Consumer Technology Association™

GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH DATA

Consumer Technology Association™

GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH DATA

Introduction

Personal health technologies continue to be one of the fastest-growing segments in the information and digital technology space. Now more than ever, consumers can obtain instant feedback on everything from their blood pressure to the patterns of their resting heart rate.

As consumer preferences and comfort with technology evolve, so too are company products and services. Innovative technologies like remote monitoring, artificial intelligence and machine learning, and digital therapeutics continue to transform health care and the ways that health care providers and consumers/patients use data to improve care coordination, diagnostic accuracy, and quality of care. Consumers have an increased desire to actively manage and monitor their health, and share their data with health care providers, applications, caregivers and family members.

The Consumer Technology Association ("**CTA®**" or "**we**") believes that collaboration among the health care sector, technology stakeholders and consumers can help drive better patient care and facilitate better coordination. The collection and sharing of health information is critical to improving the quality and safety of health care and advancing health care innovation that can improve the health and wellbeing of consumers. That said, CTA® recognizes legitimate consumer concerns regarding the privacy of their personal health data.

Companies in the personal health ecosystem understand that they must be good data stewards to maintain consumer trust. Consumers now expect that companies will provide the:

- Right to access their own data.
- Right to withdraw consent.
- Right to modify inaccurate data.
- Right to the portability of data.
- Right to information about how entities are sharing their data.
- Right to be forgotten.

With trust in mind, CTA® recommends that companies incorporate these Guiding Principles for the Privacy of Personal Health Data ("**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 data.

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 data, taking into consideration any particular factors applicable to their technology and the kinds of data that they collect.

In these Principles, we use the term "personal health data" to refer to any data collected through personal health applications, monitoring devices, websites, and other digital or online tools that specifically relates to a consumer's health. Personal health data 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.
- Usable by any technology innovators, service providers, app developers and new-to-market companies in the personal health 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 data but may also guide your practices with regard to consumer data that is not personal health data.
- 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 data 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 data).
- Use a consumer-friendly or user-friendly format with clear, concise, and easy to understand language.
- Ensure that your Privacy Policy is accessible for the populations you serve, including providing the Policy in multiple languages and providing alternatives for consumers with disabilities like blindness.
- 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 data to you or create an account.

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

- Review your Privacy Policy at least annually and when you make changes to your privacy practices.
- Proactively notify consumers of any changes to the Privacy Policy.
- Provide meaningful notice to, and obtain an acknowledgement 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.

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

While use of personal health data can provide you and 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 data 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 data abide by those same expectations.

We recommend that you:

- Minimize the personal health data 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.
- Periodically review the process by which you anonymize or de-identify data.
- Be descriptive and clear about the purpose for which you are collecting, storing and using personal health data. Any activities not included in this description will be considered a secondary purpose.
- Use personal health data only for the purpose(s) for which you collected it. If you want to use personal health data for a secondary purpose, make sure that the secondary purpose is consistent with the initial purpose, or otherwise ensure that the consumer opts into the use of their personal health data for the secondary purpose; 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 data should be in line with the consumer's expectations. Do not use personal health data in ways that are unexpected, unjust or deceptive to consumers, such as ways that are not clearly disclosed in your Privacy Policy.
- Obtain consent or have a robust opt-in system for the use of personal health data and other personally identifiable information involving third parties.
- Allow consumers to withdraw their consent or opt-in and ensure the process to withdraw is easy to understand and execute.
- If the data will be used for purposes of clinical research, you must obtain the appropriate informed consent as required under applicable law.
- Perform Privacy Impact Assessments. There are publicly available templates that can get you started, but we recommend customizing them for your specific needs. From a compliance perspective, however, it is advisable for a third party to perform the Privacy Impact Assessment.

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.

- If using algorithms or automated solutions to assist in human care decisions, provide a clear description of what is being predicted and what is the expected output of the algorithm or automated solution. You should comply with responsible AI practices (such as the ANSI/CTA Standard *The Use of Artificial Intelligence in Health Care: Trustworthiness ANSI/CTA-2090*)
- Periodically review algorithms and automated decisions to confirm that they are applied fairly and without prejudice to certain classes of consumers.
- Keep personal health data only as long as you need it 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 data and empower them to do so.

Consumers should have the ability to access and control the sharing of their personal health data. 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 modify their personal health data.
- 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 data.
- 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 the data you maintain about them. You should implement administrative, technical and physical safeguards that are appropriate to the type of personal health data you collect, process and store. When determining what is appropriate, you should consider the size, scope and type of business, the number 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 data. From a compliance perspective, however, it is advisable for a third party to perform these assessments.
- Work closely with your information technology and information security teams to determine what measures are appropriate for the type of personal health data you collect.
- Periodically review your cybersecurity policies to ensure they meet current standards which tend to evolve quickly.
- Use encryption technology to protect personal health data 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.

- Limit access to personal health data 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. The list of Service Providers and those in the company who need access to personal health data should be reviewed and updated regularly.
- Continually evaluate and improve, where necessary, the effectiveness of your current safeguards for limiting security risk.
- Where possible, you should implement multi-factor authentication for access to certain personal health data, particularly involving more sensitive data such as mental health or HIV status.

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 data.
- 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 data. 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 data.

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 data. Education and training should be recurring—and take place at least once a year or more frequently as events dictate. 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 data.
- Stay informed about changes to and interpretation of privacy laws that apply to you. Remember that the laws that apply to you may also include the jurisdiction in which your consumer lives. You can sign up for alerts and mailings from your applicable regulators, outside counsel, and industry groups.
- Remind consumers that they have shared responsibility in maintaining the privacy of personal health data, including selecting strong passwords, not sharing passwords, etc.
- Lead by example to model a culture of ethics and integrity.

The Guiding Principles for the Privacy of Personal Health Data 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.