Gaps In Care Member Interview Learnings

Virgin Pulse, March 2019

TL;DR:

Members **want to be in control** of their data, regardless of what they think is sensitive. This includes the choice to **opt-in** rather than opt-out.

Members want **a simple explanation** of where their data comes from and what we're doing with it, along with **their rights** if we fail to protect it.

Our security layer sends a strong signal that we're **serious about protecting our members**. We should enhance this but be attentive to daily experience.

Interview Details

- 4 Members interviewed, recruited from the group that took our Survey (~500 Members) in the fall.
- We contacted Members that were wary of us using outside data **AND** offered well-written explanations.
- Questions all dealt with:
  - Thoughts on security/privacy in general
  - Thoughts on their trust of Virgin Pulse
  - Some questions on planned Gaps in Care functionality

Member Survey Reminder

Security was a major concern even for people who were comfortable with sharing. It was top of mind.

People were far more **scared of general security/data breaches** than they were of their employer or insurer.

Most common theme: **this is between me and my doctor**.

A small but vocal minority of Members *really* didn’t want this. Allowing them to **opt out** is probably necessary to avoid a backlash that could negatively affect usage.

Identified Themes

1. What is Virgin Pulse?
2. Sensitive information
3. Trust
4. Informed consent/simple language
5. Opt-in

Theme 1: What is Virgin Pulse

All participants referred to us as some version of “**a (fun) activity & habit tracking program**”.

Most said that **what we’re planning made sense**, that it seemed like an expected move for us.

1 Member said she didn’t think we should do anything with healthcare because **it would “ruin” the platform if she was required to use it**.

Interpretation:

Most Members will be ok with our changes. Some will not be, but they already perceive our service as slightly burdensome to them.

Program design will need to offset some of this effect.

Theme 2: Sensitive Information

Everyone had different ideas of what sensitive information was, but **fear of it being “used against you”** was the common factor.

They all mentioned wanting **specific, granular control of that sharing**.

Interpretation:

Being in control makes people more comfortable.

Letting them control sharing removes the “creepy” factor we worried about, possibly because the Member gets to decide and do their own cost/benefit analysis.

Theme 3: Trust

Every participant places some level of trust in us. We show strong signals of trustworthiness.

They all said **they would believe us** if we told them in app that nothing would be shared with their employer. They also said that message should be repeated.

Every participant mentioned that a component of that trust was knowing that **they have recourse against us** through things like HIPAA if there was ever a problem.

Interpretation:

People have accepted that a certain level of abuse has become inevitable with all the data out there. They want to be in control and know what they can do about abuse.

Constant reinforcement of privacy and security messaging is a vital part of keeping trust.

Theme 4: Informed Consent/Simple Language

Everyone wanted to know exactly what was going on with their data, **explained to them in simple language**, as part of choosing what they would let us do with that information.

3 said that if they liked the explanation they'd let us use the info even though they were skeptical at first. 1 said she would never, but **if the explanation seemed aboveboard she wouldn't worry** about what we were doing, even if she wouldn't use it herself.

Interpretation:

Being clear and transparent increases trust, may increase utilization, and may decrease complaints.

Theme 5: Opt-in

Every participant preferred an opt-in model. This matched their stated need to be in control of their data.

Opt-in made the people who weren't comfortable with using the feature **comfortable with its existence** and reinforced their trust in us.

Offering **rewards changed people's minds** to opt-in, in both the survey and the interviews.

Interpretation:

Opt-in is the build option that preservers most Members' trust in us as a company. We should consider it as a platform-wide directive.

Reward-seeking behavior also seems to overcome some objections as long as a Member trusts us.

Conclusions

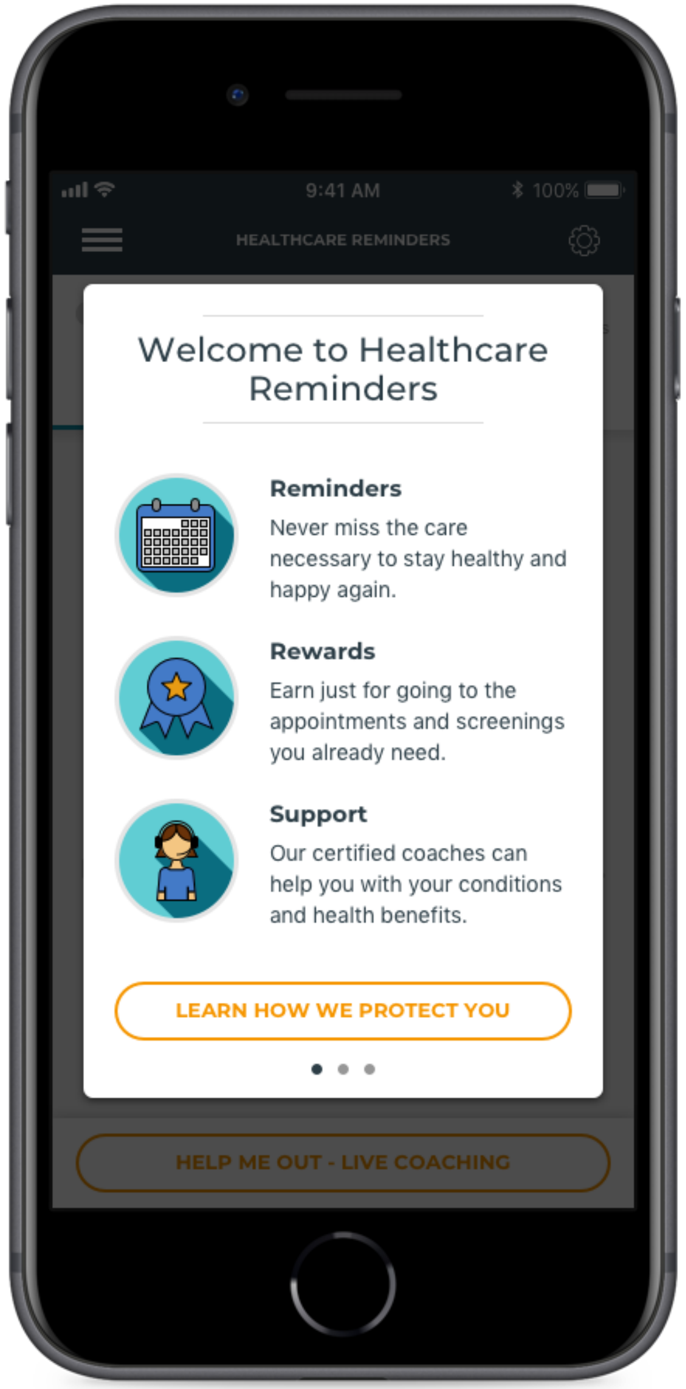
Members **trust** us already, but it will be very easy to lose that trust.

