humetrix®

April 15, 2016

Via E-Mail to ONCMPN@hhs.gov

Dr. Karen DeSalvo
National Coordinator
Office of the National Coordinator for Health IT
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C., 20201

Re: Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice

Dear Dr. DeSalvo:

Thank you for the opportunity to provide feedback on the Office of the National Coordinator for Health Information Technology's ("ONC's") efforts to further modernize the Personal Health Record Model Privacy Notice ("MPN"). Humetrix has been using the current MPN with respect to a number of its applications, such as the ONC award-winning iBlueButton, since 2013. We look forward to ONC updating the MPN and appreciate this opportunity to share our experience and suggestions.

For your convenience, we have provided our comments in response to the topics that you have identified.

1. ***User Scope***

Question:

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

Response:

We encourage the use of the MPN by any consumer-facing applications that collect health or fitness information about a consumer. This would include both HIPAA-covered entities and entities that are not covered by HIPAA.

We recommend against limiting the scope of the MPN to "personal health records." First, with multifunction apps, it has become increasingly difficult to distinguish what is or is not a personal health record. For example, many apps maintain consumer health information as a byproduct of their service, but may not be thought of as a "personal health record" because

storage of health information on behalf of the consumer is not the app's primary function. Second, "personal health record" is a term with which most consumers are not familiar.

Additionally, we caution against limiting the scope of MPN to "health" and suggest inclusion of fitness apps. This is because the line between health and fitness data continues to blur, with an increasing number of apps potentially collect both types of information.

2. Information Type

Question:

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.

Response:

We recommend that the MPN encompass all of the categories of information provided as examples, along with any other information that is collected about a consumer, including aggregate, statistical, and de-identified information. This is especially important for information that the consumer does not input and may not recognize is being collected, such as geo-location information.

While we believe that a consumer has a lesser privacy interest in the use or disclosure of aggregate, statistical, or de-identified information, we nevertheless recommend addressing these types of information in the MPN. First, other than the de-identification standards under HIPAA, there may be ambiguity as to what qualifies as "aggregate" or "statistical" data. Accordingly, information that is described as "aggregate" may be re-identifiable by the recipient. Second, some consumers may be less inclined to use an app if their information is being used and disclosed for any secondary purpose, even at an aggregate level.

We also recommend aligning the MPN with EU standards to the extent feasible. Apps are potentially used on a global scale, and an MPN that is consistent with standards and expectations outside of the United States would be very helpful for app developers.

3. Information Practices

Question:

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; retention or destruction of consumer data when the relationship between the health technology developer and consumer terminates.

Response:

We recommend that the MPN seek to identify any uses and disclosures that are unrelated to providing the app service. This is because any such use or disclosure would not necessarily be anticipated by the consumer. These can be broken out into: (1) internal uses of identifiable data; (2) internal uses of aggregate, statistical, or de-identified data; (3) external disclosure of identifiable data; and (4) external disclosure of aggregate, statistical, or de-identified data. For external disclosures, we recommend identifying whether it will involve the sale of the data.

We recommend against limiting the list of uses and disclosures to only a few categories, as was done in the original MPN. The consumer potentially has an interest in any use or disclosure that is unrelated to providing the service, even if it is not for "marketing and advertising," for example.

We recognize the challenge in potentially offering this much information in a user-friendly manner. First, we recommend against primarily offering the MPN as a PDF. This format does not necessarily work well on small screens, yet the consumers using these apps will often be accessing the information from a mobile device with a small screen, such as a smartphone. Instead, we recommend that ONC create an online tool where companies can enter the information necessary to generate the model notice, and then the tool would create code for an HTML page that is optimized for viewing on mobile devices.

Instead of the current format, we recommend using a layered format that can provide a clean, high-level view, while offering the consumer an easy way to learn more information if the consumer would like to do so.

For example, instead of trying to identify five particular types of disclosures, as was done in the previous format, the MPN can provide the following:

> **Is your identifiable information disclosed to others in order to provide the service? Yes/No**

[If yes, the individual can expand to see how information is disclosed to others to provide the service. This could include identifying a cloud-based hosting company, and the option to include a link to its notice of privacy practices.]

