Best Practices for Consumer Wearables & Wellness Apps & Devices

August 17, 2016

The *Best Practices for Consumer Wearables & Wellness Apps & Devices* was produced with support from the Robert Wood Johnson Foundation.

Highlights

Providing Consumer Choices

1. Opt-in consent for sharing with third parties
2. Ban on sharing with data brokers, information resellers, and ad networks
3. Opt-outs for tailored first-party advertisements
4. Access, correction, and deletion rights
5. Enhanced notice and express consent for incompatible secondary uses

Supporting Interoperability

6. Compatible with global privacy frameworks
7. Supports compliance with leading app platform standards

Elevating Data Norms

8. Supports sharing data for scientific research with informed consent
9. Strong de-identification standard
10. Strong data security requirements

TABLE OF CONTENTS

Introduction 1

I. Definitions 4

II. Notice/Transparency 5

III. Choice/Consent 6

IV. Advertising 6

V. Limitation on Collection and Uses 7

VI. Sharing 7

VII. Access, Accuracy, Correction, & Deletion 8

VIII. Limited Retention 9

IX. Data Security 9

X. Accountability & Enforcement 9

About FPF 11

BEST PRACTICES FOR CONSUMER WEARABLES & WELLNESS APPS & DEVICES

Wearable and mobile devices and related apps and services ("Wearables") that help users track physiological information hold the potential to greatly improve consumers' lives. Wearables deploy sensors to collect environmental, behavioral, and social data for and from their users. Consumer-generated data from these devices is already generating substantial benefits for users, helping individuals manage their fitness, exercise, and biofeedback; improving personal productivity and efficiency; and making other technologies simpler and easier to use. Research based on data collected by wearables could reveal insights that could provide broad societal benefits.

This same data, if not properly protected, or if used in unethical or illegal ways, could be used to put individuals' privacy at risk. Critics worry that users could find themselves unfairly discriminated against by employers or insurers on the basis of their self-generated information, or have their reputations damaged or their safety put at risk by a data breach.

Given the potential benefits that wearables and consumer-generated wellness data may provide to consumers and society, it is important that this data be subject to privacy controls and be used responsibly. Many leading wearables providers and app developers have already set clear parameters for the collection and use of consumer-generated wellness data. Platforms and devices that enable third-party apps or services to access data have also set forward terms for how those apps or services may use data collected via those devices or platforms.

It is important to note that in many areas data collected by wearables is also subject to other legal protections. In the U.S., this includes sector-specific legislation such as COPPA, FCRA, or the ADA, as well as federal and state laws governing insurance and illegal discrimination.[1] In many cases, personal wellness information is covered by the Health Insurance Portability and Accountability Act (HIPAA), which imposes certain privacy and security requirements on healthcare providers and their business associates. Medical devices that can be worn or carried like a consumer wearable are also regulated for safety by the FDA.[2] Where health-related information or tools falls outside of these laws, they may also be governed by state and federal consumer protection laws.

However, many wearables collect data that will be unlikely to be covered by specific sectoral protections. Sometimes this data will be of low sensitivity and of the sort that some users will share publicly or with friends. Other times the data will be of the sort that can reveal highly sensitive facts about users and is information users will expect to be treated confidentially. Depending on the type of app and the types of uses, the same data may be subject to very different user expectations. In many instances, user expectations for data uses by new apps and new services are still evolving as new benefits and new risks become apparent.

This document seeks to add protections to data that may not be covered by specific sector legislation and to add specific guidance in areas where general privacy statutes are applicable.

---

[1] *See, e.g.,* FPF List of Federal Anti-Discrimination Laws, FUTURE OF PRIVACY.ORG, https://fpf.org/2014/05/21/fpf-list-federal-anti-discrimination-laws/.

[2] While the FDA may regulate the safety and efficiency of certain consumer wearables, it does not set privacy standards. Accordingly, devices subject to FDA regulations are intended to be covered by these best privacy practices.

