Your privacy: Microsoft Health and HealthVault FAQ

Microsoft account

Why do I need a Microsoft account?

Microsoft Health uses your Microsoft account in order to store your data in the cloud. Learn more about Using a Microsoft account with your Microsoft Band.

When I use Microsoft Band and Microsoft Health, what information is collected and where is it saved?

After you set up your Microsoft Band with Microsoft Health, it keeps track of your fitness data. Examples include heart rate, steps, and calories burned. Find out what data your Microsoft Band collects. See also Learn more about what sensors are on Microsoft Band.

Your Microsoft Health data is stored in the cloud, in the data center closest to you when you setup your account. Microsoft Health data centers are located in the United States, EU and Australia. No data is transferred to the cloud unless you pair your Microsoft Band via Bluetooth with Microsoft Health.

How do I delete my account?

To delete your data from the Microsoft Band and Microsoft Health, follow these steps:

1) On your Microsoft Band, tap the **Settings Tile >Power.** Then swipe left, tap **Reset Device**, and tap **Yes** when asked if you want to erase all data.
2) Open the Microsoft Health app, and tap **Expand >My Microsoft Band > Unregister your band.**

To delete the information from the Microsoft Health Service contact Customer support.

How is location and GPS used with Microsoft Band and Microsoft Health?

When you turn GPS on during distance travel activities like running, biking, or golfing, it records your route and collects info about the distance you've travelled. When you sync your Microsoft Band with your phone, you'll find a map of your route in the Microsoft Health app so you can retrace your favorite routes later.

GPS data is also used to refine distance and speed calculations. Learn more about using GPS mapping

Manage tiles and notifications on your Band

You can choose which tiles appear on your band and when they notify you. Some tiles have additional settings you can modify, so you can do things like turn notifications on or off, set up quick response messages, and more. Learn how to manage Tiles and Notifications.

Microsoft HealthVault

What are the Privacy principles for HealthVault?

Our privacy efforts are built on four core principles:

1. The HealthVault data you create in HealthVault is controlled by you.
2. You decide what goes into your HealthVault data.
3. You decide who can see and use your HealthVault data.
4. HealthVault does not use your health information other than to provide the Service unless you clearly tell us we may.

In addition to the core privacy principles listed above:

- HealthVault does not use your data to display advertising to you without your opt-in and explicit consent.
- You can see a history of what data has been added, updated, or deleted and by whom, for records where you are a custodian.
- Microsoft has established stringent privacy guidelines for Microsoft HealthVault.

Does Microsoft access my HealthVault data?

Microsoft may access and/or disclose your personal information in HealthVault:

- If you give us explicit consent, such as when you are working with Microsoft Customer Support to resolve certain issues
- If we believe such action is necessary to: (a) comply with the law or respond to legal process served on Microsoft; or (b) protect the rights or property of Microsoft (including the enforcement of our agreements).

By policy, access to the record database is limited to a small number of authorized personnel (whose access is audited) and only as needed to operate the service.

Does Microsoft collect health data about me from my health care providers?

Microsoft does not contact doctors, hospitals, insurers, or other entities to add data to your HealthVault records without your permission. Health information is only through connections that you, or people you authorize, specifically create.

How can I keep my data in HealthVault private?

You play an important role in protecting the privacy of your data.

- Use the additional security features with the ID you use to sign in to HealthVault, such as your Microsoft account (learn more) or Facebook ID (learn more). This can help protect your account from being accessed if somebody learns your account password.
- Use a password or passcode to secure any PC or mobile device (such as your phone) that has a HealthVault-connected app.
- Be thoughtful and careful about people you share your HealthVault records with and their level of access. Occasionally review who has access to your records, which you can do on the Sharing page when you're signed in to the HealthVault website.

You can find many tools and tips for protecting your data privacy at Microsoft.com/security.

What if someone gains access to my HealthVault account?

Microsoft is committed to protecting your privacy and helping consumers have a positive online experience. If we learn of any potential breach of a HealthVault account, we will investigate, and, where appropriate, take actions possibly including blocking or suspending access to your account.

If we determine there might have been a breach of your HealthVault account, we will notify you via the contact information you have provided in your account. We encourage you to provide alternate contact information, so that if your login ID is compromised or blocked, we will still be able to get in touch with you.

Where can I learn more about managing my HealthVault account? (how to close my account, edit contact information, etc.)

Learn more about managing your HealthVault account here.

How do I share my HealthVault data? How do I add a custodian to my record?

There are several ways to share your HealthVault data. You can give another HealthVault user online access to part or all of your HealthVault account, create an emergency profile, print information or use encrypted messaging. Learn more about Sharing Health Information.

HealthVault, HIPAA and government regulation compliance

Does HIPAA apply to HealthVault accounts?

HIPAA doesn't apply to HealthVault accounts. HIPAA is a U.S. law that regulates the data of healthcare providers, health insurers, and others in the healthcare industry.

HealthVault is, very simply, **a tool for individuals to manage health information that is under their control**. It is not a tool for healthcare companies to manage their patients' or insureds' data. Individuals, not hospitals or insurance companies, control how their information is used and shared. As a result, HIPAA does not apply (either under the rules for HIPAA covered entities or for their business associates).

What requirements do apply to HealthVault?

Microsoft operates HealthVault according to the commitments we make to HealthVault customers in our service agreement and privacy statement. In addition, for data collected in the US, the HITECH Act, a U.S. law that supplements HIPAA, regulates HealthVault as a personal health record. The HITECH Act requires, for example, that we notify you if a security breach compromises your HealthVault information.

HealthVault and Data Protection in the European Union

The European Union has strict rules about the use and disclosure of information regarding health. Microsoft Corporation as the data controller for HealthVault services is committed to follow those rules. Please see our Privacy Statement for information how to reach Microsoft.

If you choose to share your data with organizations that operate connected applications, those organizations can become data controllers for the services they provide. We recommend in that case that you review the privacy practices of those organizations.

HealthVault is designed to provide users with control over their personal information, flexible choices for how to use and share it, and the ability to maintain their health records independent of any particular healthcare provider.

A contract is required before an organization can connect its application with any HealthVault record. Microsoft requires certain technical and organizational measures from our partners as well as written security and privacy commitments in the agreement. The agreement recognizes that each party has a duty to protect the privacy, security and integrity of its users' data. Microsoft does not approve providers' privacy notices or generally review their practices, but does reserve the right to suspend or terminate connectivity if we become aware they may not be not fulfilling their privacy and security commitments to users.