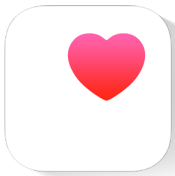


Health Privacy Overview

Learn how the Health app and HealthKit protect your privacy

May 2023

Contents

Introduction

The Health app makes it easy for you to access your health and fitness information and provides you with meaningful insights to live a healthier life. It brings together over 150 different types of health data from Apple Watch and iPhone, authorized third-party apps and devices, and connected healthcare providers. HealthKit securely stores your health and fitness information and lets you control each health data type read from and written to the Health app.

As people live more of their lives online, they're sharing more personal data than ever. The proliferation of data has been accompanied by a dramatic rise in attacks on data. The overwhelming majority of breaches involve sensitive personal information.

Nothing is more personal than your health information, so we built the Health app and HealthKit with privacy in mind from the beginning. Apple builds software that protects this data and puts you in control of which data is stored in the Health app and which data is shared with third-party apps and people you trust.

Privacy by design

There are four privacy principles that inform everything we do at Apple: data minimization, on-device processing, transparency and control, and security. We built each of these four pillars into our Health features from the beginning.

Data minimization

iOS minimizes the amount of health data sent to Apple's servers by generating health metrics on-device. For users with two-factor authentication, a device passcode, and a device running iOS 12 or later Health app data is end-to-end encrypted. As a result, data in the Health app is not readable by anyone - even Apple.

On-device processing

Data shown in the Health app like Trends & Highlights, resting heart rate, and Cycle Tracking predictions are calculated on-device. This on-device storage and computation helps ensure that Apple does not see this data in order to provide health metrics and summaries.

Transparency and control

Health data is sensitive, so we make sure you're in control of what data is shared, who it is shared with, and how it is used. You can view and control data sharing with friends, family, and healthcare providers in the Sharing tab of the Health app. Apps can request access to different types of data through HealthKit — and you can decide what data you want to share, if any.

Security

Health and fitness data gathered from iPhone and Apple Watch is encrypted on your device with a passcode, and is securely synced from Apple Watch to iPhone. As a result, data in the Health app is not readable by someone with physical access to your device unless they have your passcode. For users with

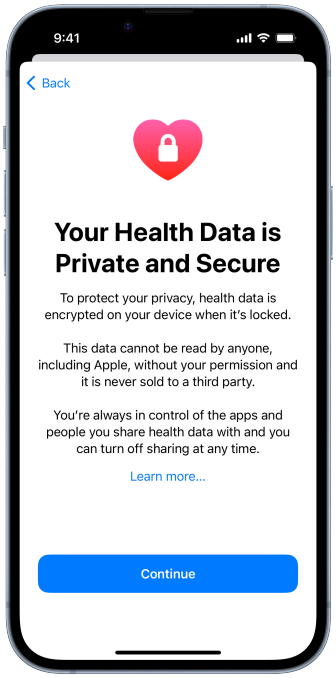
Apple's privacy principles

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

On-device processing
We minimize data collection by processing as much of your data on your device as we can, rather than sending it to a server.

Transparency & 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
Security protections, such as end-to-end encryption, are the foundation of privacy.



The first time that users with two-factor authentication and a passcode launch the Health app, they learn about how their data is protected.

two-factor authentication, a device passcode, and a device running iOS 12 or later data in the Health app is end-to-end encrypted when synced between devices. As a result, no one can view your Health data without your permission.

End-to-end encryption

What is end-to-end encryption?