In Europe and other jurisdictions, national (and soon EU-wide) privacy laws also set baseline privacy and security expectations. While such laws provide the starting point for data protection, they often also impose higher standards on personal information that is considered especially sensitive, such health or financial data. In some cases, consumer-generated wellness data is likely to fall within such protected categories. The European Data Protection Supervisor, for example, has noted that "Lifestyle and well-being data will, in general, be considered [sensitive] health data, when they are processed in a medical context…or where information regarding an individual's health may reasonably be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise)."[3] Where lifestyle or wellness data *is* considered sensitive, additional restrictions on data processing are imposed.

As the Article 29 Working Party has noted, however, "On the other side of the spectrum . . . there is a category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as [sensitive] health data."[4] There are also some apps and devices where "it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data."[5] It is important to distinguish between personal data that are, on the one hand, clearly akin to medical information which reveal inherently sensitive details about an individual's health status and, on the other hand, those raw or low-impact personal data that do not expose an individual's private health information, especially given that most data collected by commercial wearable apps and devices exist in a grey zone between these poles.

Given the lack of bright lines between sensitive health and non-sensitive lifestyle data, treating all health-related personal data the same would be a mistake. The stringent privacy, security, and safety requirements appropriate for medical devices and medical data would render many commercial fitness devices impractical for everyday consumers. At the same time, it would be a mistake to treat wellness data as if it were generic personal information without any sensitivity.

Rather, we should recognize that these data exist on a spectrum and that privacy protections and legal frameworks should be calibrated to the nature and sensitivity of the data. Where personal health or wellness data are inherently more sensitive, for example, their collection and use should be based on a narrower specification of purpose; additional consents should be required for each specified use; and all advertising should be based on express consent. But where data are less inherently concerning health, a specified purpose should appropriately capture a *range* of tightly-related purposes, rather than requiring individualized notices for each and every compatible collection or use of wellness data, and advertising should be presented on an opt-*out* basis. For example, an app that captures a user's steps, height, and weight and whose purpose is to improve users' general fitness and wellness should be able to offer users the opportunity to consent to all

---

[3] European Data Protection Supervisor, Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection (May 21, 2015), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf.

[4] Article 29 Working Party, Letter, *Annex – health data in apps and devices* (Feb. 5, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[5] *Id.*

compatible wellness/fitness uses of their data at once, rather than requiring additional notices and consents for every related purpose.

In determining where data fall on this spectrum, some relevant factors to consider would include: the context and purpose for which data are collected and used; whether data are inherently medical data; whether the data is made available to a member of the medical community; whether there is a clear and close link between the data and a user's health status; whether data is used to measure or predict health risks and/or to enable medical follow-up; whether conclusions are or can be reasonably drawn about the health status of a user based on the data; the compatibility of the use; and the existence of appropriate safeguards.[6]

This document seeks to build upon existing legal expectations by providing organizations with practical guidance that can be further tailored to meet local requirements. It should be noted that this document is not intended to describe *every* privacy practice applicable to wearable devices or related apps or services; rather, it attempts to provide guidance specific to the collection and use of consumer-generated wellness data. Apps and devices that capture other personally identifiable information should look to existing best practices and guidance documents, such as the FTC *Internet of Things Report*,[7] the Article 29 Working Party *Opinion on the Recent Developments on the Internet of Things*,[8] or the FPF-CDT *Best Practices for Mobile Application Developers.*[9]

The principles set out in this document set a baseline of responsible practices intended to support a targeted FIPPs-based trust framework for the collection and use of consumer-generated wellness data. We have described these as best practices in order to recognize that, in a number of places, they set limits or extend protections that go beyond current law. For example, this code sets limits on the transfer of data to data brokers and information resellers, even with express consumer consent. By building on best practices that support consumer trust, as well as developing responsible guidelines for appropriate research and other secondary uses of consumer-generated wellness data, we hope to ensure continued innovation and consumer trust within the wearables ecosystem.

