Consumer Technology Association™

April 15, 2016

Office of the National Coordinator for Health Information Technology Department of Health and Human Services
200 Independence Avenue, S.W. Suite 729-D
Washington, D.C. 20201
ONCMPN@hhs. gov

RE: MPN RFI
Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice
Comments of the Consumer Technology Association

Dear Dr. DeSalvo:

The Consumer Technology Association ("CTA")[1] respectfully submits these comments in the above-captioned Request for Information.[2] CTA shares the goal of the Department of Health and Human Services ("HHS") Office of the National Coordinator for Health Information Technology ("ONC") to develop voluntary, concise consumer disclosures that empower consumers to make informed decisions about their health and well- being. CTA believes that the current Model Privacy Notice ("MPN")[3] can be adapted easily to include new types of information practices with very little modification, while remaining highly relevant to and useful for consumers.

I. Introduction

There is a vibrant and innovative market for health, fitness, and wellness devices and software ("health technology") that helps consumers keep track of their health and fitness. In the United States, CTA estimates that fitness trackers have an installed base of 33.3 million units—nearly double that of 2015—and smart watches, which often

---

[1] The Consumer Technology Association (CTA)™, formerly Consumer Electronics Association (CEA)®, is the trade association representing the $287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

[2] Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice, 81 Fed. Reg. 10634 (March 1, 2016) ("MPN RFI"), https://www.gpo.gov/fdsys/pkg/FR-2016-03- 01/pdf/2016-04239.pdf.

[3] For ease of reference, we refer to the template available on ONC's website as the "current MPN," while the "Updated MPN" is the proposed future product of this RFI.

incorporate fitness tracking features, have an installed base of 13 million units.[4] Furthermore, consumers have a strong intent to buy these products: 11% of consumers who have never owned fitness trackers intend to purchase them, and 6% intend to buy smart watches.[5] Health technologies are spearheading a trend away from reactively treating conditions to proactively maintaining a healthy lifestyle.[6]

Consumers faced with an ever-growing array of health technologies may be understandably concerned about the privacy and security of their personal health data. To gain consumer trust, developers are working to make their privacy and security practices transparent and secure. For example, last year CTA published its *Guiding Principles on the Privacy and Security of Personal Wellness Data*, a first-of-its-kind effort.[7] The Principles lay out the essential steps companies can take to address privacy and security risks related to wellness data. In particular, CTA strongly supports concise notices that accurately communicate a company's data management practices.

Effective notices must articulate information that directly addresses privacy risks to consumers, not merely condense a privacy policy into an alternative format. Consumers will ignore laundry lists that do not immediately highlight relevant information be- cause such lists do not capture their attention.[8] Therefore, it is important to judiciously select the information presented in privacy and security disclosures. To do this, developers should focus on disclosing information that clearly addresses the risk of privacy harms to consumers. Research shows that third party data transfers and transfers of identifiable information are particularly relevant here. For example, consumers under- stand that sharing such data could lead to certain undesirable outcomes, such as un- expected eligibility determinations or unsolicited messages.[9]

---

[4] 1*8th Annual Consumer Technology Ownership and Market Potential Study,* CONSUMER TECHNOLOGY ASSOCIATION, at 17 (March 2016).

[5] *Id*. While these figures might seem moderate, CTA's experience is that, initially, "[e]merging technologies often show a high 'never buy' percentage among [households], often due to lack of awareness or understanding of the product." *Id*. at 68.

[6] "A majority of consumers bought health and fitness products for fitness reasons." *Consumers Journey to Purchase: Health & Fitness*, CONSUMER TECHNOLOGY ASSOCIATION, at 8 and 23 (Oct. 2015).

[7] *Guiding Principles on the Privacy and Security of Personal Wellness Data*, CONSUMER TECHNOLOGY ASSOCIA- TION (Oct. 2015) ("CTA Privacy Principles"), https://www.cta.tech/CorporateSite/media/gla/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf.

