Health & Fitness Apps Privacy Overview

Learn how to protect your privacy when using third party health & fitness apps

September 2025

Contents

Introduction

At Apple, we believe that privacy is a fundamental human right. You should be in control of your personal and private data and have visibility over how it's used. Apple builds products that protect this data and put you in control over who you share it with.

Sharing data with third party health and fitness applications can be a great way to evaluate your well-being. But often, the information you choose to share with these apps is some of the most personal and private data you have. We have built several ways for users to understand, control, and protect how apps handle your private health data. In this document, we will cover what you should look for when downloading third party health and fitness applications, what controls you have over data you share with them, and how to update data sharing settings as you wish.

To start, it is important to understand that we design our products and services guided by our four key privacy principles:

Data minimization
We use innovative technologies and techniques to minimize the personal data that we, or anyone else, can access.

On-device processing
We process data on the device wherever possible, rather than sending it to Apple servers, to protect user privacy and minimize data collection.

Transparency and control
We help you better understand the data being collected so that you can make your own choices over who you share that data with and how it's used.

Security
We believe security protections, such as end-to-end encryption, are the foundation of privacy.

Using these four principles, Apple provides users with protections on all of our platforms across hardware, software and services. In addition to these built-in privacy protections, we want to ensure that users know how to fully take advantage of Apple's privacy tools.

Privacy Nutrition Labels on the App Store show you an easy-to-understand snapshot of an app's privacy practices, as reported by the app's developer.

App Tracking Transparency requires an app to ask you for your permission before it can track your activity across apps and websites. If you see a request to track your activity, you can tap Allow or Ask App Not to Track. You can still use the full capabilities of the app, regardless of whether you allow the app to track your activity.

How to understand information apps might collect

The App Store provides various ways for you to better understand a health and fitness app's privacy practices before you download the app onto an Apple device.

Privacy Nutrition Labels

Apple has implemented tools to help users easily locate and review apps' privacy policies to understand how their data may be used by an app developer. Starting with iOS 14.3 in December 2020, Apple launched a new privacy information section for product pages on the App Store called Privacy Nutrition Labels. This created an easy-to-understand system for all apps, where the information is self-reported by the developer. The privacy information section helps you understand an app's privacy practices on any Apple platform.

On each app's product page on the App Store, you can scroll down to the "App Privacy" section to learn about some of the data types the app may collect, and whether that data is linked to you or used to track you. You can learn about the different types of data an app might collect — including location, contact info, health info and more — and some of the ways the developer or its third party partners may use it, like for advertising or analytics.

App Privacy Report

With iOS 15.2 or later and iPadOS 15.2 or later, you can turn on App Privacy Report to see details about how often apps access your data — like your location, camera, microphone, and more. You can also see information about each app's network activity and website network activity, as well as the web domains that all apps contact most frequently. Together with Privacy Nutrition Labels, App Privacy Report helps give you a more complete picture of how the apps you use, like health or fitness apps, treat your data.

To access the App Privacy Report, go to the Settings app, select Privacy & Security, scroll to App Privacy Report, and choose to Turn On App Privacy Report.

App Tracking Transparency

Starting in iOS 14.5, iPadOS 14.5, and tvOS 14.5, apps must ask for permission before tracking your activity across other companies' apps and websites. Tracking occurs when information about you or your device collected from one app is linked with information about you or your device collected from other companies' apps, websites, and other locations, for the purposes of targeted advertising or advertising measurement, or when the information collected is shared with data brokers.

If you see a request to track your activity, you can tap "Allow" or "Ask App Not to Track." You can still use the full capabilities of the app, regardless of whether you allow the app to track your activity. You can change your choice at any time in Settings > Privacy & Security > Tracking, and choosing an option for each app that has requested to track. Alternatively, you can choose to universally allow or not allow tracking requests for all apps with "Allow Apps to Request to Track."

The app developer may choose to add a message in the request to explain why the app is asking to track your activity. You can also better understand how the app developer uses your data by viewing the app's Privacy Nutrition Labels located on the app's product page on the App Store.

If you choose Ask App Not to Track, the app developer won't be able to track you based on device details. The app is also not permitted to track your activity using other information that identifies you or your device, like your email address. Finally, any app that interacts with data from the Apple Health app is never allowed to use Health data for tracking purposes.

How to grant permissions to apps

Permissions to access your data
Apple gives you transparency and control over how you share your data with apps. Apps may request access to things such as your location, contacts, calendars, microphone, camera, photos, or Health app data. No app can access this data without your permission. You'll receive a prompt with an explanation the first time an app wants to access this data, so you can decide whether you want to grant it permission. Even if you grant access, you can always change it later in Settings > Privacy & Security.