Member want to be **informed**, and to give or revoke their consent based on that information.

Any use of Member data, regardless of the source, should be opt-in to keep them in **control**.

All of these factors will add up to building and maintaining the trust of our Members.

Ideas: Feature Intro

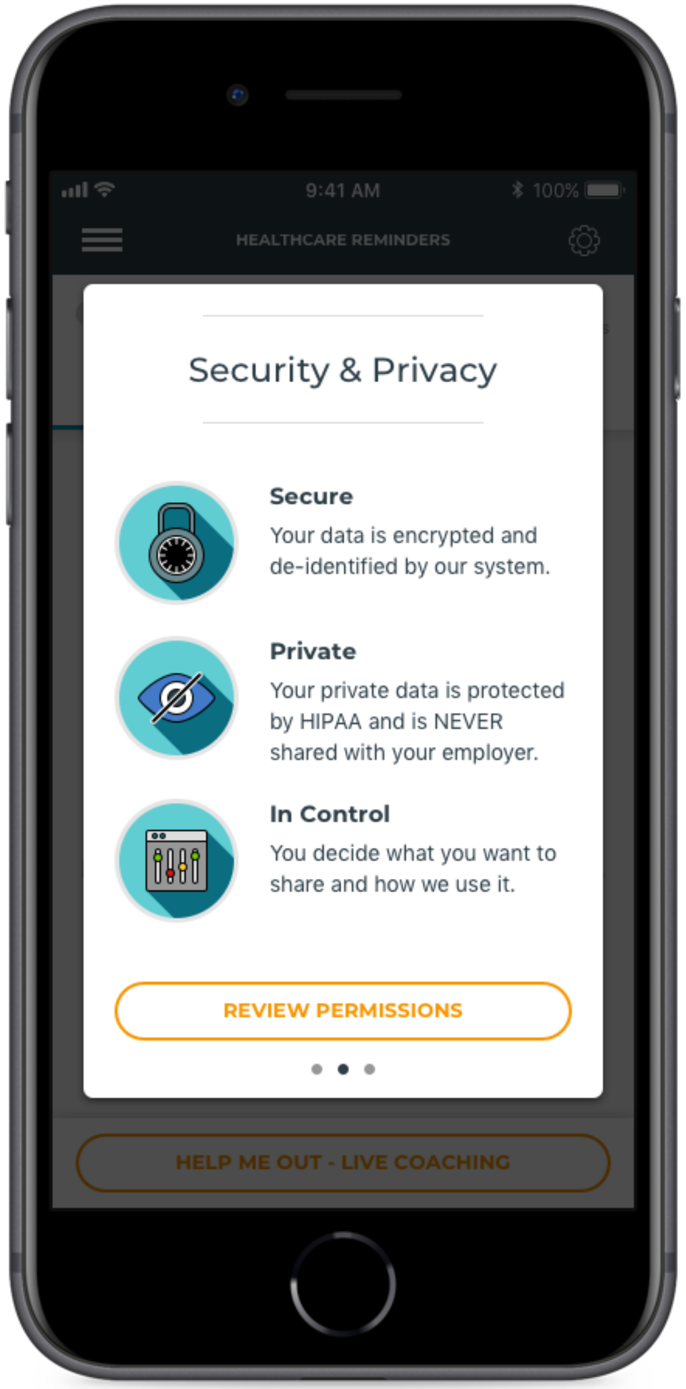


Welcome to Healthcare Reminders

Reminders
Never miss the care necessary to stay healthy and happy again.

Rewards
Earn just for going to the appointments and screenings you already need.

Support
Our certified coaches can help you with your conditions and health benefits.

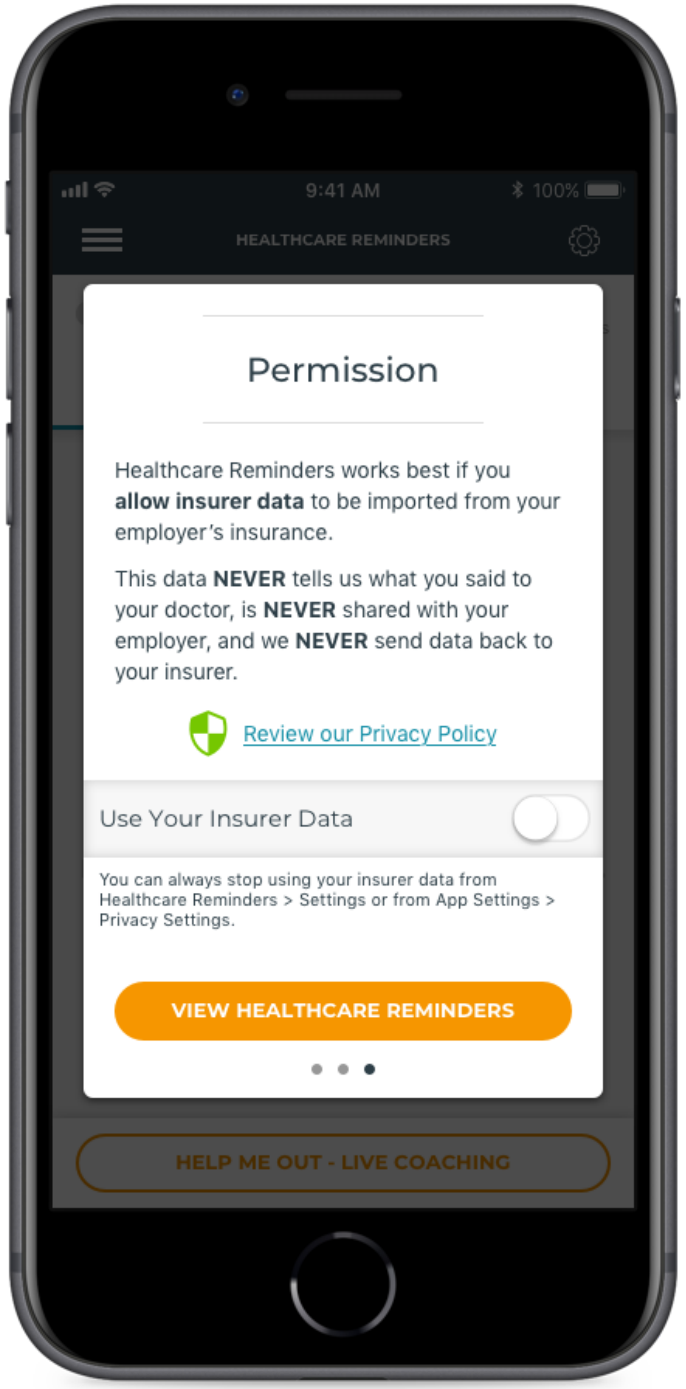


Security & Privacy

Secure
Your data is encrypted and de-identified by our system.