[8] *See Spring Privacy Series: Mobile Device Tracking*, Workshop Slides, FEDERAL TRADE COMMISSION, at 68 (Feb. 19, 2014) (explaining "Factors that increase attention" in notifications), https://www.ftc.gov/system/files/documents/public_events/182251/mobiledevicetrackingseminar- slides.pdf.

[9] A CTA study concluded that "[t]wo-thirds (65%) of fitness tracker owners say they are willing to share personal data with the fitness tracker device manufacturer (36% "willing," 29% "extremely willing"), while less than half (44%) would be willing to share similar information with third-party apps or other service providers (26%, 18%)." *Wearable Activity Trackers: Engaging Consumers to Monitor their Health*, CONSUMER TECHNOLOGY ASSOCIATION, at 50 (Jan. 2015).

ONC clearly recognizes that third party transfers and identifiable information are prior- ities, since the current MPN addresses those issues. Therefore, it requires very little modification. Specifically, ONC should replace the definition of Personal Health Record ("PHR")—which confines the MPN's scope—with an open space that developers can use to define the type of data they manage.

II. ONC Should Permit Health Technology Developers Themselves to Define the Information that Is In Scope for an Updated MPN

CTA appreciates ONC's thorough discussion of the data elements that could be included in a voluntary Updated MPN. We share ONC's goal of giving consumers the under- standable and relevant information they need to make informed decisions. The MPN RFI asks what "information types" and "information practices" should be considered in and out of scope.[10] CTA urges ONC not to expand the scope of information types and practices in an Updated MPN. The only modification ONC should make is to remove the definition of "PHR data" and create an open space on the Updated MPN to allow health technology developers to choose how to describe the data they collect.

The current MPN already addresses the most impactful privacy risks to consumers. Consumers recognize that third party data transfers—not how developers use that da- ta internally—could create privacy risks. For example, CTA found that 65% of fitness tracker owners said they are willing to share personal data with the device manufacturer versus 44% who say they are comfortable sharing personal data with unaffiliated third parties.[11]

Consumers also recognize that identifiable data shared with third parties creates risks. For example, CTA found that consumers become more willing to share biometric data about themselves in a broad range of use cases if identifiable information is stripped out.[12] Moreover, existing laws like the Health Information Portability and Accountability Act ("HIPAA")[13] and industry privacy best practice principles recognize that non- identifiable data poses fewer risks to consumer privacy.[14]

---

[10] MPN RFI at 10635.

[11] *See supra* note 7.

[12] *Biometric Technologies: Understanding Consumer Sentiments*, CONSUMER TECHNOLOGY ASSOCIATION, at 17 (March 2016) (showing that willingness to share biometric information increases at least 11% when identifiable information is stripped out).

[13] *Guidance Regarding Methods of De-identification of Protected Health Information in Accordance with HIPAA Privacy Rule*, HHS (Nov. 26, 2012), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[14] CTA Privacy Principles, at 2 (excluding de-identified data from the principles). *See also Privacy Principles for Vehicle Technologies and Services*, ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC., ASSOCIATION OF GLOBAL AUTOMAKERS, at 4 (Nov. 12, 2014), http://www.autoalliance.org/index.cfm?objectid=CC629950- 6A96-11E4-866D000C296BA163 (excluding information that could be linked to a vehicle or its owner from its definition of "covered information").

The current MPN addresses both third party transfers and identifiable information. The "Release" sections asks whether PHR companies release personal (*i.e.*, identifiable) and statistical data to organizations other than the developer and its service providers, and for what purpose.[15] By comprehensively disclosing this information, the current MPN addresses consumer privacy risks.

However, the current MPN's application is limited by the definition of PHR.[16] To expand it, ONC will need to revise the scope of data to which the MPN applies.[17] CTA cautions against creating a definition that includes specific information types and practices, as any such list is bound to become over- or under-inclusive as health technology progresses.

Instead, ONC should give health technology developers maximum flexibility to modify the scope of the Updated MPN, taking into account their unique products and data management practices. A blank space on the Updated MPN where developers could describe the data they collect, store, use, and transfer would achieve flexibility while still giving consumers relevant information.

