



Tips to Protect Your Health Data This Holiday Season

HIPAA Rules Don't Always Apply to Apps You Download on Your Phone or Tablet.

Chicago, IL, Nov 4, 2022 (GLOBE NEWSWIRE) -- Wearables like FitBit, smart watches, smart or connected health monitoring devices and their associated apps are popular holiday gifts that collect and store your health data. Despite stringent privacy laws intended to safeguard your personal health information (PHI), data breaches are on the rise and can lead to everything from medical identity theft to billing fraud to blackmail. The Health Insurance Portability and Accountability Act (HIPAA) [doesn't cover everything](#).

A 2021 investigation by [Consumer Reports](#) found that privacy policies for a number of companies behind health apps left open questions about their privacy practices, and recent [research](#) indicates end users do not have full awareness of what their consent entails.

This holiday season, as part of their *Better Health is in Your Hands*™ campaign, the American Health Information Management Association (AHIMA) Foundation, shares tips and a [new animated video](#) that walks consumers through the steps to protect the privacy and security of health information on their personal cell phone or tablet.

“Your personal health data may include individually identifying information, such as your name, address, age, social security number, and location, as well as the places you travel, what doctors you visit and for what medical treatments or services, any diagnoses or conditions, current health status, and more,” said Anisa Tootla, AHIMA Foundation Executive Director. “And if you are setting up a new device for yourself or helping a loved one or are getting rid of an old one, there are ways to reduce privacy and security risks associated with your health information.”

1. **Turn off the location services on your personal cell phone or tablet.** This increases the privacy of information about your activities, your location, and the places you travel.
2. **Avoid 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).
3. **Use adequate security to send or receive health information over public Wi-Fi networks.** Open Wi-Fi networks at airports and other public locations can be an easy way for unauthorized users to intercept your information. Also be aware of any Bluetooth connections that you establish, like that rental car you authorized to use your phone.
4. **Delete all stored health information before discarding or reusing the mobile device.** When you use software tools that thoroughly delete (or wipe) data stored on a mobile device before discarding or reusing the device, you can protect and secure health information from unauthorized access.

5. **Avoid downloading unnecessary or random apps, especially those that are “free.”** In general, a free app is likely to include a lot of advertising and is therefore more likely to share your personal information with advertisers than a paid app.

As an enterprise, AHIMA is actively advocating for privacy policies to ensure appropriate protections are put in place when health information is gathered and shared by [entities not covered by HIPAA](#).



About AHIMA Foundation:

AHIMA Foundation is a 501(c)(3) nonprofit organization and philanthropic arm of the American Health Information Management Association (AHIMA) dedicated to empowering people with health information literacy to achieve better health outcomes. Founded in 1962, AHIMA Foundation programs, research, and projects help families make informed health decisions, guide evidence-based healthcare system policies and practices, and educate and train aspiring and current health information professionals. Recognizing that health information is human information, AHIMA Foundation works extensively to convene interdisciplinary stakeholders to identify unmet public health and education needs. Learn more at [AHIMAFoundation.org](https://www.ahimafoundation.org) and follow on [Facebook](#), [Twitter](#), [LinkedIn](#), and [YouTube](#).

Published 11/04/2022

Last Updated 11/07/2022

Source AHIMA Foundation (Copyright © 2022)