

Privacy Resources for Digital Health Data



What your users may do to address digital health data privacy concerns

Users with privacy concerns for their digital health data who download and use apps and fitness trackers that collect and store digital health data may refer to the following resources for additional privacy guidance.



BEFORE DOWNLOADING AN APP OR USING A PRODUCT/SERVICE

- [Review](#) this consumer product guide explaining data collection, security and transfer practices of apps and smart devices.
- [Read](#) this article for privacy assessments of reproductive health apps.
- [Review](#) information and guides from software companies like [Apple](#) and [Android](#), for help understanding app store privacy ratings and nutrition labels.
- [Read](#) this guidance from the Department of Health and Human Services to learn about geolocation tracking on mobile apps.

WHILE USING AN APP, SERVICE OR PRODUCT

- [Read](#) this article to learn how ad blockers and browser extensions provide greater privacy protections when searching for health data or other sensitive information.
 - This article on incognito mode [provides](#) further guidance.
- [Check](#) this list for encrypted messaging apps to use for private conversations.
- [Take](#) these actions to protect reproductive health data.
 - Review this step-by-step guide to [enable](#) secure access for a popular fertility tracking app.
- [Read](#) this explanation of the Global Privacy Control to opt out of tracking.



AFTER DELETING AN APP OR HALTING USE OF A PRODUCT/SERVICE

- [See](#) if your state recognizes consumers' "right to delete."
- See if your state recognizes universal opt-out requests: [California](#), [Virginia](#), [Colorado](#), and [Montana](#).
- [Follow](#) these steps to request a company delete your personal data.



Here's what you can do to protect digital health data

The following is a nonexhaustive list of third-party resources, frameworks and guidance organizations can consider when increasing protections for products and services that collect, use and/or sell digital health data.

TO CONDUCT DATA ASSESSMENTS

- [Review](#) this guide to the EU General Data Protection Regulation from the French data protection agency, the Commission nationale de l'informatique et des libertés.
- [Read](#) the final Proposed Consumer Privacy Framework for Health Data from the Center for Democracy and Technology and eHealth Initiative.
- Download the HHS' Security Risk Assessment tool for Health Insurance Portability and Accountability Act-covered entities and business associates to determine whether any protected health information could be at risk.



TO UNDERSTAND YOUR ORGANIZATION'S DATA AND ITS USE

- [Learn](#) the principle of data minimization from the U.K. Information Commissioner's Office.
- [Take](#) these steps to protect health data for technology companies.
 - Health care entities can also [take](#) steps to mitigate risk.
- [Learn](#) the best practices for data retention policies.
- [Gain](#) a better understanding of the impact of user trust from this report.

TO FAMILIARIZE YOUR ORGANIZATION WITH SECTOR-SPECIFIC LAWS AND REGULATIONS

- [Review](#) the Federal Trade Commission's key considerations for health app developers.
 - This interactive tool [provides](#) further guidance.
- [Read](#) the HHS' incidental disclosure precautions.
- [Learn](#) about the FTC's Health Breach Notification Rule.