III. ONC Should Not Add New Information to an Updated MPN

To be effective, a concise privacy notice needs to present information that is most impactful to consumers, rather than merely condense a privacy policy into a short for- mat. ONC inquires whether the Updated MPN should include a broad range of detailed information. CTA strongly believes that minimizing the information presented in a concise notice like the MPN will improve its usability. More detailed information should remain in a developer's privacy policy.

User scope. All types of health technology developers should be able to use an Updated MPN. Providing health technology developers with a means to define the scope of information they manage—as we describe above—will broaden the Updated MPN's user base.

Information type. ONC should not designate certain types of data as in or out of scope for the Updated MPN. Instead, it should continue to focus on *uses* of data, as it does now, and allow health technology developers to describe the data that is in scope for the particular product to which the MPN applies.[18]

Information practices. An Updated MPN should primarily focus on the purposes for which a health technology developer releases or transfers identifiable information to third parties. Data that is not identifiable or never transferred to a third party has significantly fewer privacy impacts for consumers. Such disclosure is better articulated in a privacy policy than in a concise notice format.

---

[15] *See Model Privacy Notice Template,* HHS ONC, at 1–2 ("MPN Template"), https://www.healthit.gov/sites/default/files/phr-model-privacy-notice-final-2011.pdf.

[16] *Id*. at 2.

[17] MPN RFI at 10635.

[18] MPN Template at 1 (describing the purposes for which a PHR company would release data).

Sharing and storage. While CTA encourages companies to thoroughly explain their data management practices,[19] it is not necessary or even desirable to communicate de- tailed information about a company's data collection and storage practices in a concise format like the MPN. First, such information would increase the Updated MPN's length, distracting consumers from more immediately relevant information. Detailed information properly belongs in a developers' privacy policy.

Second, companies will have widely varying collection and storage practices depending on the nature of their products. Companies may have legitimate reasons for declining to adopt collection and storage practices that other companies may deem essential. For example, one company may prefer to store all its data on computers it owns, while a similarly situated company uses a foreign data center. Comparing such practices in a compressed format like the Updated MPN, without the opportunity to provide con- text, would be like comparing apples and oranges. At best, consumers would be con- fused, and at worst, a comparison without context could lead them to make poorly informed choices. If ONC decides to include sharing and storage information in an Updated MPN, it should only require that a company link to the relevant parts of its privacy policy.

Security and encryption. The threats health technology developers face are increasing, constantly changing, and complex.[20] In this environment, the methods developers use to prevent unauthorized access and disclosure of all types of data must also change rapidly, in timeframes that are measured in days or hours. CTA urges ONC not to add additional information to the Updated MPN with respect to security and encryption. Describing security practices in detail could open developers to attack and create a significant administrative burden as they make updates every time a security practice changes. Moreover, attempting to describe security practices accurately in a compressed format is difficult and likely to lead to consumer confusion.

Access to other device information. ONC should not address access to other types of information in an Updated MPN because such information would be redundant. Consumers very often have notice about, and the ability to set permissions for, such information—such as when they download software applications from app stores, and when they access app settings menus.[21]There is no need to duplicate such information in the Updated MPN.

---

[19] *See generally* CTA Privacy Principles.

[20] *See Internet Security Threat Report*, SYMANTEC, at 5-8 (Apr. 2016), https://www.symantec.com/security-center/threat-report.

[21] *See, e.g.*, Control Your App Permissions on Android 6.0 and Up, GOOGLE PLAY HELP (last accessed Apr. 13, 2016), https://support.google.com/googleplay/answer/6270602; About Privacy and Location Services, APPLE SUPPORT (last accessed Apr. 13, 2016), https://support.apple.com/en-us/HT203033.

IV. Conclusion

Voluntary, concise notices and disclosures are an effective means of informing consumers about companies' health information practices. CTA applauds ONC's effort to update its MPN to be applicable to new health information practices. However, we caution that an Updated MPN should narrowly address the most immediate privacy risks to consumers so that they are informed, not overwhelmed. ONC can accomplish this by giving companies that adopt the Updated MPN the ability to define the data to which it applies.