♦ ♦ ♦

---

[6] *See* Article 29 Working Party, Letter, *Annex – health data in apps and devices* (Feb. 5, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[7] FTC Staff Report, Internet of Things: Privacy & Security in a Connected World (Nov. 2013), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[8] Article 29 Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[9] Future of Privacy Forum & the Center for Democracy & Technology, Best Practices for Mobile Application Developers (Dec. 2011), https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf.

BEST PRACTICES FOR CONSUMER WEARABLES & WELLNESS APPS & DEVICES

I. DEFINITIONS

a. Covered data.

a. Covered data is personal information about a user collected by a sensor-enabled device, app, or service that is used by the device, app, or service for non-medical lifestyle or wellness purposes.[10]
b. Covered data includes both data collected via a sensor and data that a user directly inputs (e.g., self-reports by manually entering in the data) that is related to the service which utilizes the sensor.

b. Excluded data. Covered data does *not* include:

1. Data governed by the Health Insurance Portability and Accountability Act (HIPAA).
2. Data regarding the download or usage of a particular app or service by a user.
3. De-identified data, which is data that cannot be reasonably associated with a particular consumer or a particular device associated with a consumer.[11]

c. Enhanced notice. Enhanced notice means providing consumer notices that are clear, prominent, and conveniently located outside of a traditional privacy policy. For example, such notice could be provided before an application is installed, as part of the process of downloading an application to a device; at the time that a device or application is opened for the first time; at the time covered data is collected; in the device or application settings that are presented to the user; or in other ways.

d. Express consent. Express consent means a user's statement or clear affirmative action in response to a clear, meaningful, and prominent notice regarding the collection, use, and sharing of data for a specific purpose.

e. Third parties. Third parties are entities that are not under the control of an organization and are not related to it by common control or ownership. For the purposes of this document, a company's vendors, partners, affiliates, agents, and similar parties are not third parties provided that appropriate contractual controls bind such parties, including limitations on data uses, prohibitions on attempts to re-identify data, and adequate data security

f. Research. Research is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge or for publication. Research does not include activities intended to develop or improve new or current products.

---

[10] This document is intended to apply to wellness data collected and utilized outside of a medical context, including lifestyle and fitness data that may include an individual's habits or behaviors but do not inherently relate to that individual's health status. However, when wellness data is used for a medical purpose (e.g., to measure or predict health risks or to enable medical follow-up), those uses would no longer be within the scope of this document.

[11] Data is not reasonably associated with a particular consumer or device when both direct and indirect identifiers have been masked or eliminated.

g. Product development. Product development may include any activities intended to improve, maintain, or add new features, including testing or analysis done for such purposes.

h. Compatible uses. Internal operational activities such as security improvements, stability refinements, and product improvement and development are considered compatible secondary uses of data. Research may or may not be considered compatible, depending on the nature of the investigation. In determining whether or not a secondary use is compatible with the primary purpose of the app or service, companies should take into account:

1. Any link between the purposes for which the data have been collected and the purposes of the intended secondary use;
2. The context in which the data have been collected, in particular regarding the relationship between data subjects and the controller;
3. The nature and sensitivity of the data;
4. The possible consequences of the intended secondary use for the user or consumers; and
5. The existence of appropriate safeguards, which may include encryption or pseudonymization.

II. NOTICE/TRANSPARENCY

a. Privacy notices. Companies must maintain clear and conspicuous access to a publicly available privacy policy or other online documentation[12] that specifies (when applicable):

1. What data is collected and how it is collected, stored, used, secured, and disclosed.
2. Uses of data for advertising.
3. De-identification commitments.
4. Whether any covered data will be used or shared for Research.
5. Users' options regarding access, correction, or deletion of covered data.
6. Under what circumstances covered data is intended to be collected from non-users.
7. How the company responds to requests for users' covered data from federal, state, local, or foreign law and civil enforcement agencies.

b. EU privacy notices. Additionally, when collecting and using and covered data from EU individuals, companies must maintain a prominent, publicly available privacy policy or other online documentation that is easily accessible to users that specifies:

1. The identity and contact details of the device, app, or service developer and the contact details of a data protection officer (if any).
2. The purpose and legal basis of the intended data collection and processing.

