ACT | The App Association

April 15, 2016

ATTN: Maya Uppaluru; Michael Lipinski
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human
Services 200 Independence Avenue, SW
Washington, District of Columbia 20201

RE: Comments of ACT | The App Association regarding the Office of the National Coordinator for Health Information Technology's Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice

ACT | The App Association writes to provide input to the Office of the National Coordinator for Health Information Technology (ONC) in response to its request for information on the scope and content of the ONC Voluntary Personal Health Record Model Privacy Notice (MPN).[1] ACT | The App Association appreciates the ONC's seeking of public input towards updating the MPN to better align with the current consumer health technology landscape.

ACT | The App Association represents more than 5,000 app companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions across modalities and segments of the economy, with healthcare as a prime example. Through our Connected Health Initiative (CHI), we clarify outdated health regulations, incentivize the use of remote patient monitoring, and foster an environment where patients and consumers can see improvement in their health.[2] This coalition of leading mobile health companies and key stakeholders works with Congress, the Federal Drug Administration (FDA), the Center for Medicare & Medicaid Services (CMS), and other key policymakers to promote policies that encourage mobile health innovation while keeping sensitive health data private and secure.

[1] Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice, 81 FR 10634 (Mar. 1, 2016) ("RFI").
[2] http://connectedhi.com/

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

I. General Views of ACT | The App Association on the FDA's Draft Guidance

ACT | The App Association agrees with ONC that the consumer health technology landscape has experienced a great deal of change since the MPN was first released. Today, connected health devices have the potential to radically improve American society. With over 60% of the population already using mobile apps to help track their conditions and make informed choices about their health,[3] mobile-app enabled innovations that utilize patient-generated health data (PGHD) continue to represent the most promising avenue for improved care quality, reduced hospitalizations, avoidance of complications, and improved satisfaction, particularly for the chronically ill.[4]

No data is more personal to Americans than their own health data. While the rise of the Internet of Things through an ever-increasing amount of Internet protocol-enabled products holds great promise, this environment also faces increasing security threats due to a broadened attack vector which necessitates more evolved and dynamic risk management practices. ACT | The App Association members appreciate this and put extensive resources into ensuring the security and privacy of sensitive health data to earn and maintain the trust of consumers, hospital systems, and providers. It is more important than ever for end users to understand companies' privacy and security policies and information practices. The MPN can and should augment how this important information is communicated to end users.

For these reasons, ACT | The App Association supports ONC's proposal to create a new version of the MPN that would expand its scope beyond personal health record companies and include more types of information practices.

II. Specific Views of ACT | The App Association on the FDA's Draft Guidance

Based on the above, ACT | The App Association provides the following specific recommendations in response to questions posed in the Request for Information (RFI).

[3] Get Mobile, Get Health: The Appification of Health & Fitness Report, Mobiquity (2014), available at https://www.mobiquityinc.com/mobiquity-white-papers?ref=mHealth-report-2014

[4] See, e.g., Hindricks, et al., The Lancet, Volume 384, Issue 9943, Pages 583 - 590, 16 August 2014 doi:10.1016/S0140-6736(14)61176-4.

1. User scope: What types of health technology developers, including non-covered entities and potentially HIPAA-covered entities, could and should use an updated voluntary MPN?

   ACT | The App Association tends to draw distinctions between three types of entities within the scope of those that are collecting PGHD:

   - The first category of these are health and fitness apps and devices which collect basic biometric information (e.g., Fitbit, Map My Run, etc.), including heart rate, calories consumed and burned, height, weight, age, etc.
   - The second are "wellness" entities, which are those technologies that allow for their users to maintain and monitor their own health outside of the care of a medical professional. Those apps would include apps for monitoring symptoms, monitoring glucose levels, heart rate over time, blood pressure over time, etc. The distinction is that there is no medical professional involved in the collection or maintenance of the data.
   - The third would be true medical apps and technologies that require the intervention of a physician. Those would include connected glucometers and applications created by and for hospitals/physician practices.

   All of these categories would benefit from a robust MPN. Those entities not covered by HIPAA would benefit most because the MPN will provide them with a template for being transparent with their users and an improved method for providing accurate and helpful privacy policies. Similarly, covered entities would have a better way to be transparent with their patients in a simple easy-to- understand way, rather than complex legal documents and forms.

2. Information type: What information types should be considered in and out of scope for the MPN? Examples could include, but are not limited to: Names, account access information, credit card numbers, IP address information, social security numbers, telephone numbers (cell and landline), GPS or geo-location data, data about how a consumer's body functions ranging from heart rate to menstrual cycle, genomic data, and exercise duration data such as number of steps or miles clocked.

   ACT | The App Association believes that any data points included in the 18 HIPAA identifiers[5] should be considered in scope for the MPN.

[5] 45 C.F.R. § 164.512(b)

3. Information practices: What types of practices involving the information types listed in Question 2 above should be included in the MPN? An information practice is what the company does with the data that it has collected. Types of practices that could be in scope for the MPN include, but are not limited to: Sale of data, including geo-location data; sale of anonymized or de-identified data, with or without restrictions on re- identification; sale of identifiable data; sale of statistics aggregated from identifiable data; use of data by the original collector to market products to the consumer; allowing third parties to use the data for marketing purposes; allowing government agencies to access the data, and for what purposes (such as law enforcement or public health); allowing researchers at academic and non-profit institutions to access either identifiable or de-identified data; access to the data by employers, schools, insurance companies or financial institutions with or without the consumer's consent; and retention or destruction of consumer data when the relationship between the health technology developer and consumer terminates.