Private
Your private data is protected by HIPAA and is NEVER shared with your employer.

In Control
You decide what you want to share and how we use it.



Permission

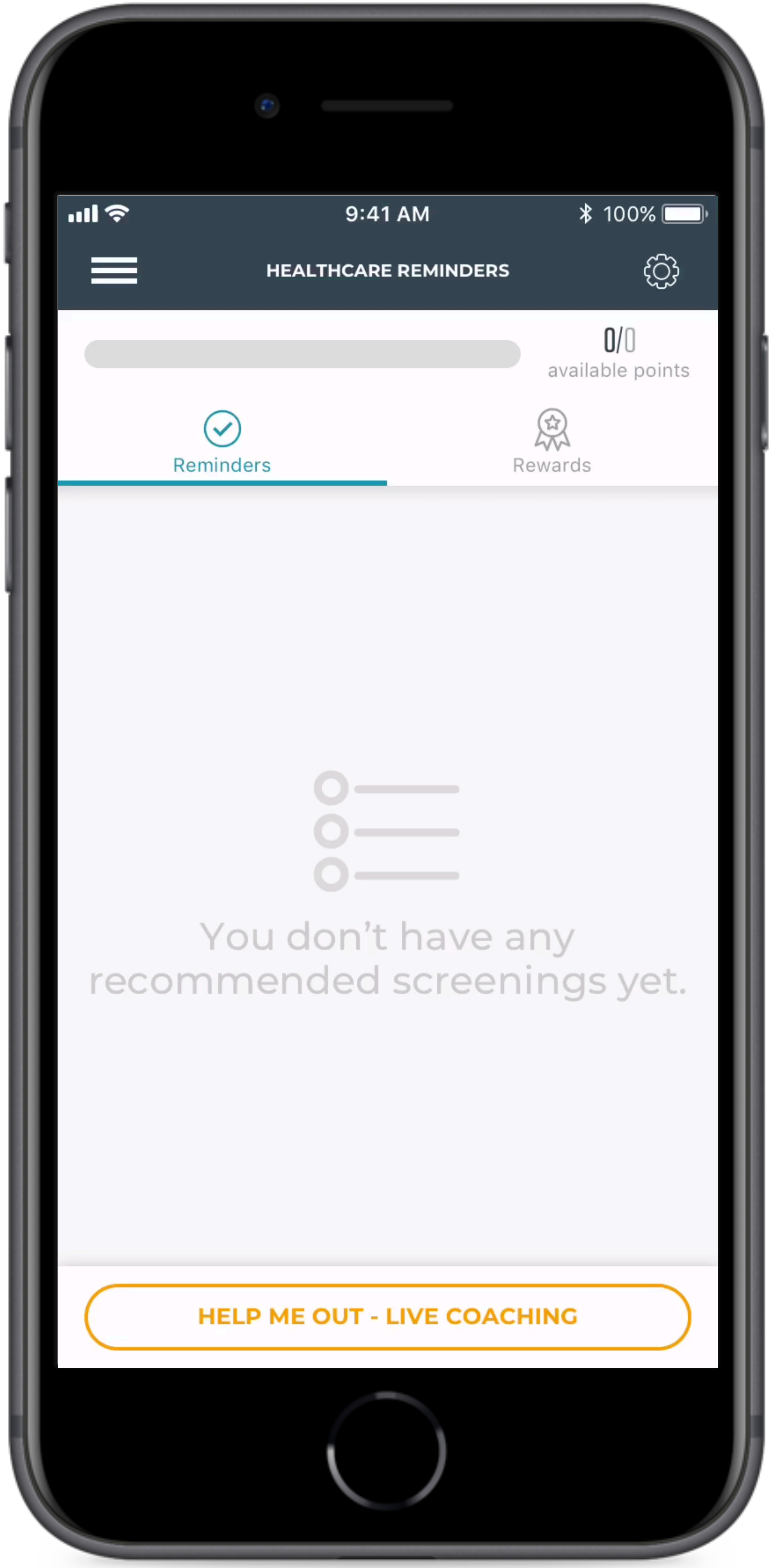
Healthcare Reminders works best if you **allow insurer data** to be imported from your employer's insurance.

This data **NEVER** tells us what you said to your doctor, is **NEVER** shared with your employer, and we **NEVER** send data back to your insurer.

Review our Privacy Policy

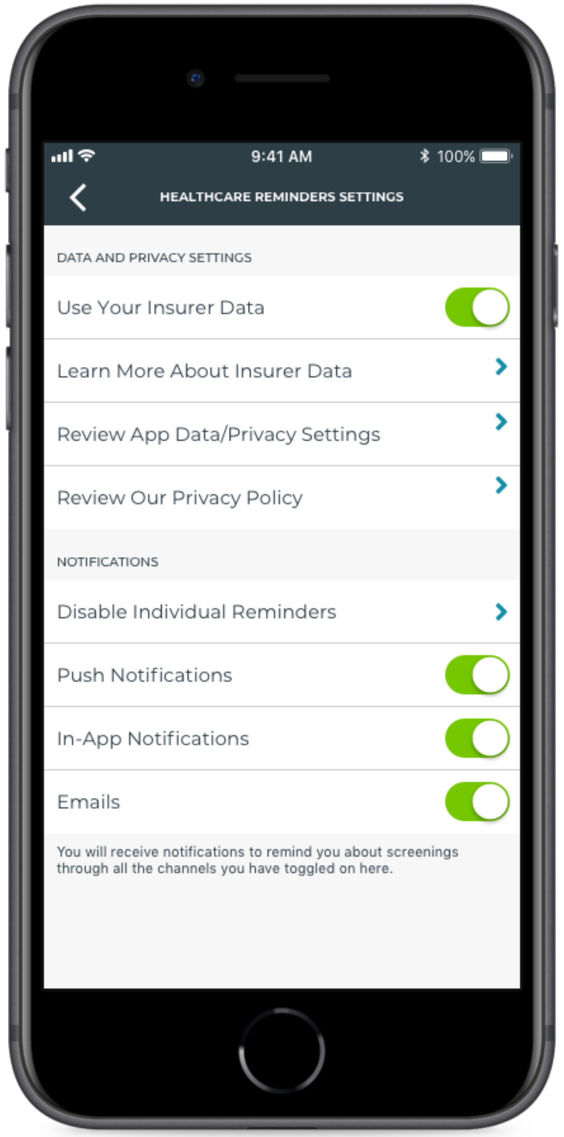
Use Your Insurer Data ○

You can always stop using your insurer data from Healthcare Reminders > Settings or from App Settings > Privacy Settings.



