Tips to keep your personal health information safe

By Julia Haskins

Your personal health information is a great resource for keeping tabs on your health and wellness. There are many benefits to accessing personal health information, such as your medical history, insurance information and test results, says Lana Moriarty, MPH, director of the Office of Consumer eHealth at the Office of the National Coordinator for Health Information Technology.

Reviewing your personal health information can help you make better decisions about your health, coordinate with your family and members of your care team and cut down on unnecessary testing and procedures, she notes.

Your personal health information tells a lot about you, which is why it's so important to keep these records private and only share them with trusted sources. Some simple measures can help you ensure that your health information stays in good hands.

Do you know that you have the right to access your personal health information and know who else has seen it? Thanks to a U.S. law called the Health Insurance Portability and Accountability Act, you can control how you receive your personal health information and who you want to view it. This is helpful for correcting any errors and making sure that your records are up to date.

For the most part, you can decide who gets to see your personal health information. There are some people and groups, such as your employer, that can't view this data without your permission. Knowing your rights under the law can help you take control of your personal health info and keep it safe.

There are many different ways to review your health information quickly and easily, but they all come with some risk.

When you request your health information from a health care provider, make sure that you know the risks involved and how to keep them at a minimum.

You may have a digital patient portal through your doctor's office, for example. Providers work hard to keep the data stored in these portals secure, but you can take extra steps to be more cautious. Moriarty recommends creating strong, unique passwords for each platform you use to access your health information.

You can download a password manager that will encrypt and store your passwords or create a new complex password each time you log in to a platform.

If possible, use two-factor authentication for passwords, says Margeaux Akazawa, MPH, public health analyst at the Office of the National Coordinator for Health Information Technology.

That means logging into your device with two different forms of verification. For example, you can receive a confirmation code via text message after logging into an online portal with your password. With two-factor authentication, you have another layer of security if a breach happens.

Another point to keep in mind is safe internet access. Moriarty advises against using public computers and Wi-Fi when looking at your health information. It's always better to use your own device with a secure, password-protected network.

Many people also use apps on their phones or tablets that store certain health information about fitness, nutrition and other health goals. An app to keep track of your daily exercise regimen may look harmless, but how can you be sure? Always thoroughly research an app before purchasing or downloading it, Akazawa says. Look at the app's privacy policy and terms and conditions.

You may be surprised to find that an app can tap into your contacts, share your location or connect to your camera. It could even be selling your data to advertisers. All those possibilities could put your personal health information in the wrong hands. If it seems like an app is doing more than just logging your steps each day, consider deleting it from your device.

You may not realize it, but you probably have lots of documents that also count as personal health information. Even if it doesn't come directly from your doctor, certain info shouldn't be public knowledge, Akazawa says.

Everyday health-related information such as a receipt for a prescription shouldn't be tossed in a public trash can. Instead, shred all health-related documents with personally identifiable information before recycling them.
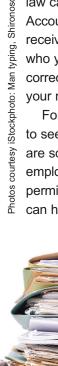
If you want to keep paper copies of your personal health information on hand, make sure that these documents are organized and stored in a secure place in your home, such as a locked file cabinet, Moriarty recommends.

>> For more, visit www.healthit.gov

Be careful on social media

It's easy to get carried away on social media, sharing details of your life with friends and family. But do you really need to broadcast every last doctor's visit? Remember that even if your social media account is private, the information that you share may not stay that way. So think before you post, snap or tweet.

Once you've shared something, there's no way to be sure that the people who can see it won't misuse it or that it won't go outside your circle of contacts.