2016 Model Privacy Notice

Draft Preamble

As of December 2, 2016

The Model Privacy Notice (MPN) is a voluntary, openly available resource designed to help health technology developers provide transparent notice to consumers about what happens to their digital health data when the consumer uses the developer's product. The MPN's approach is to provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.

The Office of the National Coordinator for Health Information Technology (ONC) is updating the 2011 version of the MPN. The 2011 version focused on personal health records (PHRs), which were the emerging technology at the time. The health information technology market has changed significantly in the last five years and there is now a larger variety of products such as exercise trackers, wearable health technologies, or mobile applications that help individuals monitor various body measurements. As such, it is increasingly important for consumers to be aware of health technology developers' privacy and security policies, including data sharing practices.

Preamble for Health Technology Developers	
What is the Model Privacy Notice (MPN)?	The MPN is a voluntary, openly available resource to help health technology developers who collect digital health data clearly convey information about their privacy policies to their users. Similar to a nutritional label, the MPN provides a snapshot of a company's existing privacy and security policies to encourage transparency and help consumers make informed choices when selecting products. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.
Who is the MPN for?	The MPN is for health technology developers whose technology or app uses and/or shares users' health data[1].
What laws might apply to you?	Health technology developers should consult the Federal Trade Commission (FTC)'s Mobile Health Apps Interactive Tool (which was developed in conjunction with the following Department of Health and Human Services offices and agency: ONC, Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)) to determine if they need to comply with the FTC Act, the FTC's Health Breach Notification Rule, HHS's Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules, or FDA rules implementing the Federal Food, Drug & Cosmetic Act, as applicable. This tool is not meant to be legal advice about all compliance obligations, but identifies relevant laws and regulations from these three federal agencies.
Does use of this MPN satisfy HIPAA requirements to provide a notice of privacy practices?	No. The MPN does not ensure compliance with HIPAA or any other law. However, the MPN may be used, as applicable, in conjunction with a HIPAA notice of privacy practices (please see MPN). To find more information on HIPAA directed towards health technology developers, visit the HIPAA Q's Portal for Health App Developers.

2016 Model Privacy Notice

Draft Content

As of December 2, 2016

Note: Developers of consumer health technology or apps ("health technology developers") that collect digital health data about individuals would use this template to disclose to consumers the developer's privacy and security policies. "**We**" refers to the health technology developer or technology product and "**you/your**" refers to the user/consumer of the health technology. For all endnotes provided in the MPN, the information specified in the endnote is required to be included in the privacy notice. However, for purposes of the Challenge, flexibility is permitted for how the information is presented (e.g., use of a link or pop up box) as long as the format maintains clear interfaces.

***Directions for the health technology developer:** If the health technology developer is a HIPAA covered entity, select one of the following statements to be inserted in the privacy notice:

Option 1: Please note that the health data we collect as part of this [insert name of technology product] are not protected by HIPAA and our company's HIPAA Notice of Privacy Practices does not apply.
Option 2: Some of the health data we collect as part of this [insert name of technology product] also are protected by HIPAA. Read our HIPAA Notice of Privacy Practices (embed link or popup] for more information.

Use: How we use your data internally
We collect and use your **identifiable data**[2]: ☐ To provide the primary service[3] of the app or technology ☐ To develop marketing materials for our products ☐ To conduct scientific research ☐ For company operations (e.g., quality control or fraud detection) ☐ To develop and improve new and current products and services (e.g., analytics[4]) ☐ Other: _____
Share: How we share your data externally with other companies or entities
We share your **identifiable data**[5]: ☐ To provide the primary service[6] of the app or technology ☐ To conduct scientific research ☐ For company operations (e.g. quality control or fraud detection) ☐ To develop and improve new and current products and services (e.g., analytics[7]) ☐ Other:_____ ☐ We DO NOT share your identifiable data[8]
We share your **data AFTER removing identifiers (note that remaining data may not be anonymous):** ☐ For the primary purposes of the app or technology ☐ To conduct scientific research ☐ For company operations (e.g., quality control, fraud detection) ☐ To develop and improve new and current products and services (e.g., analytics[9]) ☐ Other:_____ ☐ We DO NOT share your data after removing identifiers