Respectfully submitted,
CONSUMER TECHNOLOGY ASSOCIATION
F/K/A CONSUMER ELECTRONICS ASSOCIATION

By: */s/ Julie M. Kearney*

Julie M. Kearney
Vice President, Regulatory Affairs Alexander B. Reynolds
Director, Regulatory Affairs
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

April 15, 2016

CTA's Guiding Principles on the Privacy and Security of Personal Wellness Data

I. Introduction

Wellness-related wearable devices represent one of the fastest-growing segments of the Internet of Things. Consumers now harness data about themselves—calories, steps, heart rate, and more—to improve their well-being. In the future, these devices will tell consumers even more about themselves, providing analytics and insights that will empower them to lead richer and healthier lives. Society also will benefit as we develop sophisticated tools to research health and wellness on an aggregated basis.

All of these benefits depend on the collection and use of data, some of which can be considered personal or sensitive. Companies in the health and fitness ecosystem understand that they must be good stewards of that data to maintain consumer trust.

With trust in mind, these Guiding Principles ("Principles") articulate the Consumer Technology Association's ("CTA") recommendations for voluntary best practices that mitigate risks that consumers may perceive with respect to personal wellness data.[1] These Principles articulate practices that can be followed by a broad variety of companies in the health and fitness wearable ecosystem. If adopted, they may help companies obtain and maintain consumer trust. Since the Principles are baseline recommendations, companies following them will retain flexibility on how to implement them, accounting for each company's unique combination of products, services, and users.

Data privacy and security are continually evolving concepts that require a dialog among companies and consumers. As consumer preferences and comfort with technology evolve, so too will companies' products and services. CTA encourages companies to maintain an ongoing dialog with consumers to both discuss the potential value of health and fitness technologies and the privacy options such technologies offer and also to understand their potential sensitivities about the use of this data.

[1] These Guiding Principles are recommendations that a CTA working group has developed for voluntary best practices. They are not intended to supplant rules developed for doctors and other healthcare professionals under the Health Insurance Portability and Accountability Act (HIPAA). Nor do they represent a negotiated, industry-wide self-regulatory code of conduct.

The Principles begin by defining key terms. Next, we list each principle and the issue it attempts to address. We then offer a more complete discussion of each principle. CTA intends to review this document on a regular basis in concert with its members to ensure that it accurately reflects current data privacy and security concerns.

II. Definitions

Company.

Any person, including corporate affiliates, that manufactures a device, develops software, or provides a service that collects, stores, or uses personal wellness data. As used in this document, company refers to the entity providing a product or service to the user, not the software or hardware platform on which the product or service may rely.

Unaffiliated Third Party.

Any person other than (1) a user of a company's products or services; (2) a company's employees; or (3) a vendor or supplier to a company when such vendor or supplier is used to provide a product or service related to personal wellness data.

User.

A consumer who uses a company's product or service and from whom a company collects personal wellness data in connection with that product or service.

Personal Wellness Data.

Wellness data that a company collects, stores, or uses about an identified user through a device, software, or service that is primarily used to collect wellness data. However, data that has been reasonably deidentified[2] is not personal wellness data and therefore is not covered by these Principles.

[2] De-identification of data—removing information from data that could reasonably be used to identify an individual person—is a subject of intense debate. These Principles do not endorse any particular method of de-identification or set a standard for when data has been adequately de-identified. Instead, companies should use their expertise, taking into account the type and use of personal well- ness data and using the technical tools available to them, to determine how to de-identify such data.

III. Principles to Address Privacy and Security Risks

Security

Robust security measures are the foundation of good data management. While consumers have access to many tools that allow them to secure their data, companies must do their part to secure personal wellness data from the outset.

A company should secure personal wellness data by deploying measures that are reasonable and proportional to the sensitivity of that data, taking into account that consumers generally have heightened expectations of security with respect to personal wellness data. Companies should make arrangements with their vendors or suppliers who may handle personal wellness data to secure it using reasonable administrative, physical, and technical safeguards.

Policy and Practice

Consumers need to understand how personal wellness data is handled to be comfortable using health-related devices and services.

A company should have a clear and easily understood written policy for collecting, storing, using, and transferring personal wellness data. That policy should reflect broadly recognized fair information practice principles, address reasonably foreseeable security risks, and ensure compliance with applicable laws.