[12] Note that specific disclosures can also be provided via enhanced notice mechanisms.

3. What data is collected and how it is collected, stored, used, secured, and disclosed, including the categories of covered data that will be processed and, where applicable, the recipients or categories of recipients of the covered data.
4. Whether covered data will be transferred from the user's device and, if so, to which recipients or categories of recipients.
5. The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period.
6. That consent to the collection and use of covered data may be withdrawn at any time, without affecting previously collected and processed covered data.
7. That use of the device, app, or service is strictly voluntarily, but requires user consent to permit the processing of covered data.
8. If covered data will be used for automated decision-making, meaningful information about the logic involved and the significance and envisaged consequences of such processing for the user.
9. Users' rights to lodge a complaint to a supervisory authority.
10. Users' options regarding access, correction, or deletion of covered data, as well as to object to the processing of covered data.

c. Enhanced notice is required:

1. When a material change is made to the privacy policy.
2. When covered data is sold or shared with third parties.
3. For secondary uses of covered data that are incompatible with the primary purpose of the app or service.

III. CHOICE/CONSENT

a. Consent for Non-Research Activities.

1. Express consent is required:
   i. Before covered data is used in any materially different manner than claimed when the data were collected.
   ii. To share covered data with third parties or to make covered data public except as otherwise permitted in this document.
   iii. For secondary uses of covered data that are incompatible with the primary purpose of the app or service.
2. Express consent may be obtained:
   i. By a device, app, or service directly; or
   ii. By a platform or other third party requesting on behalf of the device, app, or service.
3. Express consent to share covered data with a third party may be obtained:
   i. At the point of sharing;
   ii. As part of the download or installation flow, but before data is collected; or
   iii. Via a separate process where the individual user provides the third party with express consent to access the data.
4. Express consent may be withdrawn at any time, without affecting the previously collected and processed covered data.

b. Consent for Research. Where covered data is shared for Research or incompatible, interventional Research[13] is conducted on users, informed consent must be obtained from participants[14] unless otherwise approved by an ethical review process. [15, 16]

IV. ADVERTISING

a. No third-party sharing. Covered data may not be sold to advertising platforms, data brokers, or information resellers, even with express consent.

b. First party advertising. If a company tailors advertisements on the basis of covered data, it must provide users an ability to opt-out of such advertising.

V. LIMITATION ON COLLECTION AND USES

a. Restricted uses. Covered data must not be collected or used for the following purposes without express consent: employment eligibility, promotion, or retention; credit eligibility; healthcare treatment eligibility; and insurance eligibility, underwriting, and pricing.

b. Secondary uses. Secondary uses of covered data must not be incompatible with primary purpose(s) of the app or service described in the privacy policy, unless enhanced notice is provided and express consent is obtained.

VI. SHARING

a. Prohibited sharing.

1. Covered data may not be sold to advertising platforms, data brokers, or information resellers, even with express consent.[17]
2. Covered data may not be transferred in conjunction with the sale, merger, bankruptcy, sale of assets or reorganization of the company, unless:
    i. The successor entity is subject to these same commitments for previously collected covered data, or

---

[13] Intervention is defined, consistent with the Common Rule, as "both physical procedures by which data are gathered ... and manipulations of the subject or the subject's environment that are performed for research purposes." *See* 45 CFR 46.102(f)."

[14] As informed consent is often subject to specific regulatory guidance, companies should consult local laws and regulations in their jurisdiction. Such consent will often include the (i) nature, purpose, and duration of the Research; (ii) procedures, risks, and benefits to the participant; (iii) information about confidentiality and handling of data (including any sharing with third parties); (iv) a point of contact for participant questions; and (v) the withdrawal process.

[15] The goal of an ethical review process is to identify both the risks and the benefits of the secondary use or Research and to balance the prospective risks to the user, prospective benefits to users or to the public, the rights and interests of the user, and the legitimate interests of the data holder.