For example, sometimes it may be useful for an app to know your location, such as in a fitness app. Apple gives you control over the collection and use of this location data on all your devices. Before the app can collect that data, you will receive a prompt explaining why the app needs the data, and you can choose to allow or not allow it to different degrees. Apple recognizes that location data, including, for example, a user's location when visiting a health provider, is some of your most sensitive data. Starting with iOS 14, iPadOS 14, and watchOS 7, you can choose whether apps have access to your approximate location — an area of about 10 square miles — rather than your precise location. Note that by default, your Location Service data is not shared with anyone, including Apple, and is disabled. You can enable it when you first set up your device, and you can always turn it off — or back on again — if you change your mind. You can grant location access to each individual app, and revoke it later in Settings > Privacy & Security > Location Services > app name. Or you can turn off location services for all apps at once when you go to Location Services.

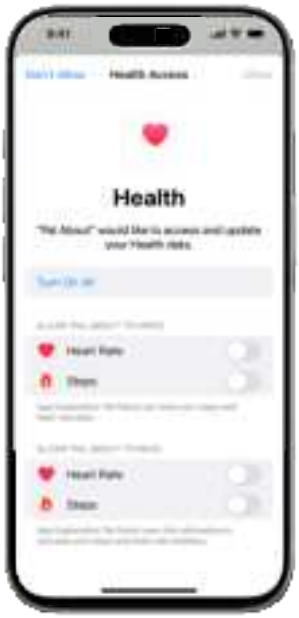
Permissions to access your Apple Health app data
Because health data can be sensitive, the Apple Health app provides you with fine-grained control over the information that you share with third party health and fitness apps. In addition to being encrypted, data in the Health app is only shared with apps when you give explicit permission for each data type.

The Apple Health app is designed with privacy in mind, so that apps can't see or add any Health data without your permission. Before accessing any data, apps must prompt you to access that specific type of Health app information, and you must affirmatively allow the access. You have control over precisely which Apple

Health data you want to share with a third party app. By default, no information is shared. If you choose to deny access to a type of data (like blood pressure, for example), the third party app cannot tell if you denied permission or if the data type does not exist in your Apple Health app. For example, a user can give an app access to their steps without giving access to their Cycle Tracking data, and the app would not know if the user is using the Health app to monitor their ovulation cycles. This is designed to prevent apps from inferring your health status by learning which types of data that you are logging. The Health app data that you choose to share is provided directly to the app, and Apple does not get access. If you later decide you don't want an app to access your Health app data, you can remove access at any time from Settings > Privacy & Security > Health.

Apps must meet certain criteria in order to request access to Health app data, medical data, and health research data. Health app data may only be requested by third parties that provide a health or fitness service. To access Health app data, all apps must provide an explanation at the time of the request explaining why they are requesting access to that data, and users can choose whether to grant or deny access to each data type.

Information that you choose to share with apps in the health, fitness, and medical research context may not be used for advertising, marketing, other use-based data mining purposes, or sold to data brokers. The data can only be used to improve health management, or for the purpose of health research, and then only with your permission. All apps must provide a privacy policy describing how you can revoke consent or request to delete your data.



Apps must ask for your permission before accessing your health data. You have granular controls over which health data types are shared with apps.

How to review and revoke permissions to access your data

It is important to periodically review access that you have granted to apps. You can do this by going into Settings > Privacy & Security, going through each data type and reviewing which apps you've granted access to. For example, you can go into the Health section to review a list of apps you have granted access to your Apple Health data, select one of those apps from the list, and either Turn Off All the Health selections, or remove individual Health items. Similarly, you could select Location Services under Privacy & Security, select an app from the list, and choose whether you want to allow that app to access your location; alternatively, you can disable Location Services altogether if that is what you choose, and that will disable access to your location to all apps and services on your device. There is no limit to your ability to enable and disable access to your data.

Safety Check is a feature available under Privacy & Security settings in the Settings app that allows you to quickly review, update, and stop sharing your information with apps. Safety Check allows you to manage sharing and access options so that you may review and make individual changes, or for you to use Emergency Reset to immediately stop sharing all information.

Conclusion

Information about your health and your location data is some of the most private and personal data on your device. At Apple, we believe everyone should have control over their health data, and have transparency around how apps might collect and use their data. Data protected in Apple's own Health app is encrypted by default on-device and inaccessible when locked with a passcode, Touch ID, or Face ID. Third party health apps may have different policies, so it's important to understand what information they are requesting, what their privacy policies are, what data they use, and then for you to make an informed choice on which apps you wish to download and use. You also have the ability to check your App Privacy Report to understand how frequently apps have been accessing your data, and you can review and revoke access to sharing data in the future with any apps at any time. To learn more about Apple's commitment to privacy, go to apple.com/privacy.

Steps you can take to protect your privacy

Understand what apps might collect
Tools like Privacy Nutrition Labels, App Privacy Report, and App Tracking Transparency can give you an idea of an app's privacy policies, and allow you to make an informed decision on what you wish to share.

Grant permissions that are right for you and your needs
Apps must request access to your data. You have the ability to choose whether to share that information or not.

Review and revoke permissions to access your data
It is important to review if you want to continue to grant apps access to your data. This is in your control, and you can revoke access at any time.