Concise Notice

Consumers may be unable to understand lengthy privacy policies, which would impede their ability to understand how personal wellness data is collected and used.

A company should make publicly available a summary of how it collects, stores, uses, and transfers personal wellness data. Companies are encouraged to provide these summaries in creative formats and through accessible methods that facilitate rapid learning, such as graphics, icons, charts, video, or audio.

Unaffiliated Third Party Transfers

Consumers seek transparency about and sometimes want to control personal wellness data transfers among companies.

A company should obtain affirmative consent before transferring personal wellness data to an unaffiliated third party, unless otherwise required by law or the company discloses in its privacy policy circumstances, such as emergencies, in which notice is sufficient. A company need not obtain affirmative consent from the user for subsequent personal wellness data transfers to the same unaffiliated third party, unless the type of personal wellness data to be transferred materially changes or the unaffiliated third party indicates a material change in the purpose for which it will use such data. Users should be able to revoke consent for the company to continue transferring personal wellness data to unaffiliated third parties at any time, unless otherwise required by law. A company should notify users if revoking consent will disable certain functions of a product or service.

Fairness

Personal wellness data collected from Internet of Things devices, combined with new data analytics, can provide many consumer benefits. Analytics can help consumers learn more about their health, enable them to reach their goals, and produce socially useful outcomes. Companies need to guard against the possibility that data analytics unintentionally could create unjust or prejudicial outcomes for consumers. While CTA is not aware of any such outcomes, this principle, which is inspired by existing U.S. federal, anti-discrimination laws, guards against that possibility throughout the lifecycle of their products.

A company should not knowingly use or disclose personal wellness data in ways that are likely to be unjust or prejudicial to consumers' eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance.

Companies are encouraged to periodically review algorithms or automated decision methodologies that use personal wellness data to guard against the possibility that they could create unjust or prejudicial outcomes for different categories of consumers.

Personal Data Review, Correction, and Deletion

Consumers wish to manage personal wellness data carefully. The ability to re- view, correct, or delete personal wellness data permits consumers to guard against inaccuracies or dissemination of the data beyond their control.

A company should provide a user with a means to review and correct the company's stored personal wellness data if the company intends to share it with a third party that will determine the user's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance. A company need not give a user the ability to review or correct personal wellness data if the user already has a means to do so.

A company should give a user the ability to request the deletion[3] of that user's personal wellness data and grant that request to the extent: (1) that deletion is technically, economically, and legally feasible, (2) that the company can attribute personal wellness data to the requesting user, and (3) that the user does not already have the ability to delete his or her personal wellness data. If a company transfers a user's personal wellness data to its vendor, supplier, or other service provider, that company should make technically, economically, and legally feasible efforts to promptly notify the transferee(s) that a user has requested deletion of his or her personal wellness data. Companies are encouraged to include in their contracts with vendors, suppliers, or other service providers a requirement that such transferees delete personal wellness data upon receiving notification from a company when technically, economically, and legally feasible.

Advertising Communications

Advertising is a useful tool that facilitates communication between companies and consumers. However, consumers want to control how personal wellness data is used for that communication.

A company that tailors advertising based on users' personal wellness data should provide users with the ability to opt out of such advertising.

[3] Deletion could mean either (1) erasure of the data or (2) removing information from data that could reasonably be used to identify an individual person. Such deletion should occur in a reasonable period of time reflective of the technical infrastructure at the company (for example, whether the company maintains personal wellness data on disaster recovery systems).

Consistent with the Unaffiliated Third Party Transfers Principle, a company should obtain affirmative user consent before knowingly transfer- ring personal wellness data to unaffiliated third parties who intend to use it for their own advertising purposes.

Law Enforcement Response

> *Consumers and companies alike are concerned about government access to personal wellness data. While companies must comply with legal process, they can be transparent with consumers about when and how they respond to lawful requests for data.*

A company's privacy policy should describe how it responds to requests for users' personal wellness data from federal, state, local, or foreign law and civil enforcement agencies.