[16] Note that section III.b. is not applicable if research is compatible with the primary purpose for which covered data was collected, as defined in section I.h.

[17] This section does not intend to address sharing covered data, with a user's express consent, with organizations such as, e.g., employee wellness plans, insurers, research institutions, service providers, etc. whose primary purpose is not reselling personal information to third parties.

ii. Users provide express consent before covered data is used in any materially different manner than claimed when the data were collected.

b. Government access. Express consent is not required when covered data is used or shared as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation.

c. Permissible sharing. Covered data may be shared without express consent:
1. With the company's vendors, affiliates, partners, agents, and similar parties that are contractually engaging in providing device services, provided that appropriate contractual controls bind such parties, including limitations on data uses, prohibitions on attempts to re-identify data, and adequate data security.
2. If disclosure is reasonably necessary to comply with the law.
3. To preserve the security and safety of people or property.

VII. ACCESS, ACCURACY, CORRECTION, & DELETION

a. Access. Companies must make covered data available to the user it refers to in a reasonably complete way as soon as reasonably practical and technically feasible, at little or no cost to the requester.

b. EU access. Additionally, when collecting and using covered data from EU individuals, companies must provide users with confirmation as to whether or not covered data concerning them are being processed and, where such covered data are being processed:
1. Where covered data are transferred to a third country or to an international organization, the appropriate safeguards for such transfer.
2. Where the covered data are not collected from the user, any available information as to their source.

c. Accuracy. Companies must, in a manner that is reasonable and appropriate for the privacy risk associated with covered data, establish procedures to ensure that covered data under their control are accurate and, where necessary, kept up to date. In developing such procedures, companies should consider the costs and benefits of ensuring the accuracy of covered data.

d. Correction. Companies must allow users to dispute and resolve the accuracy or completeness of covered data pertaining to them. The means of resolving a dispute should be reasonable and appropriate for the privacy risks and the risk of an adverse action against an individual that are associated with such covered data. If a company declines to correct or amend the covered data, the company must, upon request, delete the covered data without undue delay.

e. **Deletion.** Companies must provide users with easily accessible mechanisms to delete or request the deletion of their covered data, and take reasonable steps to

delete or de-identify data without undue delay as reasonably practical and technically feasible and in compliance with applicable law.

VIII. LIMITED RETENTION

a. Retention policy. Companies must set internal policies for data retention.

b. Covered data. Covered data must not be maintained for longer than is needed for the reasonable operation of the app or service, or as long as the user maintains an account with the company.

IX. DATA SECURITY

a. Companies must maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of covered data against both internal and external risks, such as unauthorized access, or unintended or inappropriate disclosure. Such a program must contain administrative, technical, and physical safeguards commensurate to the nature, context, and scope of its activities and the sensitivity of the covered data, having regard to the state of the art and the costs of implementation, including, as appropriate:

1. The pseudonymization and encryption of covered data;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing covered data;
3. The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[18]

X. ACCOUNTABILITY & ENFORCEMENT

a. Accountability. Companies must implement and document internal processes and procedures reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for users, and (2) protect the privacy and confidentiality of covered data.

b. Enforcement. Companies must include these provisions, as applicable, in their terms of service, developer terms, or other relevant agreements. This includes contractually obligating:

---

[18] For guidance on reasonable security requirements, see FTC, *Start with Security: A Guide for Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; NIST, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53 Rev.4) (Apr. 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814) (Annex to Article 9) (Ger.), http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0181.

1. Vendors, partners, agents, and similar parties that are contractually engaging in providing device services to implement and maintain appropriate security safeguards and use data only for designated purposes.
2. Recipients of de-identified data to make no attempt to re-identify data.
3. Recipients of covered data to affirmatively represent that they will comply with all applicable laws (including, *e.g.*, the ADA, EEOC rules, and/or non-discrimination statutes).

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a catalyst for privacy leadership and scholarship, advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups.

The document was produced with support from the Robert Wood Johnson Foundation.

1400 Eye Street, NW, Suite 450
Washington, DC 20005
info@fpf.org