You don’t have any recommended screenings yet.

Ideas: Privacy Settings



HEALTHCARE REMINDERS SETTINGS

DATA AND PRIVACY SETTINGS

Use Your Insurer Data

Learn More About Insurer Data

Review App Data/Privacy Settings

Review Our Privacy Policy

NOTIFICATIONS

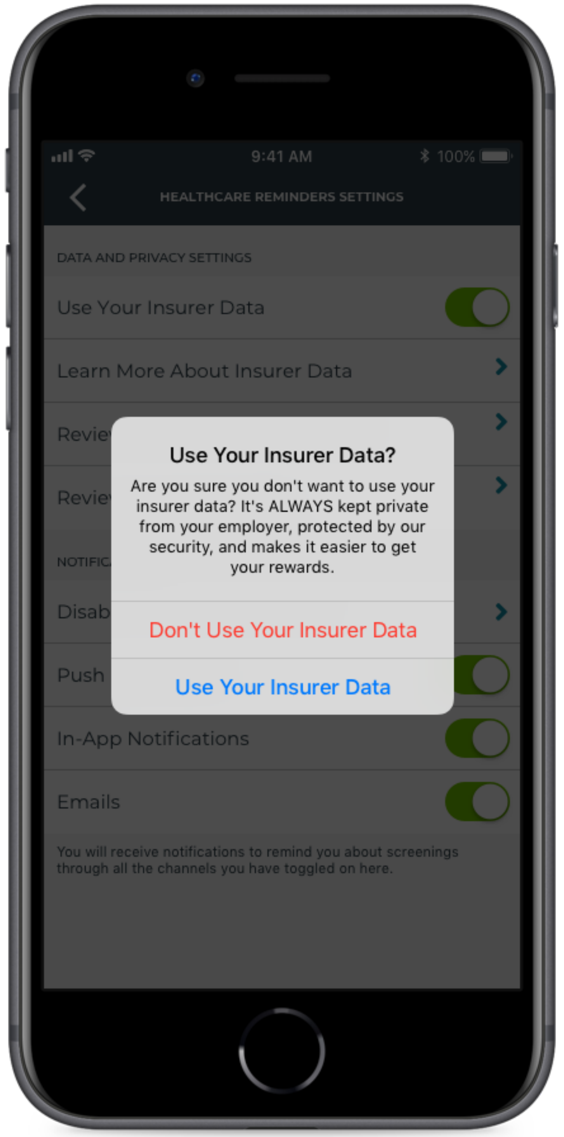
Disable Individual Reminders

Push Notifications

In-App Notifications

Emails

You will receive notifications to remind you about screenings through all the channels you have toggled on here.



HEALTHCARE REMINDERS SETTINGS

DATA AND PRIVACY SETTINGS

Use Your Insurer Data

Learn More About Insurer Data

Revie

Revie

NOTIFIC

Disab

Push

In-App Notifications

Emails

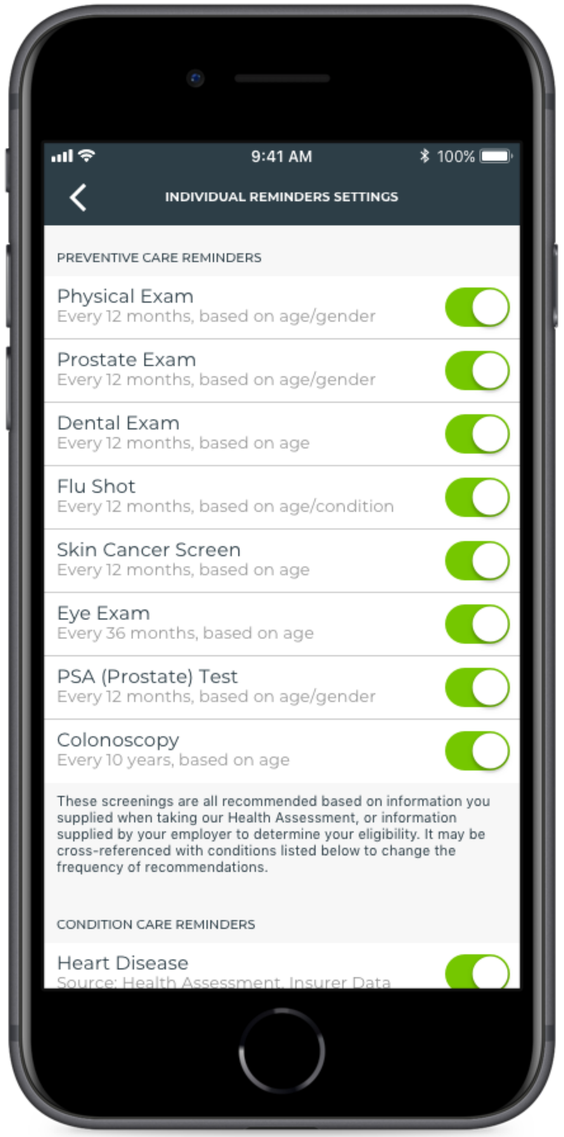
You will receive notifications to remind you about screenings through all the channels you have toggled on here.

Use Your Insurer Data?

Are you sure you don't want to use your insurer data? It's ALWAYS kept private from your employer, protected by our security, and makes it easier to get your rewards.