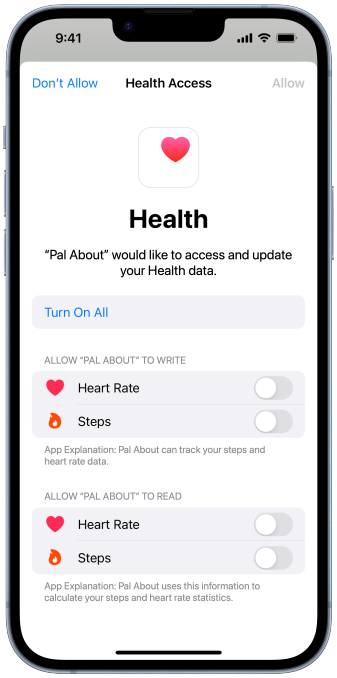
End-to-end encrypted data can be decrypted only on your trusted devices where you're signed in with your Apple ID. No one, not even Apple, can access your end-to-end encrypted data unless you choose to share it. If you lose access to your account, only you can recover this data, using your device passcode or password, recovery contact, or recovery key.

Health data, stored in HealthKit, is encrypted on-device and is only accessible with your passcode, Touch ID or Face ID. Medical ID is still available when your device is locked to help first responders access your critical medical information from the Lock Screen in an emergency. For users with two-factor authentication, a device passcode, and a device running iOS 12 or later - Health app data synced to iCloud is also not readable by Apple. As of August 2022, over 95% of active iCloud users have two-factor authentication enabled.

Syncing your Health app data

Health app data is also end-to-end encrypted when synced across your devices through iCloud. As a result, each of your devices will show the latest health and activity data without revealing your health information to Apple. You can choose to turn off syncing of Health app data in Settings > Apple ID > iCloud > Health.

Third-party app controls



Apps must ask for your permission before accessing your health data. You have granular controls over which health data types are shared with 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. Apps use HealthKit to ask your permission to access your Health information.

Apps can't see any Health app data, or add any data to the Health app, without your permission. Before accessing any data, apps have to prompt you to access Health app information. You have fine-grained control over precisely which Health app data you want to share with a third-party app. By default, no data is selected. If you deny access to a type of data, the app cannot tell if you denied permission or if the data type does not exist in your Health app. For example, a user can give an app access to their steps without giving access to their blood glucose levels, and the app would not know if any blood glucose data existed on the phone. 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 remove access to Health app data for a particular app in Privacy & Security settings, that app will no longer be able to read your Health data.

Requirements for apps using HealthKit

Apps must meet certain criteria in order to request access to Health app data through HealthKit, and these requirements are detailed in the App Store Review Guidelines and the Developer Program License Agreement. HealthKit information may only be requested by third parties that provide a health or fitness service, and you must give permission for your data to be shared. All apps must provide an explanation for why they are requesting Health app data that is shown to you at the time they request access. Information that you choose to share with apps through HealthKit may not be used for advertising, marketing, or sold to data

brokers. All apps integrating with HealthKit must provide a privacy policy describing how you can revoke consent or request to delete your data.

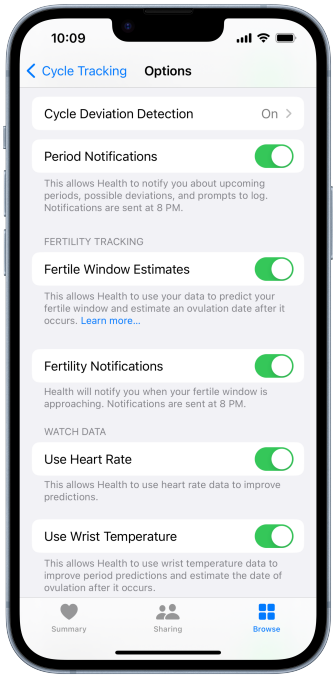
Cycle Tracking can use use wrist temperature and heart rate data from Apple Watch to improve predictions and provide retrospective ovulation estimates.

On-device processing and controls

In addition to storing encrypted Health app data in iCloud to support syncing across devices, Apple also minimizes how much health data is on Apple's servers. As a result, iPhone and Apple Watch generate the metrics shown in the Health app entirely on-device. Sensors built into Apple Watch, like the optical heart sensor, or built into iPhone, like the gyroscope, feed information to the operating system. The operating system then locally computes the health summaries stored in HealthKit and are ultimately shown to you on your Apple Watch and in the Health app.