   If a company is selling and/or sharing user data, that company should clearly explain why and how that data is being shared, and how it will be used. All of the following noted in the RFI should be covered by the MPN, as it is in the best interest of the consumer/user to understand how their data is being used outside the app:

   > Sale of data, including geo-location data; sale of anonymized or de- identified data, with or without restrictions on re-identification; sale of identifiable data; sale of statistics aggregated from identifiable data; use of data by the original collector to market products to the consumer; allowing third parties to use the data for marketing purposes; allowing government agencies to access the data, and for what purposes (such as law enforcement or public health); allowing researchers at academic and non- profit institutions to access either identifiable or de-identified data; access to the data by employers, schools, insurance companies, or financial institutions with or without the consumer's consent; and retention or destruction of consumer data when the relationship between the health technology developer and consumer terminates.[6]

   ACT | The App Association believes that companies should neither use or disclose health data for behavioral or interest based advertising, nor should they sell health data or otherwise transfer health data to advertising platforms, data brokers, or information resellers. However, we understand that some companies may use or disclose health data for behavioral or interest based advertising. These companies should therefore communicate with their users in a transparent way about how that data is/will/can be used. It is imperative that the MPN helps companies implement and foster that transparency.

[6] RFI at 10635.

4. Sharing and storage: What privacy and security issues are consumers most concerned about when their information is being collected, stored, or shared? Examples could include whether a health technology developer stores information in the cloud or on the consumer's device, or whether the information collected is accessed, used, disclosed, or stored in another country.

   ACT | The App Association members appreciate that no data is more personal to Americans than their own health data and put extensive resources into ensuring the security and privacy of sensitive health data to earn the trust of consumers, hospital systems, and providers. Fully leveraging technical measures, including end-to-end encryption (defined as a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key), is a critical element to accomplishing this. For example, the use of encryption is critical to meeting obligations under the above-noted HIPAA security and privacy rules. Assurances that such measures are being utilized will assuage many of these privacy and security concerns.

5. Security and encryption: What information should the MPN convey to the consumer regarding specific security practices, and what level of detail is appropriate for a consumer to understand? For example, a health technology developer could state that the product encrypts data at rest, or that it uses 128-bit or 256-bit encryption. How can information about various security practices, often technical in nature, be presented in a way that is understandable for the consumer? Examples could include encryption at rest or encryption in transit, or whether information is encrypted on the device or in the cloud.

   The MPN needs to help developers clearly outline their cybersecurity risk management practices and what is to be done in the event of data being compromised. The approach of each particular company will vary due to its circumstances, however, so the MPN should not be overly prescriptive in presuming specific security practices.

6. Access to other device information: What types of information that an application is able to access on a consumer's smartphone or computer should be disclosed? How should this be conveyed in the MPN? Examples include a health application accessing the content of a consumer's text messages, emails, address books, photo libraries, and phone call information.

   ACT | The App Association believes that the MPN should make known and clearly explain each method by which data held by a company will be accessed and disclosed.

7. Format: How should the MPN describe practices about the format in which consumer information is stored or transmitted (e.g., individually identifiable or de-identified, aggregate, or anonymized), particularly when their information is being shared with, or sold to, third parties? How should anonymized or de-identified information be defined for the purposes of the MPN? What existing definitions of "anonymized" or "de-identified" information are widely in use that could be potentially leveraged in conjunction with the MPN to clearly convey these practices to consumers?

   ACT | The App Association describes individually-identifiable Information as information that:

   - Relates to the past, present, or future
     - physical or mental health or condition of an individual;
     - the provision of health care to an individual; or
     - payment for the provision of health care to an individual; and
   - Identifies the individual; or
   - There's a reasonable basis to believe the information can be used to identify the individual.

Further, in ACT | The App Association's view, information can be de-identified in two ways.

First, under the "Safe Harbor" method, information that has had all of the following 18 identifiers removed is considered de-identified:

1. Names
2. Addresses or corresponding geolocation tags
3. Birth date, admission date, discharge date, and date of death
4. Phone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.

Second, information is considered de-identified if an expert statistician determines that there is only a very small chance of being able to identify someone from data even if some of the above identifiers are present.

8. Information portability: How should the MPN describe to consumers whether an application enables the consumer to download or transmit their health information? How should the MPN describe the consumer's ability to retrieve or move their data when the relationship between the consumer and the health technology developer terminates? Examples include if a consumer ends their subscription to a particular health technology service, or when a health technology developer's product is discontinued.

   ACT | The App Association believes the customer should have full control of their data. The MPN should help developers outline how customers can access and change or delete their data, how long the developer will keep the data after the customer deletes the account, and other relevant details.

Further, the MPN should make clear that the user should be in control of their health data. The goal of HIPAA is to improve patient access to their medical records. Similarly, innovative technologies should facilitate user control of their data. The MPN should help developers understand this and make it easy for the consumer to recognize as well. Outlining timelines for requesting data, when they will receive it, when it will be changed/deleted/etc., should therefore be built into the MPN.

III. Conclusion

ACT | The App Association appreciates the opportunity to provide input to the FDA on its Draft Guidance. The FDA is encouraged to contact ACT | The App Association with any questions.

Sincerely,

[signed]

Morgan Reed
Executive Director
ACT | The App Association