Consumer Technology Association™

GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH AND WELLNESS INFORMATION

Consumer Technology Association™

GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH AND WELLNESS INFORMATION

Introduction

Personal health and wellness technologies continue to be one of the fastest-growing segments in information and digital technology. Now more than ever, consumers can obtain instant feedback on everything from the number of steps they walk, the patterns of their resting heart rate to their online medical information.

The advantages of these technological developments and increased accessibility are multi-faceted. Consumers benefit first and foremost with more information about their health and wellness and a better ability to choose a fitness plan, make health- and wellness-related decisions, and even navigate complex medical issues. Health care companies, science and society may benefit too. It is now possible to develop sophisticated tools to research health and wellness on an aggregated basis, resulting in better and quicker diagnoses and treatment for certain conditions.

All of these benefits depend on the collection, use and sharing of consumer data.

Companies in the health and wellness ecosystem understand that they must be good data stewards to maintain consumer trust. With trust in mind, the Consumer Technology Association ("**CTA**" or "**we**") recommends that companies incorporate these Guiding Principles on Privacy ("**Principles**") into their technologies and practices. Awareness of these Principles through a technology's development and deployment stages may help mitigate risks that consumers may perceive with respect to their personal health information.

We intend these Principles to be baseline recommendations. We want companies to retain flexibility on how to implement the Principles so they can account for differences in technology, products, and services. We also want companies to preserve control over how they communicate with their consumers. Consumer preferences and their comfort with technology will evolve, and a company's approach to communication should evolve, too. We encourage companies to maintain an ongoing dialogue with consumers to discuss the value of their technologies, as well as the privacy options they offer. We also encourage companies to understand their consumers' potential sensitivities about the use of their personal health information, taking into consideration any particular considerations applicable to their technology and the kinds of data that they collect.

In these Principles, we use the term "**personal health information**" to refer to any data collected through personal health and wellness devices, applications, websites, and other digital or online tools that specifically relates to a consumer's health and wellness. Personal health information can refer to demographic information (such as a consumer's age, gender, and ethnicity), fitness information (such as a consumer's exercise activities or fitness abilities), and medical information (such as medical history, genomic data, vital signs, height, weight, and other physiologic parameters, and patient-reported outcomes).

Scope

The Principles are:

- Voluntary, but companies may publicly commit or attest compliance with these Principles through their own marketing or promotional materials.
- Intended for use by members of CTA, but usable by any technology innovators, Service Providers (defined below), app developers and new-to-market companies in the personal health and wellness ecosystem who seek information about maintaining consumer privacy.
- Based on privacy concepts currently present and developing in U.S. law, while recognizing the importance and potential impact that international privacy laws have on U.S. companies.
- Offered to complement, not supplant, the applicable legal requirements and regimes with which companies need to comply.
- Applicable to personal health information, but may also guide your practices with regard to consumer data that is not personal health information.
- Available to consumers so that they can learn about CTA's Principles and make informed choices about the apps and companies with whom they choose to interact.

Privacy Principles

1. Be open and transparent about the personal health information you collect and why.

Being open and transparent about your privacy practices help consumers make informed decisions about how they use your technology.

We recommend that you:

- Draft a Privacy Policy that explains how you collect, use, and share consumer data (including personal health information).
- Use a consumer-friendly or user-friendly format with clear, concise, and easy to understand language.
- Post a link to your Privacy Policy in your mobile app and website where it is easily accessible to consumers before consumers provide their personal health information to you or create an account.
- Review your Privacy Policy at least annually and when you make changes to your privacy practices.
- Provide meaningful notice to, and obtain an acknowledgment from, consumers regarding updates (such as through a banner, pop-up, or electronic communication) that are material or otherwise affect their privacy rights.
- For mobile apps, provide a "short form" version of your Privacy Policy that is easy to read on smaller screens.

A **Privacy Policy** is a method of communication information about how you collect, use, and disclose consumer data.

---

2. Be careful about how you use personal health information.

While use of personal health information can provide your consumers with many benefits, you should guard against the possibility that such use could infringe on the privacy rights of consumers. You should use personal health information in ways that consumers would expect you to use it (given the anticipated purpose of the collection) and have requirements and safeguards in place to provide that all who process that personal health information abide by those same expectations.

We recommend that you:

- Minimize the personal health information you collect, use and disclose. You can use techniques such as anonymization or de-identification to minimize the privacy impact your practices have on consumers.
- Use personal health information only for the purpose(s) for which you collected it. If you want to use personal health information for a secondary purpose, make sure that the secondary purpose is consistent with the initial purpose, or otherwise obtain the consumer's consent or ensure the secondary use occurs under another available pathway under applicable law.