Sell: Who we sell your data to	
We sell your **identifiable data**[10] to data brokers[11], marketing, advertising networks, or analytics firms**.**	☐ Yes ☐ Yes; only with your permission[12] ☐ No
We sell your **data AFTER removing identifiers (note that remaining data may not be anonymous)** to data brokers[13], marketing, advertising networks, or analytics firms.	☐ Yes ☐ Yes; only with your permission[14] ☐ No
Store: How we store your data	
Are your data stored on the device?	Yes / No
Are your data stored outside the device at our company or through a third party?	Yes / No
Encryption: How we encrypt your data	
Does the app or technology use encryption[15] to…	
encrypt your data in the device or app?	☐ Yes, by default ☐ Yes, when you take certain steps (click to learn how) ☐ No ☐ N/A
encrypt your data when stored on our company servers or with an outside cloud computing[16] services provider?	☐ Yes, by default ☐ Yes, when you take certain steps (click to learn how) ☐ No ☐ N/A
encrypt your data while it is transmitted?	☐ Yes, by default ☐ Yes, when you take certain steps (click to learn how) ☐ No ☐ N/A
Privacy: How this technology accesses other data	
Will this technology or app request access to other device data or applications, such as your phone's camera, photos, or contacts?	☐ Yes, only with your permission. It connects to... ☐ Camera ☐ Photos ☐ Contacts ☐ Location services ☐ Microphone ☐ Health monitoring devices ☐ Other: _____ ☐ [If yes] Here is how you can check your settings, including permissions set as a default…No
Does this technology or app allow you to share the collected data with your social media accounts, like Facebook?	☐ Yes ☐ Yes, only with your permission. ☐ [If yes] Here is how you can check your settings…No

User Options: What you can do with the data that we collect	
Can you access, edit, share, or delete the data we have about you?	☐ Yes. You can… ☐ Access your data ☐ Edit your data ☐ Share your data ☐ Delete your data [If yes] Here is how to do this… ☐ No
Deactivation[17]: What happens to your data when your account is deactivated	
When your account is deactivated/terminated by you or the company, your data are…	☐ Deleted immediately ☐ Deleted after x years ☐ Permanently retained and used ☐ Retained and used until you request deletion
Policy Changes: How we will notify you if our privacy policy changes	
Describe how/if the company will notify consumers of privacy policy changes (e.g. merger or acquisition) and provide link to section in privacy policy.	
Breach[18]: How we will notify you and protect your data in case of an improper disclosure	
(Company name] complies with all applicable laws regarding breaches. Describe how the company will protect consumers' data in the case of a breach and provide link to section in privacy policy.	
Contact Us	
[Legal Entity Name] **[Link to full privacy policy]** **[Link to Online Comment/Contact Form]** **[Email Address]** **[Phone Number]** **[Address; minimum, Country]**	

[1] Health data can include, but is not limited to: wellness information (e.g., exercise or fitness habits, nutrition, or sleep data), health markers (e.g., blood pressure, BMI, or glucose), information on physical or mental health conditions, insurance or health care information, or information that integrates into or receives information from a personal health record.

[2] Include definition of "identifiable data." Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.

[3] If unclear, specify what the developer considers the primary service.

[4] Include definition of "analytics." Analytics means: the process of examining data to draw conclusions from that information. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.

[5] Include definition of "identifiable data." Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.

[6] If unclear, specify what the developer considers the primary service.

[7] Include definition of "analytics." Analytics means: the process of examining data to draw conclusions from that information. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.
[8] Include definition of "identifiable data." Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.
[9] Include definition of "analytics." Analytics means: the process of examining data to draw conclusions from that information. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.
[10] Include definition of "identifiable data." Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.
[11] Include definition of "data broker." Data broker means: companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies (*From FTC: https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data).*
[12] Direct consumers how to adjust permissions.
[13] Include definition of "data broker." Data broker means: companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies (*From FTC: https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data).*
[14] Direct consumers how to adjust permissions.
[15] Include definition of "encryption." Encryption means: a method of converting an original message of regular text into encoded text in such a way that only authorized parties can read it. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.
[16] Include definition of "cloud computing." Cloud computing means: a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.
[17] Include definition of "deactivation." Deactivation means: an individual takes action or a company ceases operation or deactivates an individual's account due to inactivity. *Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback*.
[18] Include definition of "breach." Breach means: an unauthorized disclosure.