Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet

Protecting Your Health Information

Your health information provides insight into the personal, often-sensitive details of your life. Protecting the privacy and security of this information, including what doctors you visit and what medical treatments or services you receive, allows you to control who has access to information about you, how much access they have, and when they have access. This enables you to protect yourself from potential discrimination, identity theft, or harm to your reputation.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules protect the privacy and security of your medical and other health information when it is transmitted or maintained by covered entities (health plans, most health care providers, health care clearinghouses) and business associates (people and companies that provide certain services for covered entities). This information is referred to as protected health information (PHI), and it includes individually identifying information, such as your name, address, age, social security number, and location, as well as information about your health history, any diagnoses or conditions, current health status, and more.

The HIPAA Rules generally *do not* protect the privacy or security of your health information when it is accessed through or stored on *your* personal cell phones or tablets. The HIPAA Rules apply only when PHI is created, received, maintained, or transmitted by covered entities and business associates. For example, the HIPAA Rules do not protect the privacy of your Internet search history, information you voluntarily share online, or your geographic location information. In most cases, unless the app is provided to you by a covered entity or its business associate - PDF, the HIPAA Rules also do not protect the privacy of data you've downloaded or entered into mobile apps for your personal use, regardless of where the information came from.

The information that your device or apps collect about you may be viewed or collected by other entities or used by the device or app vendors to send you specific ads. It may also be sold to a data broker, someone who obtains and shares consumer information without their knowledge, often selling it for marketing or other purposes.

Although the HIPAA Rules do not protect this information, there are steps that you can take to increase the privacy of your information when using your personal mobile device.

How can I keep data about my location and activity on my personal cell phone or tablet private?

It is not possible to eliminate your digital footprint entirely. But there are steps you can take to decrease how your cell phone or tablet collects and shares your health and other personal information, such as where you go and what you do, without your knowledge. In addition to these steps identified below, it is also prudent to:

- Avoid, in the first place, downloading unnecessary or random apps, especially those that are “free.”
- Avoid, when asked, giving any app permission to access your device’s location data, other than those apps where the location is absolutely necessary (*e.g.*, navigation and traffic apps). Many of the apps that resell data to data brokers don’t really need your location information.

To increase the privacy of information about your activities, your location, and the places you travel, you can turn off the location services on your personal cell phone or tablet. The instructions below should apply to most Apple iOS and Android devices, but older versions and hardware may be slightly different. In these instances, please use the links to Apple and Android privacy websites included at the end of each list.

On Apple iOS devices:

- Go to **Settings** -> **Privacy** -> **Location Services**.

Here, you can turn off access to **Location Services for** all apps. However, doing this may limit app functionality. For example, mapping apps will not know where you are, so you will need to enter in your location to get directions from where you are to

where you want to go. To turn off access to location information for apps individually, set **Allow Location Access** to **Never** for each app that you do not want to have access to your location.

- Go to **Settings** -> **Privacy** -> **Location Services** -> **System Services**.

Here, you can turn off location access for various system services. However, doing this may limit the functionality of your phone or tablet. For example, you may not be able to locate your device using Find My iPhone/iPad because it relies on location information to track your device. You can also view recorded location information and turn off the function that records the locations where the phone or tablet has been by going to **Significant Locations**. Here, you can also delete recorded location information by selecting **Clear History**.

- Go to **Settings** -> **Privacy** -> **Tracking**

Apple requires app developers to get your permission to track your activity across apps and websites to target advertising to you. To automatically deny app developer requests to track your activity, turn off **Allow Apps to Request to Track.** This will automatically deny all new requests for app tracking. However, Apple also retains its own settings related to targeted advertising. To turn off this function, go to **Settings** -> **Privacy** -> **Apple Advertising** and turn off **Personalized Ads**.

- Information from Apple regarding the privacy of your data on Apple devices is available at: https://www.apple.com/privacy/control.

On Android devices:

- Go to **Settings** (*i.e.*, the gear icon) -> **Location**

Set **Location** to “off.” Next, choose (depending on your version of Android) **Location Services** or **Advanced**. Here, you can turn off location access for various system services. However, doing this may limit the functionality of your phone or tablet.

- Go to **Settings** -> **Location** -> **App permission** or **App location permissions** (depending on your version of Android)

Here, you can view the list of apps that have access to your location information and turn off location access to apps individually. Select the app and choose **Don’t allow**.

However, turning off location access to the app may limit app functionality. For example, mapping apps will not know where you are, so you will need to enter your location to get directions from where you are to where you want to go.