Consent should be a clear affirmative act that signifies a freely given specific, informed, and unambiguous indication of a consumer's agreement, such as a written statement, checking a box, or other clear, affirmative action.

- Put yourself in the consumer's shoes. Your use of personal health information should be in line with the consumer's expectations. Do not use personal health information in ways that are unexpected, unjust or deceptive to consumers, such as ways that are not clearly disclosed in your Privacy Policy.
- Obtain consent for the use of sensitive data, including personal health information and other personally identifiable information.
- Perform Privacy Impact Assessments. There are publicly available templates that can get you started, but we recommend customizing them for your particular needs.

A **Privacy Impact Assessment** is an analysis of how personally identifiable information is collected, used, shared, and maintained. The purpose of a PIA is to demonstrate that you have consciously incorporated privacy protections throughout the development life cycle of a system, program or process.

- Periodically review algorithms and automated decisions to confirm that they are applied fairly and without prejudice to certain classes of consumers.
- Keep personal health information only as long as you need it (If at all) and destroy it securely once it is no longer needed.

3. Make it easy for consumers to access and control the sharing of their personal health information, and empower them to do so.

Consumers should have the ability to access and control the sharing of their personal health information. This will enable consumers to take steps to communicate their preferences about how their data is used and shared in order to protect their privacy. You should also take steps to help consumers be empowered to exercise their choices.

We recommend that you:

- Give consumers the right and the means to access and correct their personal health information.
- Build consumer-facing privacy settings into your technology so that consumers can communicate their privacy preferences to you in real time.

- Consider adopting emerging technologies that would enhance the consumer's ability to access and control their personal health information.
- Make the settings easy to find and easy to use, such as toggles or check boxes placed in a clearly labeled menu (e.g., Privacy Dashboard or Privacy Settings).
- Honor other privacy rights provided by the laws applicable and relevant to you, such as the right to deletion, portability, or objection.

4. Build strong security into your technology.

Respecting the privacy of consumers means protecting their data. You should implement administrative, technical and physical safeguards that are appropriate to the type of personal health information you collect, process and store. When determining what is appropriate, you should consider the size, scope and type of business, the amount of available resources, and the amount of stored data.

We recommend that you:

- Perform information security risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of documents or records containing personal health information.
- Work closely with your information technology and information security teams to determine what measures are appropriate for the type of personal health information you collect.
- Use encryption technology to protect personal health information that is sensitive in nature while at rest and in transit.

Encryption is the process of encoding information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the readable content to those who are not autorized to access it.

- Aside from providing consumers access to their own data, limit access to personal health information only to Service Providers (defined below) and those in your company who have a need to know or a need to access for purposes of their job function or other legitimate reason.
- Continually evaluate and improve, where necessary, the effectiveness of your current safeguards for limiting security risk.

5. Be accountable for your practices and promises.

You should hold yourself accountable to yourself and to consumers regarding your practices and the promises you make about them.

We recommend that you:

- Appoint a data protection officer, privacy officer, or other person responsible for security and privacy of personal health information.

- Manage Service Provider risk by taking reasonable steps to select, assess, and retain Service Providers that are capable of maintaining appropriate security measures to protect personal health information. You should require Service Providers by contract to implement and maintain such appropriate security measures. You should also take steps to monitor and oversee Service Providers during the course of the engagement to confirm Service Providers are able to continually protect personal health information.

A Service Provider is any person or entity that receives, stores, maintains, processes, or otherwise is permitted access to Personal Health Information through its provisions of services.

- Educate and train your staff about these Principles and the steps you have taken to protect the privacy of your consumers and their personal health information. You should discipline your staff for violations of these Principles and your policies and procedures.
- Make yourself available to answer and address consumer concerns, such as through a toll-free number or email address. To ensure timely responses, assign the responsibility of regularly checking voice and email messages to one or a group of individuals.
- To the extent required by applicable laws, report security incidents and breaches that compromise personal health information.
- Stay informed about changes to and interpretation of privacy laws that apply to you. You can sign up for alerts and mailings from your applicable regulators, outside counsel, and industry groups.
- Lead by example to model a culture of ethics and integrity.

The Guiding Principles on Privacy do not represent a negotiated, industry-wide self-regulatory code of conduct. CTA intends to review this document on a regular basis in concert with its members to ensure that it accurately reflects current privacy issues in the technology industry.