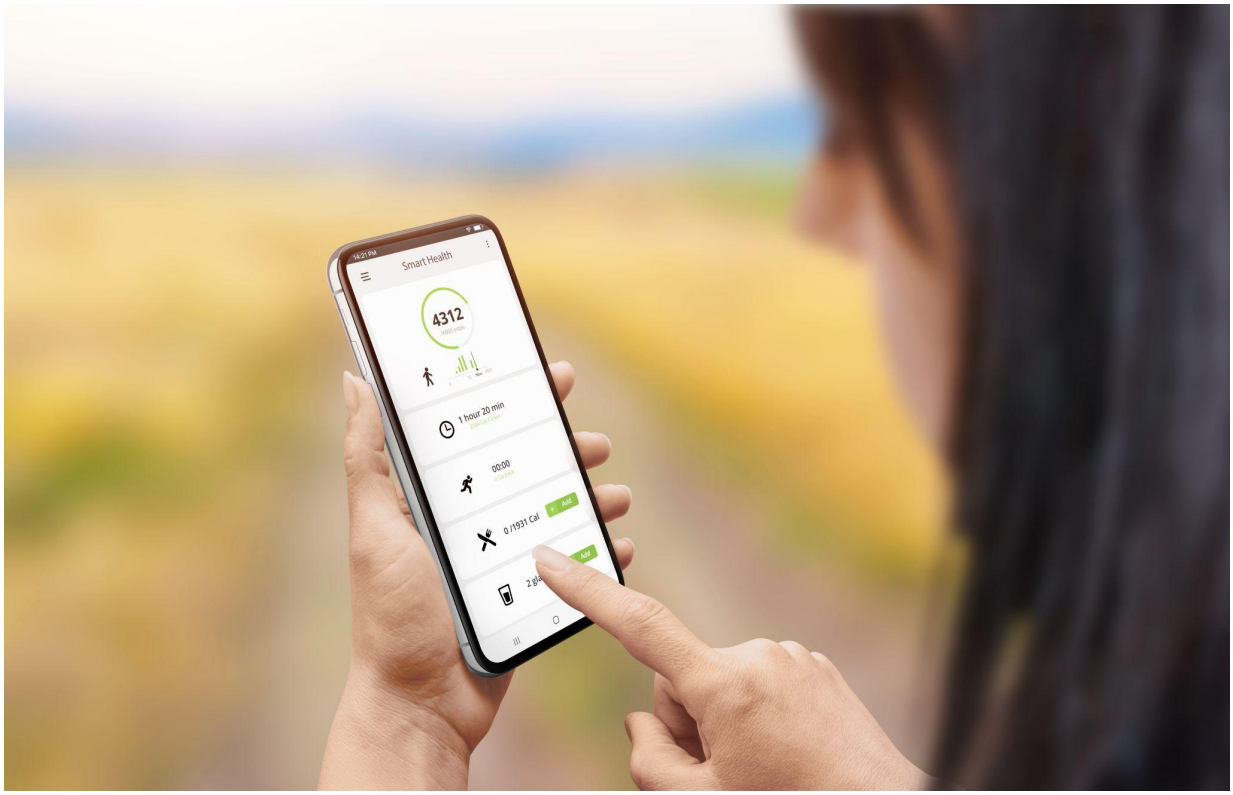
Are Health Apps Really Safe?



Health tracking apps are growing in popularity as they offer a convenient way for people to take charge of their health, even while on the go.

According to a report by the IQVIA Institute for Human Data Science, more than 90,000 new digital health apps hit the market in 2020, with 110 apps downloaded more than 10,000 times.

In America alone, 45% of people have used products like digital health apps and fitness trackers, according to research company, Gallup.

Health apps cover a diverse range of categories from women's health, to exercise, diet, and wellness apps. These apps make it easy for people to track their health status, or access health and wellness advice online.

Most of these apps require you to submit sensitive information regarding your health, financial status, weight, address, and other personal information in order to function properly.

But how safe are these apps? How do you protect your privacy in the age of information? We discuss this in greater detail below.

Can You Trust Health Apps?

According to a report published by Mozilla, 18 out of the 25 most popular reproductive and period tracking health apps share your data, without including a privacy warning. This is a particular concern in the wake of Roe and Wade where women can be prosecuted for having an abortion. Police can use the information from reproductive apps to build their case.

However, these are not the only health apps that have been reported to either leak or share data, as mental health and wellbeing apps were also found to have data breaches.

The problem is not just confined to a few data breaches either. A 2020 Security Report on Global mHealth Apps revealed that the majority (71%) of healthcare and medical apps have at least one serious vulnerability that could lead to a breach of medical data. It also found that 91% of the apps had a very serious security flaw.

Many app providers claim that their data is encrypted and not shared with any third parties. But how much can this be trusted?

In an interview published by CBC, Ann Cavoukian, a former Ontario privacy commissioner and founder of the International Council on Global Privacy and Security by Design, said:

“Simply, do not trust what companies are doing with your data. They may claim to protect your privacy, not store any of your digital data, or share it with anybody, but again and again, we've seen that they've been proven wrong. They often share it with unauthorized third parties in ways that you have not consented to."

Of course, health apps are not the only platforms that have experienced data breaches and security flaws. This issue has been reported across many different apps and websites.

However, health information is among the most sensitive personal data that we can provide about ourselves and can potentially impact insurance claims, welfare provisions, employment, and even legal proceedings.

Moreover, when the state can build a case against you on the basis of your health data and insurance companies can use it to determine any payouts, protecting your privacy is not just desirable, it is mandatory.

The Impact Of Data Breaches

So what are the consequences of data breaches? Data sharing appears to be a part of modern life. Indeed, some of the core functionality of health apps may mean that some data sharing is necessary, especially in the case of prescriptions or connecting with health practitioners.