Other than when required by law, is your identifiable information disclosed to others for a purpose that is unrelated to providing the service? Yes/No

[If yes, identify to whom identifiable information is disclosed (by name or class of entities), for what purpose, and whether in exchange for remuneration.]

Such a layered approach can preserve benefits of the "soup label" concept, giving consumers immediate access to the information that is most important to them in a manner that is the same across different companies. By including the ability to expand the answers, consumers can drill down to obtain more details. This format may also work better on smaller screens, rather than the current table approach.

We recommend that the MPN include certain template language for the expanded answers and in a particular order. This way, if an app is storing information using a cloud provider, this will be presented in the same manner and will always be presented in the same spot. But the template should provide some optional elements, such as the option of whether to identify a third party by name (such as an infrastructure-as-a-service provider) and whether to link to the third party's notice of privacy practices. The template should also provide ample room to identify "other" information, such as a disclosure to a third party that is unusual and, therefore, for which there is not template language.

4. Sharing and Storage

Question:

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.

Answer:

We recommend identifying: (1) whether the information is stored on the consumer's device; (2) whether the consumer's information is stored by the company in the cloud (either the only copy of the information or a backup of the information); (3) whether the information is stored with a third party (and, optionally, providing a link to the privacy notice of the third party); and (4) whether the information is accessed, used, disclosed, or stored in another country (and, optionally, providing information on what country, as some countries have potentially greater privacy protections than the U.S.).

5. Security and Encryption

Question:

What information should the MPN convey to the consumer regarding specific security practices? 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.

Response:

We recommend providing consumers information about: (1) whether their information is encrypted when transmitted and what level of encryption; (2) whether their information is encrypted when stored and what level of encryption; (3) whether the company providing the app has access to the unencrypted information; (4) whether any third parties (e.g., a cloud provider) have access to unencrypted information; (5) whether the company subscribes to any particular information security framework (e.g., ISO 27001) and, if so, the identification of such a framework; and (5) whether the company's information security practices have been assessed by an independent third party (with the option of providing the most recent certification or report). Information security is complicated, and it may be far more telling to identify whether the company subscribes to a particular information security framework and has had an independent assessment, rather than trying to focus on particular information security details.

6. Access to Other Device Information

Question:

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.

Response:

We recommend that the MPN identify whether the app will collect information from the operating system or other apps (such as photos, address books, phone call information, etc.) and from sensors, such as the device's camera, microphone, GPS, or accelerometer. We also recommend identifying whether the app will post information to the operating system or other apps, such as putting information on a calendar, leaving photos in the smartphone's general photo library, etc. For example, a device's calendar may be shared with other people (e.g., it may integrate with a work calendar or a shared online calendar), so it is important to know whether

potentially sensitive health information could be added to the device's calendar, which may be accessible to others.

7. Format

Question:

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?

Response:

We recommend distinguishing between the following: (1) identifiable information; (2) aggregate information that has not been de-identified in accordance with HIPAA standards (with optional space to identify what information has been removed); and (3) information that has been de-identified in accordance with HIPAA standards. While we recognize that consumers generally will not be familiar with HIPAA de-identification standards, we nevertheless recommend identifying whether de-identification satisfies HIPAA standards because HIPAA offers one of the only recognized standards for de-identification.

8. Information Portability

Question:

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.

Response:

We recommend that the MPN identify whether: (1) the consumer has the ability to download a copy of their information at any point in time, including after they terminate use of the app (and, if so, for how long after); (2) how the consumer can do so, and if there is any charge; and (3) what format the information will be in.

* * * * *

Thank you again for the opportunity to provide comments on ONC's updating of the MPN. We look forward to staying engaged with ONC on this critical issue. Please do not hesitate to reach out to me if I can be a resource on this or any other issue.

Sincerely,

[Signed]

Bettina Experton, MD, MPH
President & CEO
HUMETRIX
1155 Camino del Mar, #503
Del Mar, CA 92014, USA
Tel: (858) 259-8987, Ext. 210
Cell: (619) 980-5888