You are able to turn off the computation of certain health metrics. For example, your iPhone gathers information from the gyroscope, accelerometer and barometer, and iOS then converts it to metrics like total steps and flights climbed. You are able to turn this off in Settings > Privacy & Security > Motion & Fitness > Fitness Tracking. In the Watch app, Settings > Privacy allows you to control how your watch sensors are used to calculate metrics in the Health app.

Another example of how data is processed on-device to generate user metrics is Cycle Tracking. If a user turns on period predictions, the operating system can use their logged period days to provide period predictions and fertile windows estimates. In addition to the user-logged information for previous periods and cycle length, the Health app can use sensor data from Apple Watch as part of its on-device calculations for Cycle Tracking. Heart rate data from Apple Watch can be used to improve Cycle Tracking predictions. Wrist temperature data from Apple Watch Series 8 or Apple Watch Ultra can be used to improve period predictions and provide retrospective ovulation estimates.



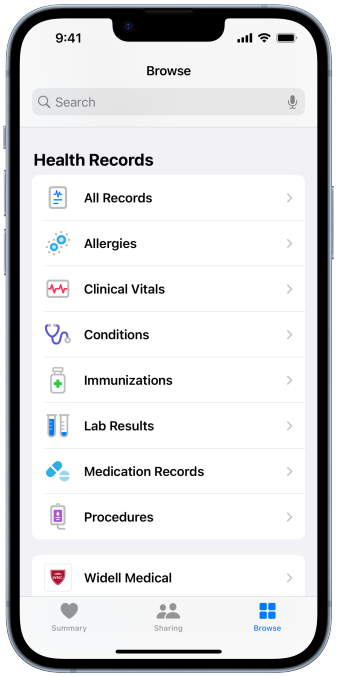
You can choose whether to include heart rate and wrist temperature data in the Cycle Tracking feature.

You are also able to control how these metrics are used in the Health app. Certain health summaries, like Sleep or Cycle Tracking, allow you to disable whether those metrics are used as part of the summary. For example, selecting the "Options" menu in the Cycle Tracking feature shows a set of toggles that control which data contributes to predictions.

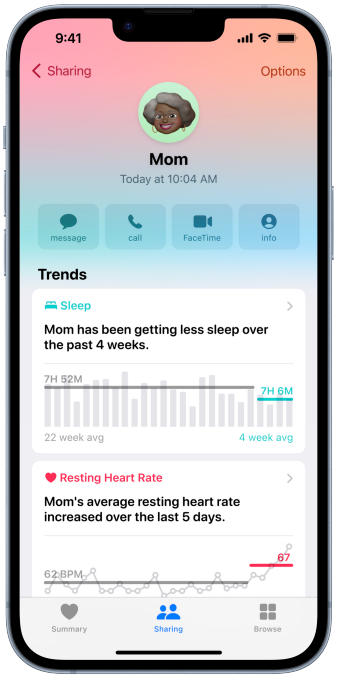
Health Records

You can use the Health Records feature on iPhone to view your health records from multiple institutions alongside the rest of your health information in the Health app. Health Records data is retrieved through a direct connection with the healthcare organizations, without any data being sent through Apple's servers.

Health Records data is encrypted in transit and at rest. To make this happen, Apple provides you with the ability to request and download your available health records using a direct and encrypted communication between your iPhone and the APIs provided by the health system or clinic. This transfer of health records data is encrypted and does not traverse Apple's network, and Apple does not maintain or have access to the encryption keys used to encrypt or decrypt your



You can import heath records from your healthcare provider into the Health app.



You can choose what types of Health data you want to share with friends or family.

health data. The analysis of any data contained in the health records, including images, is analyzed on-device. By default, Apple cannot access or view any health data stored in connection with Health Records on iPhone.

