. However, there are ways to mitigate that issue in the future.

CLIENT

In addition to the technical solutions protecting data on the server side and in transit, an important layer of security is the user’s device itself, taking into account the risk of it being stolen, lost, or accessed by third parties.

In Anonymous Mode:

- Third-party SDKs (AppsFlyer, Sentry) are terminated to prevent sending data to the third parties or to Flo servers without additional encryption in transit.
- Data related to the ancestor account is completely cleaned from the device storage.
- During feature onboarding, users are encouraged to protect their accounts with an access code.
  The device communicates with Flo servers only via OHTTP relay with very few exceptions. These exceptions include:
    - Retrieving the OHTTP public key
    - Downloading video
    - Opening auxiliary pages inside the web view (e.g., Help Center articles)

Restrictions and limitations

The Anonymous Mode feature is not available for paying web users because of the clear connection to their credit cards. Users faced with such cases should contact Flo's Support team via support@flo.health.

Also, switching to Anonymous Mode leads to some feature limitations, which is why it is not offered as a default option. For instance:

- In the current version, Flo cannot offer the additional level of privacy with Anonymous Mode when connecting wearable devices.
- Engineers will face a lack of information about crashes as the Sentry SDK is terminated.
- It is impossible to transfer an Anonymous Mode account's historical data to a new device or to recover the data in case the device is broken or stolen.
- The history of interaction with stories, chatbots, and activity in Secret Chats is not transferred to the Anonymous Mode account. Requests to the Flo Support team will not be available from the app.
- This means that although the user can send their request via email, the Support team will not be able to solve the problem with a specific account. They will only be able to provide generic advice.
- Email communication is not available.

Potential and known issues

As is the case with all technology products, in certain limited circumstances, it may be theoretically possible for a sophisticated threat actor to circumvent security measures.

Is it possible to match the digital health data within Flo with a unique combination of cycles, symptoms, and other data points received outside the app?

It's very unlikely that someone has access to such data. And even so, with 257 million users, the chance that someone will have the same or similar health patterns is high, essentially negating the ability to match. Also, even if someone already has such data, there is not much sense in doing deidentification and requesting this information from Flo.

Could the user be identified by joining request data from the gateway and relay using request timestamps?

While this is theoretically possible, the probability of such an occurrence is extremely low to nonexistent for the following reasons:

- Requests from the relay to gateway introduce some amount of additional latency, so the precise timestamp at which the relay receives a request will be different from the timestamp at which the gateway receives a request. Clock skew between the relay and gateway may also contribute further to differences in these timestamps.
- The relay services many client requests simultaneously, so a single timestamp is not sufficient to uniquely identify a specific request from a client.

Could the user's data be compromised if the gateway OHTTP key were compromised?

In practice, attacks that lead to this type of compromise are considered highly unlikely, difficult, and expensive to implement. This scenario would allow the threat actor to decrypt any data encapsulated and protected via OHTTP. However, a threat actor only has access to these encapsulated OHTTP requests if they can also compromise the TLS connection between client and relay, or between relay and gateway. Thus, OHTTP only protects against man-in-the-middle-style attacks insofar as the gateway key and TLS connections are not compromised.

If the user's physical device were compromised, could the user's data be compromised as well?

To decrease the chances for health data being compromised from direct access to the device, Flo encourages users to add an access code for their Flo Anonymous Mode account during onboarding. The access code is an additional layer of privacy in case the device is compromised. It significantly mitigates the most common risk of unauthorized access to the device (lost, stolen, accessed).

Conclusion and kudos

Flo Anonymous Mode introduces a new level of protection for our users' reproductive health data. The top-notch architecture that Anonymous Mode is built on makes it so that no single party, including Flo, can match a real person with health data inside the app, and this can be considered a significant advancement in the privacy and security of the health data of women and people who menstruate.

Anonymous Mode embraces core parts of the data journey and promotes privacy on several major levels, from a logged symptom or periods on the device over the network to the server. This groundbreaking approach allows users to continue tracking their health and benefit from the information logged before, now as privately as possible.

Offering such a level of transparency around Anonymous Mode's architecture in this white paper, Flo, as the most popular female health app, also aims to encourage other companies to raise the bar when it comes to privacy and security principles. To learn more about our commitment to privacy and security, please visit flo.health/privacy-portal.

We were lucky enough to work closely with Chris Wood, Research Lead at Cloudflare Research, and the Cloudflare team on this project. We would like to extend our huge gratitude to Chris. Without his monumental support, cutting-edge innovation, and vast knowledge, we may not have been able to offer this important feature to our users.

We also want to thank the Dechert LLP team, top-ranked and internationally recognized privacy and cybersecurity lawyers who have supported us throughout this project by providing privacy law counseling with respect to Flo's privacy program, both under US law and globally.

Additional technical resources

Oblivious HTTP Application Intermediation,
https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-04

Internet Research Task Force (IRTF),
https://datatracker.ietf.org/doc/html/rfc9180

OHTTP analysis on GitHub,
https://github.com/cloudflare/ohttp-analysis

Oblivious DNS over HTTPS,
https://datatracker.ietf.org/doc/html/rfc9230

Oblivious DNS over HTTPS (ODoH): A Practical Privacy Enhancement to DNS,
https://research.cloudflare.com/publications/Singanamalla2021/

iCloud Private Relay Overview,
https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf

Flo

September 2022