Don't Use Your Insurer Data

Use Your Insurer Data



INDIVIDUAL REMINDERS SETTINGS

PREVENTIVE CARE REMINDERS

Physical Exam
Every 12 months, based on age/gender

Prostate Exam
Every 12 months, based on age/gender

Dental Exam
Every 12 months, based on age

Flu Shot
Every 12 months, based on age/condition

Skin Cancer Screen
Every 12 months, based on age

Eye Exam
Every 36 months, based on age

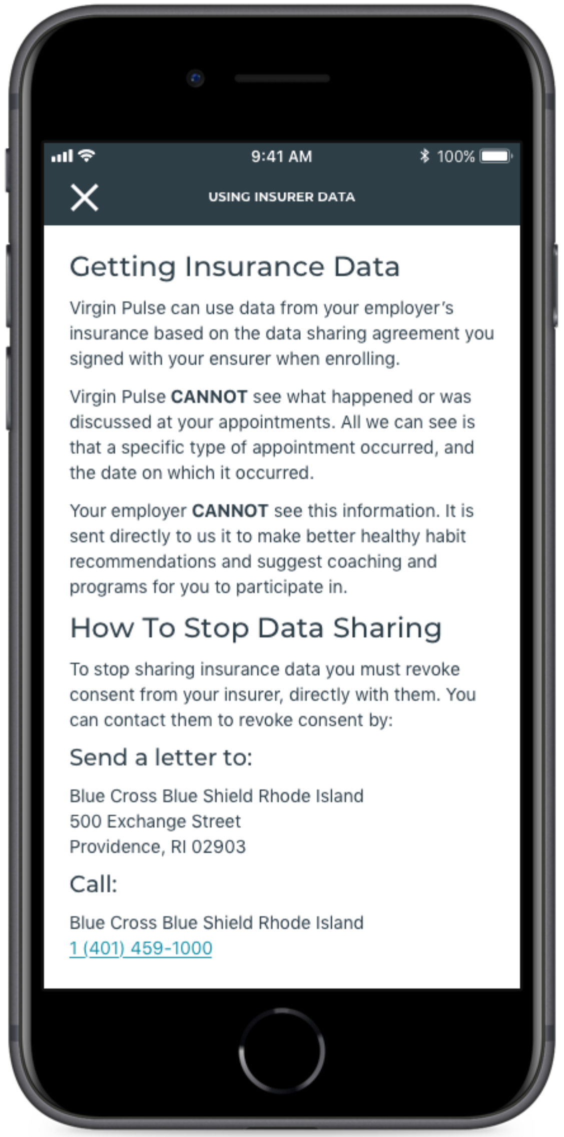
PSA (Prostate) Test
Every 12 months, based on age/gender

Colonoscopy
Every 10 years, based on age

These screenings are all recommended based on information you supplied when taking our Health Assessment, or information supplied by your employer to determine your eligibility. It may be cross-referenced with conditions listed below to change the frequency of recommendations.

CONDITION CARE REMINDERS

Heart Disease
Source: Health Assessment, Insurer Data



USING INSURER DATA

Getting Insurance Data

Virgin Pulse can use data from your employer's insurance based on the data sharing agreement you signed with your ensurer when enrolling.

Virgin Pulse **CANNOT** see what happened or was discussed at your appointments. All we can see is that a specific type of appointment occurred, and the date on which it occurred.

Your employer **CANNOT** see this information. It is sent directly to us it to make better healthy habit recommendations and suggest coaching and programs for you to participate in.

How To Stop Data Sharing

To stop sharing insurance data you must revoke consent from your insurer, directly with them. You can contact them to revoke consent by:

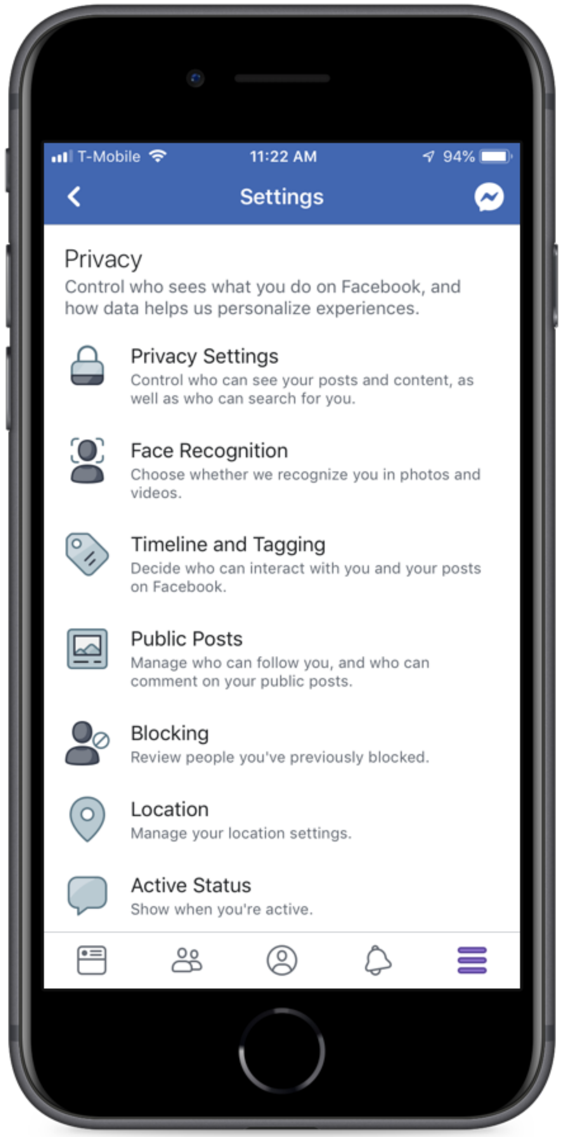
Send a letter to:

Blue Cross Blue Shield Rhode Island
500 Exchange Street
Providence, RI 02903

Call:

Blue Cross Blue Shield Rhode Island
1 (401) 459-1000

Example: Granular Privacy Controls



T-Mobile 11:22 AM 94%

Settings

Privacy
Control who sees what you do on Facebook, and how data helps us personalize experiences.

Privacy Settings
Control who can see your posts and content, as well as who can search for you.

Face Recognition
Choose whether we recognize you in photos and videos.