- Go to **Settings** -> **Privacy** -> **Ads** -> **Delete advertising ID**

Third parties track your activities to deliver targeted advertising by using your advertising ID. You can delete your advertising ID to limit such tracking from here by tapping **Delete Advertising ID**. Earlier versions of Android may **not** include this capability. In these instances, you can go to **Settings** -> **Google** -> **Ads** -> **Reset advertising ID** and tap **OK** and enable **Opt out of Ads Personalization** to request that apps not track you.

- Information regarding the privacy of your data on Android devices is available at: https://www.android.com/safety.

For specific apps:

Individual apps may have collected information about your location and activities, including the name and location of your doctor's office and the time and date of any visits. For example, apps for social media, directions, and maps, and ride sharing often collect location or activity information. Apps that enable you to "check-in" may collect information on the location, date, and time of your visit, as well as your name and other identifying information. By using such apps, you often give them permission to not only collect the information, but also to share the information with others, including data brokers, advertisers, or law enforcement. Consider logging into those apps or going to the app vendor's website and searching available help or support functions to figure out how you can delete your location and/or activity history.

What else can I do to keep personal and health information on my personal cell phone or tablet private?

In addition to tracking your location and activities, your device or your cellular service provider may store communications you send and receive on your personal cell phone or tablet, such as information on who and what you text, who you called, who called you, when you made and received calls, and in the case of a smartphone, who and what you email. To increase your privacy, consider using communication apps, mobile web browsers, and search engines that are recognized as supporting

increased privacy and security. For example, the Federal Trade Commission has published resources on how to protect your privacy when using apps at https://consumer.ftc.gov/articles/how-protect-your-privacy-apps. Also, Consumer Reports publishes reviews of the data practices of electronic products at https://www.consumerreports.org/issue/data-privacy. To identify apps with an increased focus on privacy and security, look for ones that do the following:

- Use strong encryption by default when transmitting data.
- Enable technologies to limit or block tracking tools, such as cookies and web trackers. (Tracking tools collect information about what you do online, such as who you are and which websites you visit.)
- Do not collect and store personal information.

If I follow all of these steps, will the location and activity data from my personal cell phone or tablet be unavailable to anyone other than me?

Unfortunately, no. Although the steps described above can reduce your digital footprint, it will not eliminate it. The very nature of cell phones (and some tablets) permits tracking because your cellular service provider's network records identifying information (such as subscriber and device information) when you are connected to it. This connects subscriber and device data to cell tower locations, creating a digital trail of your location as you travel and your device connects to new cell towers along the way.

Ultimately, the best way to protect your health and personal information from being collected and shared by your personal cell phone or tablet without your knowledge is to limit what personal information you send and store on or through the device. If you are concerned about your cell phone or tablet tracking your location and activities, consider leaving the device at home.

Finally, before disposing of an old cell phone or tablet, you should take **all** of these steps to protect the privacy of your health and personal information:

- Securely delete all stored data on it.
- Remove and destroy the SIM card if you do not plan to re-use it in another device.
- Recycle the cell phone at an appropriate electronic recycling location.

Additional Resources:

- FCC’s Protecting Your Privacy: Phone and Cable Records
  - https://www.fcc.gov/consumers/guides/protecting-your-privacy
- FTC’s How to Protect Your Phone and the Data on It
  - https://consumer.ftc.gov/articles/how-protect-your-phone-data-it
- FTC’s What to Know About Medical Identity Theft
  - https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft
- NSA’s Limiting Location Data Exposure
  - https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF
- ONC’s How Can You Protect and Security Health Information When Using a Mobile Device
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device
- Electronic Frontier Foundation (EFF) Surveillance Security Scenarios
  - https://ssd.eff.org/module-categories/security-scenarios
- Consumer Reports website on consumer data privacy
  - https://www.consumerreports.org/issue/data-privacy
- New York Times 3 Steps to Protect Your Phone
  - https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-privacy-tips.html
- Washington Post series, Your Data and Privacy
  - https://www.washingtonpost.com/personal-tech/data-privacy

Footnotes 1. This guidance addresses smartphones, other cellular (cell) phones, and tablets used for an individual’s own purposes. This guidance does not address other devices, such as smartwatches or fitness trackers, which may also collect or store information about your location, nor does it address email.

Content created by Office for Civil Rights (OCR)
Content last reviewed June 29, 2022

Article Source
U.S. Department of Health and Human Services
Source URL
https://www.hhs.gov
Last Reviewed
Friday, July 1, 2022