WV Executive Branch Privacy Tip

Wearable Fitness Trackers & Apps– What's the Risk?

As you know, the Privacy Office occasionally issues tips to assist you in making informed decisions in your "away from work" life. This tip is for that purpose.

Fitness trackers (such as a Fitbit) can help you take steps towards a healthier lifestyle. Many users of fitness trackers and health and wellness apps grant access to personal data without even considering the security and privacy implications.

Here are some privacy and data security issues that you should consider:

> **1. Can your data be shared with or sold to third parties? Will the third parties ensure your data is safe?**
>
> Many fitness trackers' privacy policies are vague with "We respect your privacy" and end with "We ***may*** share your information with third parties…" which means they might share your sensitive medical data without your permission. Many privacy policies indicate that they "protect your personal information from unauthorized access, use, or disclosure," but what does that really mean? Do they encrypt the information? Do they review who has access to it?
>
> **2. HIPAA can't help**
>
> With the amount of health data these devices and apps track and store, it is not formally considered Protected Health Information (PHI) unless it's shared with a doctor, hospital, or other covered entities or business associates. Therefore, they are not subject to HIPAA regulations. Your PHI could be shared with a third party for marketing, such as for sleeping pills if your device shows you have trouble sleeping.
>
> **3. Default privacy settings - Public-by-default**
>
> These apps also have a social networking aspect, and you can choose to publicize and share your information with others. Unfortunately, many times the default privacy setting is public, allowing your info to be found in search results. Always make sure you triple-check all of the default privacy settings and turn off anything you don't want to share publicly.

You should always read the device manufacturer's and the app developer's privacy policies. Yes, they are long and sometimes difficult to understand, but making sure that there actually IS a privacy policy is as sometimes as important as reading it. If you can't find the privacy policy, you may want to think twice about handing over your personal information.

The bottom line is, use basic privacy and security precautions. Password protect your device and app with a strong password. Don't leave your Wi-Fi and Bluetooth active all the time. Be careful what you share on social media. Fitness trackers and apps can be beneficial for your health if you take a few minutes to protect your information.

For additional tips, check out the Online Trust Alliance:
https://otalliance.org/system/files/files/initiative/documents/smartdevice-securityprivacy-checklist.pdf

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*