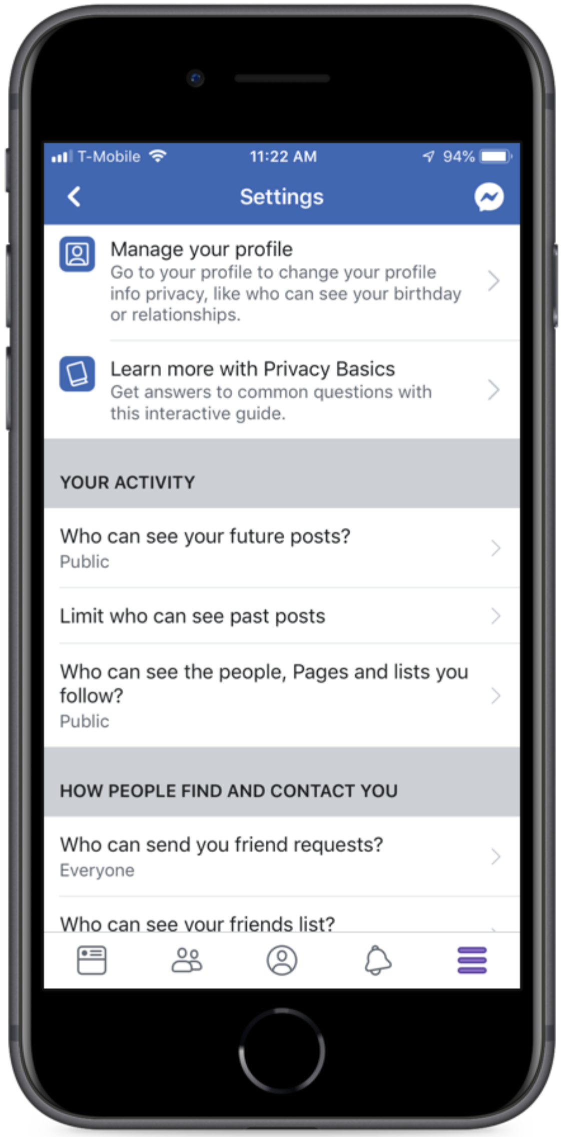
Timeline and Tagging
Decide who can interact with you and your posts on Facebook.

Public Posts
Manage who can follow you, and who can comment on your public posts.

Blocking
Review people you've previously blocked.

Location
Manage your location settings.

Active Status
Show when you're active.



T-Mobile 11:22 AM 94%

Settings

Manage your profile
Go to your profile to change your profile info privacy, like who can see your birthday or relationships.

Learn more with Privacy Basics
Get answers to common questions with this interactive guide.

YOUR ACTIVITY

Who can see your future posts?
Public

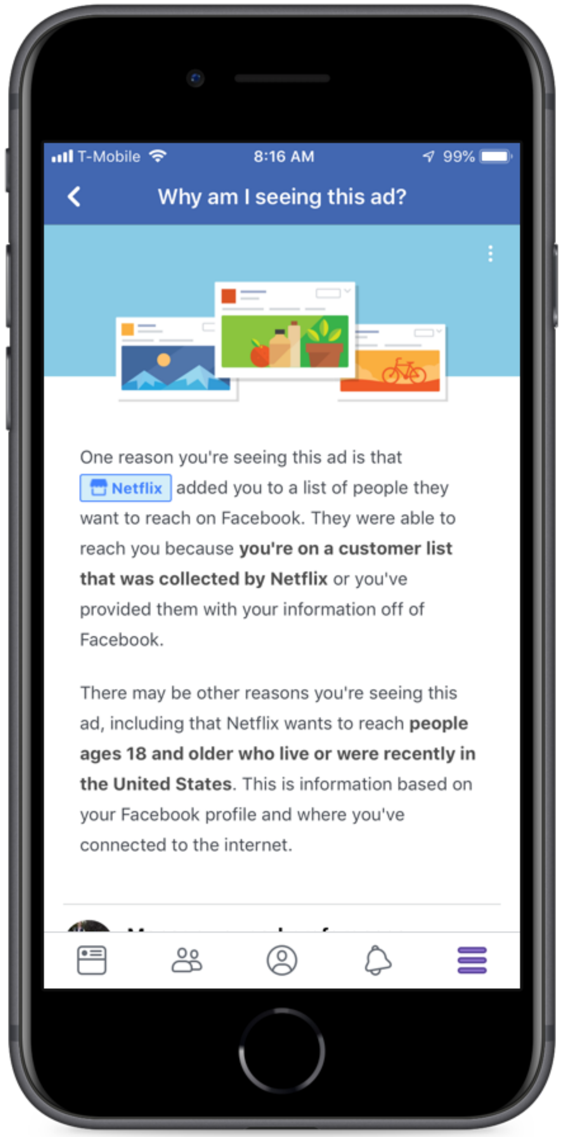
Limit who can see past posts

Who can see the people, Pages and lists you follow?
Public

HOW PEOPLE FIND AND CONTACT YOU

Who can send you friend requests?
Everyone

Who can see your friends list?

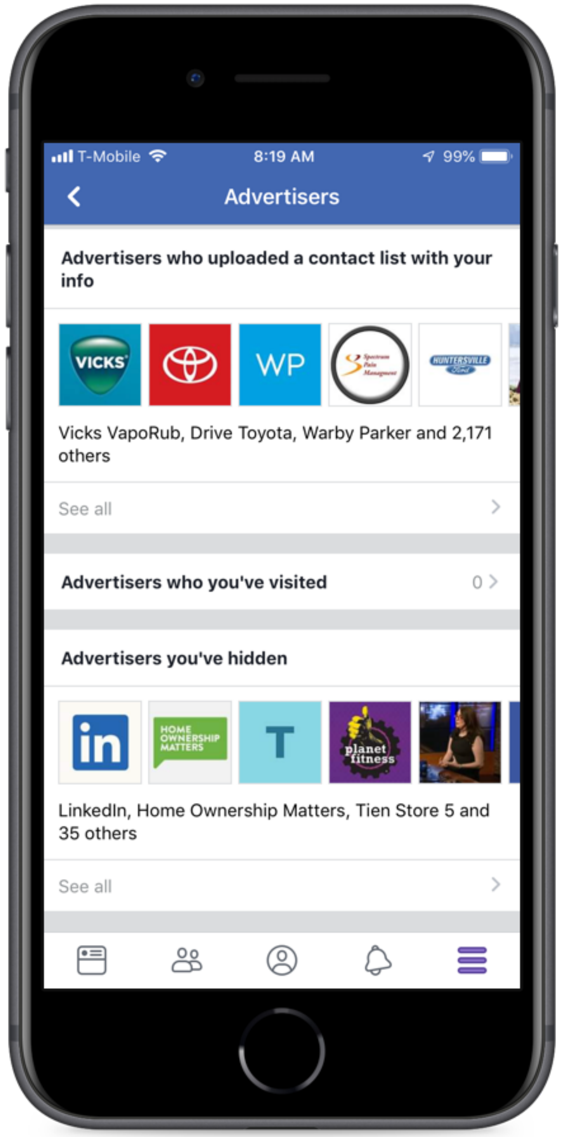


T-Mobile 8:16 AM 99%

Why am I seeing this ad?

