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

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?

   Our opinion: Non-covered entities that provide health applications, devices, or other tools or media that capture, collect, use, or analyze health data used by consumers to make decisions about health, fitness, and healthcare should be covered under the Privacy Notice. There are many tools that can be used by consumers in the area of Patient (consumer) Generated Health Data. This includes FDA approved devices such as pacemakers and insulin pumps and non-FDA approved devices such as fitness monitors and health applications. It is important that consumers be informed about how their information will be used. Further, information communicated by the health / medical device should clearly indicate the source for this advice so that the consumer is not mislead (or that the application is not practice medicine without a license).

   Covered entities are subject to HIPAA.

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.

   Our opinion: All data captured, collected, and used by consumers used by consumers to make decisions about health, fitness, and healthcare should be covered under by the Privacy Notice.

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.

   Our opinion: Consumers have a right to know how their data will be used. This is communicated in the Privacy Notice.

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.

   Our opinion: No PHI or PII should be stored outside of the United States. There is no way to enforce security, privacy, breech or enforcement of HIPAA outside of our borders. Further, we believe that the use of the word "cloud" is problematic in that most commercial applications are technically using "cloud" technology. The important key here is the data under the control of the entity (device manufacture or software), that the data center can be audited for compliance, and whether sufficient security exists to protect the data from breech.

   Consumers should have the right to share data with the individual of their choice. Further, HIPAA provides the ability for a covered entity access to data for treatment, payment and operations.

5. S*ecurity 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.

   Our opinion: All PHI and PII data should be encrypted at rest and inflight. Websites should utilize secure protocols (e.g. https://). Further, this should be explained to consumers in plain English. There should be standard / defined meanings that are used consistently by all entities with the ability to drill down to the technical specifications.

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.

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?

Our Opinion: Consumers should have the right to choose how their data will be used by non-HIPAA covered entities including the ability to block the sale of PHI and PII to third parties. HIPAA allows the sharing of data with covered entities and the business associates of covered entities for treatment, payment and operations. Further, HIPAA provides the frame work for how de-identified data can be shared. This should be communicated to the consumer in the Notice of Privacy.

Consumers should be ID-Proofed with a high level of assurance to identify the person such as LoA3 (Level of Assurance 3) in NIST 800-63-2. This will allow proper identification of the individual and help promote interoperability because providers will be able to trust that the person communicating with them is ID-Proofed and authenticated to be the actual person and not someone attempting inappropriate use of the information (e.g. identity theft).

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.

   Our Opinion: Consumers own their health data and should be able to view, download and transmit data to an electronic end point. Today, this type of exchange can be performed by using the Direct Protocol. In the future this will most likely be FHIR.

   At the termination of the relationship, the entity hold the consumers' data no longer has the right to keep that data and should be required to destroy that data.