You can log into your patient portal directly from the Health app, and each of these portals is required to use OAuth 2.0. This enables you to authenticate once to create an ongoing connection to the Electronic Health Record APIs owned by your healthcare provider. The Health app then periodically calls these APIs to download new health records and update what's shown in the Health app. You can stop receiving health records from a health institution at any time by removing an account in the Health app. By removing the account, the records associated with that account will be deleted from your device. This also deletes the account and data from other devices where you are signed in to iCloud with the same Apple ID. The Health Records feature is available in Canada, United Kingdom, and the United States only.

Health Sharing

The Health app also helps you be more engaged in your health by providing optional ways to share your Health data with family and friends. You can choose to share data in the Health app with up to five people. You are in control of what data you share, and can change what you are sharing or stop sharing at any time.

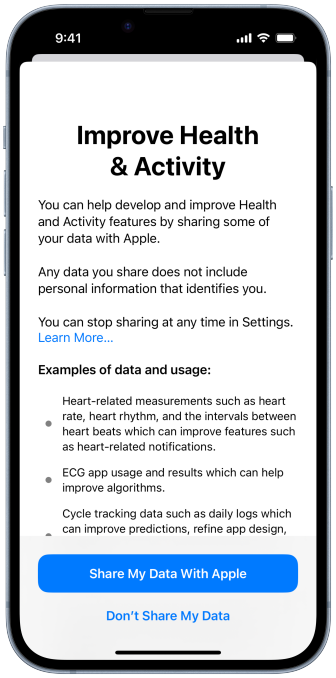
You can start sharing your Health data with one of your contacts in the Sharing tab of the Heath app. You can choose if you want to share when you receive an important Health alert, such as High Heart Rate or Noise notifications. You are also provided with fine-grained control over individual metrics you want to share that are available in the Health app, including activity, heart, and mobility metrics. If you choose to stop sharing your Health app data entirely, your Health app data is removed from the other person's device.

When Health app data is shared with another person from the Health app, the data remains end-to-end encrypted. Health Sharing encrypts the data to be shared so that only the person you're sharing with can read it.

Both the user choosing to share and the user receiving Health data need to have an iCloud account with two-factor authentication enabled, meaning that Health Sharing is only available when the data will remain end-to-end encrypted.

Sharing with healthcare providers

In addition to sharing with friends or family, you can choose to share certain Health app data with your health provider. The data is transmitted and stored by Apple such that the data you share with healthcare providers is end-to-end encrypted, meaning Apple doesn't have the ability to decrypt and view your health data. If you decide to stop sharing with a healthcare organization, the healthcare organization will no longer have access to your data through this feature. To learn more, see our whitepaper on the security and privacy of Health app data Share with Provider. Sharing Health app data with providers is available in the United States only.



If you have chosen to share iPhone analytics data with Apple, you will be additionally asked if you want to improve Health & Activity features.

Improve Health & Activity

You can also opt-in to share certain data with Apple to help improve Health and Activity features. If you have already chosen to share diagnostic data with Apple, you will be additionally asked if you want to improve Health & Activity. If you choose to share your data with Apple to help improve products, certain data such as activity, workout, and health-related information is sent to Apple solely to improve activity, fitness, and health features.

This data is not tied to your Apple ID, and is not shared with Apple unless you opt-in to Improve Health & Activity. Health and fitness data is aggregated in a way that does not personally identify you and analyzed on your iOS device and Apple Watch before being sent to Apple.

Conclusion

The Health app and HealthKit were designed with privacy in mind from the beginning, because we believe everyone should have control over their health data. Data protected by HealthKit — other than Medical ID — is encrypted and inaccessible by default on-device when locked with a passcode, Touch ID or Face ID. Additionally, if you have two-factor authentication enabled and sync Health app data to iCloud, it's encrypted end-to-end. You have controls over each type of health data you choose to share with apps, friends and family, and providers. iPhone and Apple Watch process data on-device for health metrics and summaries without sending any readable information to Apple. Data in the Health app is never shared with any third party without your explicit permission. To learn more about Apple's commitment to privacy, go to apple.com/privacy.