One reason you're seeing this ad is that Netflix added you to a list of people they want to reach on Facebook. They were able to reach you because **you're on a customer list that was collected by Netflix** or you've provided them with your information off of Facebook.

There may be other reasons you're seeing this ad, including that Netflix wants to reach **people ages 18 and older who live or were recently in the United States**. This is information based on your Facebook profile and where you've connected to the internet.



T-Mobile 8:19 AM 99%

Advertisers

Advertisers who uploaded a contact list with your info

Vicks VapoRub, Drive Toyota, Warby Parker and 2,171 others

See all

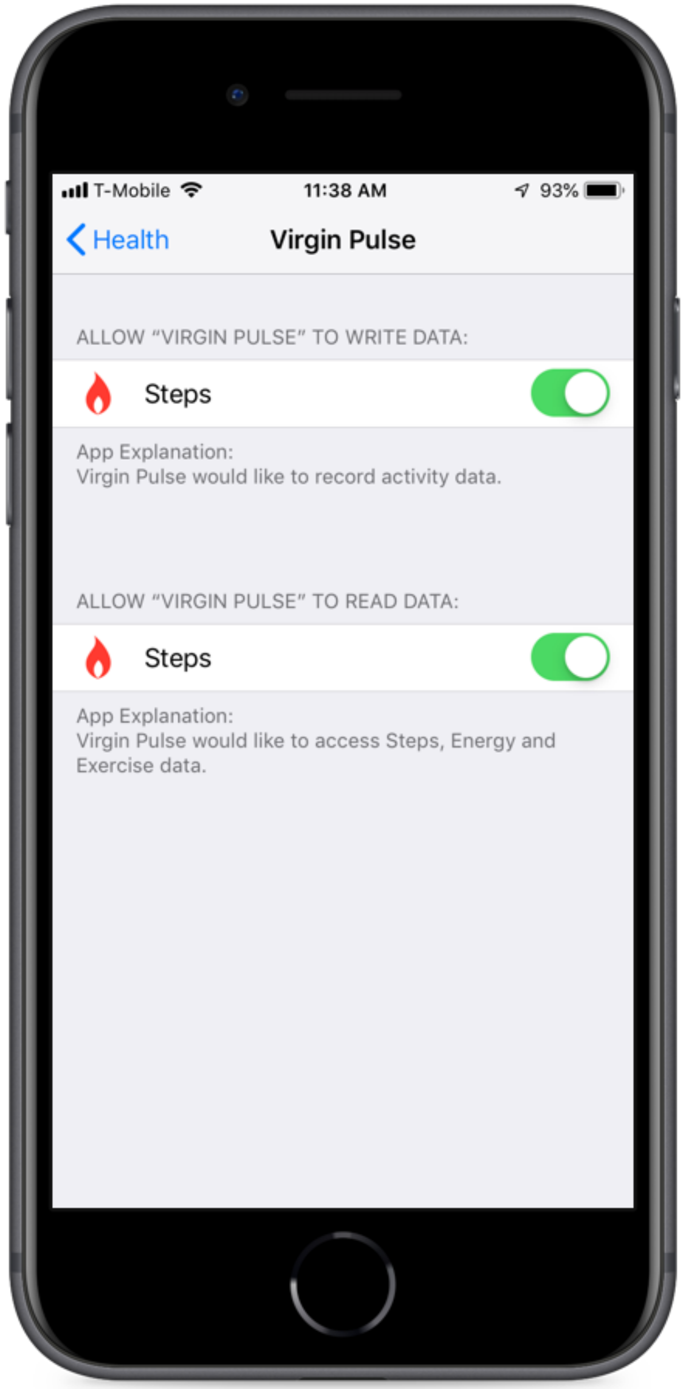
Advertisers who you've visited 0

Advertisers you've hidden

LinkedIn, Home Ownership Matters, Tien Store 5 and 35 others

See all

Example: Granular Privacy Controls



T-Mobile 11:38 AM 93%

‹ Health **Virgin Pulse**

ALLOW "VIRGIN PULSE" TO WRITE DATA:

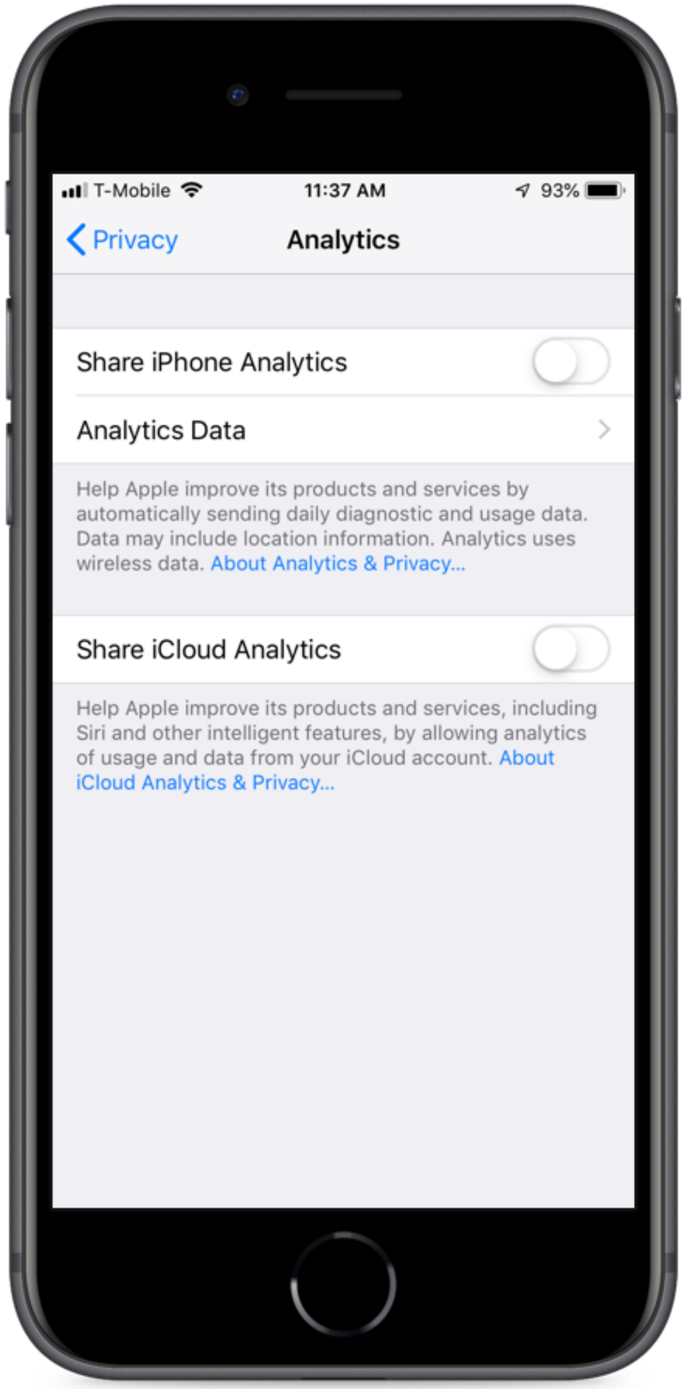
Steps ●

App Explanation:
Virgin Pulse would like to record activity data.

ALLOW "VIRGIN PULSE" TO READ DATA:

Steps ●

App Explanation:
Virgin Pulse would like to access Steps, Energy and Exercise data.



T-Mobile 11:37 AM 93%

‹ Privacy **Analytics**

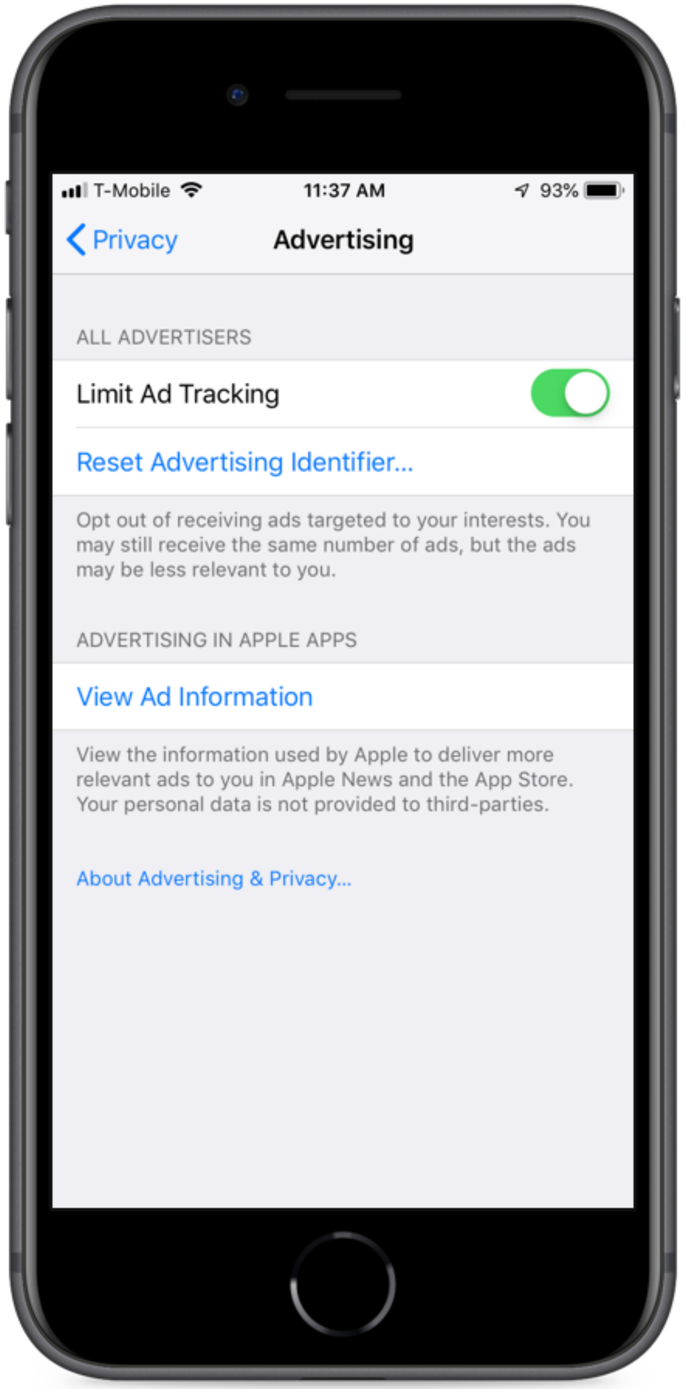
Share iPhone Analytics ○

Analytics Data ›

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Share iCloud Analytics ○

Help Apple improve its products and services, including Siri and other intelligent features, by allowing analytics of usage and data from your iCloud account. About iCloud Analytics & Privacy...



T-Mobile 11:37 AM 93%

‹ Privacy **Advertising**

ALL ADVERTISERS

Limit Ad Tracking ●

Reset Advertising Identifier...

Opt out of receiving ads targeted to your interests. You may still receive the same number of ads, but the ads may be less relevant to you.

ADVERTISING IN APPLE APPS

View Ad Information

View the information used by Apple to deliver more relevant ads to you in Apple News and the App Store. Your personal data is not provided to third-parties.

About Advertising & Privacy...

Let's Discuss:

A Truly Privacy-Focused Platform

Let’s Discuss:

A Truly Privacy-Focused Platform

This is a **platform-wide problem**. Privacy can’t be solved on individual features.

If we don’t plan and build for the platform now, we’re going to **fragment the experience further** in a really detrimental way.

This is a big swing. It’s a project on its own. And we have more just like it coming. It really can’t be handled by a single lane and successfully used across.

More Related Platform Problems

- Security presentation layer
- Privacy/data controls (in-feature and app settings)
- Communications traffic controller

I can dedicate design time to these problems, but we need to build them across the platform.

Another Item

- Improving lag time came up during the roadshow:
  - One participant works for a hospital group, gets instantaneous gaps confirmation from their EMR (through a few layers including Conifer Data Warehouse).
  - Employees are generally comfortable with this.
  - BUT they work for a healthcare organization. They’re experts and understand what’s happening.

- Wide EMR integration is probably a holy grail for us. Really hard, really expensive, really valuable.
  - There are vendors that can do this (Redox Engine).

See the results yourself:

Member Interviews: Gaps In Care (Confluence)