But ignoring unauthorized data sharing or leaks is simply not an option. Here are just a few of the consequences associated with privacy breaches:

Legal Consequences

We already mentioned that in some cases, reproductive health data can help prosecutors to build their case against a woman suspected of having an illegal abortion.

But this is not just limited to reproductive apps. For example, insurance companies can potentially use your previous health data to refuse your insurance claim.

Mental health apps can be subpoenaed to build a case against you in criminal or even financial proceedings. In extreme cases, there have been reports of sexual assault victims having their mobile data analysed and used against them when reporting attacks against them.

In fact, there are a variety of unintended ways that health data can be weaponized against you when it comes to legal proceedings.

Intrusive Ads

Have you ever been at the receiving end of creepy ads that follow you around the internet? Ever wondered where they got hold of your data?

A new study from research group the Light Collective revealed that many healthcare apps are secretly sharing your digital information with Facebook. That information is then used to generate business and advertise personalized services to you.

This raises concerns about HIPAA violations and is just one example of the ways that your personal data can be used to generate intrusive ads that monitor your online activities in very invasive ways.

Your Data is Leaked to Unknown Third Parties

Your data could be in the hands of any third party with the money to purchase it. That is a sobering thought. While healthcare providers are bound by laws that enforce patient-doctor confidentiality, healthcare apps are like the wild west where there is very little regulation.

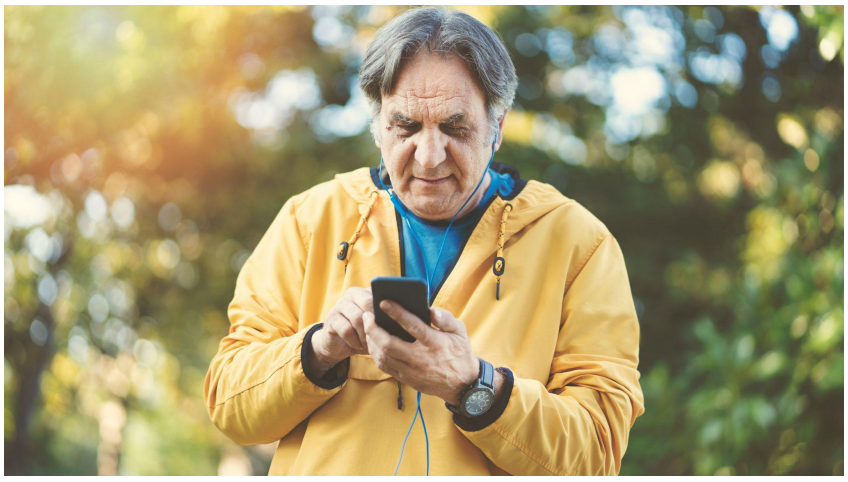
In 2019 alone, more than 25 million files were leaked in one of the biggest healthcare breaches of that year. Not knowing who has access to this highly sensitive information is something that should concern us all.

Misuse of Data

These data breaches could potentially make you vulnerable to hackers or criminals that can use your data to commit identity theft, access your financial data, commit insurance fraud or illegally order medication, or equipment.

This could not only end up costing you a fortune, it may also open you up to legal consequences.

Should You Use Health Apps?



In light of these revelations, it is understandable that some may hesitate to use health apps at all. For example, some experts have advised women to delete period tracking apps in the wake of Woe and Rade.

So is the answer as simple as simply refusing to use these apps?

The problem is that for those that rely on these apps for family planning, health tracking, or managing prescriptions, the problem is a little more complex than simply deleting apps that can play an important role in managing your health.

These apps can help to ensure that you take your medicines on time, get access to therapists and health providers, or influence your day-to-day dietary, and exercise habits.

It is also worth noting that any app can potentially leak your data or share it with third parties without your consent. This includes other sensitive apps such as banking apps or location tracking apps.

Deleting every app in the hopes that you will preserve your privacy is simply unrealistic in the age of the internet where much of what we do is online.

The key to safeguarding your app is to ensure that the platforms we use are as safe as possible.

Tips To Protect Your Privacy

Thankfully, there are many ways to protect your privacy and safeguard your health data.

Here are some of the main ways:

Be Selective With Your Health Apps

Take the time to research any health apps before downloading them. Pay particular attention to their privacy policies. You can also ask your healthcare provider or wellness expert for their advice on what apps to use. These apps are more likely to adhere to guidelines and data protection laws if they are recommended by reputable sources.

Look for apps that encrypt your data and only choose apps that specifically state that they will give you the option of storing information locally on your phone.

Check Privacy And Share Settings

Many health apps have privacy and share settings that allow you to restrict the information that is shared with third parties. Always take the time to review these settings carefully and ensure that your account is set to private.

Download Mobile Anti-virus

To protect your device against data harvesting malware, you should definitely consider downloading mobile anti-virus software such as Norton 360, which can help protect against a variety of online threats. It also includes additional security features such as a Wi-Fi analyzer and ad blocker. Norton is a great tool for learning where your details are being shared or

abused.

Monitor Online Security

Another way to safeguard your privacy is to regularly review your online information, credit reports, and online security. Thankfully, there are many tools that allow you to do this. LifeLock, a Norton 360 partner has a number of packages that all offer enhanced protection, and innovative monitoring technology designed to safeguard your online details. Currently, we are offering a promotion that offers you 25% off your first year.

Protect Your Online Privacy

Lifelock protects user devices, using real-time threat protection, a private VPN, and more.

We will send you alerts for potential identity theft by text, phone, email or mobile app. Should you ever be unfortunate enough to be a victim of identity theft, we will appoint a US-Based Identity Restoration Specialist who will personally manage your case.

Get started with protecting your online privacy today and click here to take advantage of our online offer before it closes.