Department of Health and Human Services

Office of the Secretary

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

AGENCY: Office of the National Coordinator for Health Information Technology, Department of Health and Human Services.

ACTION: Notice with comment; request for information.

SUMMARY: The Office of the National Coordinator for Health Information Technology (ONC) seeks comments on the scope and content of the voluntary Personal Health Record Model Privacy Notice (MPN) developed by ONC and published in 2011. In response to stakeholder requests for an electronic means to inform consumers about how health technology products store, use, and share health information (especially products of health technology developers not covered by the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191), we have initiated a process to update the MPN to better align with the current consumer health technology landscape.

DATES: To be assured consideration, electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on **[INSERT DATE 45 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by MPN RFI, by either of the following two methods (please do not submit duplicate comments).

- ONC website: Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft

Word. https://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice

- Email: ONCMPN@hhs.gov

FOR FURTHER INFORMATION CONTACT: Maya Uppaluru or Michael Lipinski, 202-690-7151.

SUPPLEMENTARY INFORMATION: In June 2008, the Office of the National Coordinator for Health Information Technology (ONC) began a multi-phase and iterative project to develop an easy-to-understand, voluntary Personal Health Record (PHR) Model Privacy Notice (MPN) that any PHR company could adopt to communicate its information practices to its users. Developed in collaboration with the Federal Trade Commission (FTC), the project's goals were two-fold: (1) increase consumers' awareness of PHR companies' information practices; and (2) empower consumers by providing them with an easy way to compare the information practices of two or more PHR companies. The MPN was designed to enable PHR companies to easily enter their information practices and produce a notice to allow consumers to quickly learn and understand privacy and security policies and information practices, compare PHR company practices, and make informed decisions. Similar to the Food and Drug Administration's Nutrition Facts Label, this approach did not mandate specific policies, but rather was meant to encourage user-friendly transparency of a company's existing practices.

The MPN has two sections: 1) the "Release" section; and 2) the "Secure" section. Both sections of the MPN include model language that informs consumers about how a PHR company is using an individual's health information. The current MPN can be found here, but we note that it is no longer available for use. Additional background on the MPN can be found at:

https://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice.

Since the development of the MPN, the consumer health technology landscape has greatly evolved. More consumers are now able to electronically access their health information than ever before. Not only are consumers interacting with their clinical and claims data (often collected and maintained by health care providers and health plans regulated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (i.e., "covered entities")), but they are also interacting with fitness and wellness data from devices offered by health technology developers that may not be regulated by HIPAA. In general, HIPAA regulations govern how covered entities and their business associates maintain, access, use and disclose individually identifiable health information and protected health information, otherwise known as "PHI".[1] Specifically, the HIPAA regulations include requirements for: keeping information private in the Privacy Rule,[2] which also includes notifying individuals about how their PHI can be accessed, used, and disclosed [3]; adopting administrative, technical and physical safeguards to secure electronic PHI[4]; and mandating notice to affected individuals when a breach of PHI occurs[5]. Health technology developers that may not be covered by HIPAA are often called "non-covered entities" or "NCEs."

Health technology developers make available a diverse array of products, including mobile apps, wearable devices, and sensors, and often display notices of their privacy and information practices to consumers. These developers may be subject to other federal laws,

[1] 45 CFR 160.103.
[2] 45 CFR 164.501 et seq.
[3] 45 CFR 164.520; see also Office of Civil Rights Model Notices of Privacy Practices: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/
[4] 45 CFR 164.301 et seq.
[5] 45 CFR 164.400-414

including the FTC Act's prohibition on unfair or deceptive acts or practices[6], and the FTC's Health Breach Notification Rule[7] which requires notification to affected individuals when a breach of data occurs.

We are considering creating a new version of the MPN that would expand its scope beyond PHR companies and include more types of information practices. A modernized MPN would serve as a voluntary resource for health technology developers who want to give notice of their information practices to their users in an understandable way. Therefore, ONC requests public comment from consumers, mobile and web application developers, privacy advocates, user experience and design experts, and other health technology stakeholders on any updates that should be made to the content of the MPN to make it more useful to both health technology developers and consumers.

While we encourage comments on all aspects of the MPN, ONC specifically seeks comment on the topics specified below. We note that the MPN does not recommend best practices to health technology developers, and we do not seek recommendations about best practices. Rather, ONC seeks comment concerning what information practices health technology developers should disclose to consumers and what language should be used to describe those practices in an updated MPN. Examples of information practices below are included to clarify the intent of the questions, but are not intended to be exhaustive. ONC invites commenters to discuss any examples that are relevant to the broad issues of which types of personal information and information practices should be addressed in an updated MPN.

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?

[6] 15 U.S.C. 45(a) (Section 5 of the FTC Act).
[7] 16 CFR part 318.

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.
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.
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.

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.
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[8]?
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

[8] See, e.g., 45 CFR 164.514(a) (HIPAA Privacy Rule) as a potential standard for de-identification of protected health information.

consumer ends their subscription to a particular health technology service, or when a health technology developer's product is discontinued.

ONC seeks broad input from stakeholders on updating the MPN so that the tool is useful for current health technology developers and consumers. Individuals and organizations with common interests are urged to both coordinate and consolidate their comments.

Authority: 42 U.S.C. 300jj-11; Office of the National Coordinator for Health Information Technology; Delegation of Authority (76 FR 58006, Sept.19, 2011).

Dated: February 23, 2016.

_____

Karen DeSalvo,

National Coordinator for Health Information Technology.

BILLING CODE: 4150-45-P

[FR Doc. 2016-04239 Filed: 2/26/2016 4:15 pm; Publication Date: 3/1/2016]