patientprivacyrights

Model Privacy Notice Comments
April 15, 2016

RE:
https://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-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?

All institutions and corporations holding patient-level health-related data should be subject to a MPN. That includes HIPAA CEs, HIPAA BAs that aggregate data from more than one HIPAA CE (e.g.: HIEs), data brokers that aggregate data from HIPAA CEs and BAs (e.g.: Surescripts), research and academic registries, state registries (e.g.: All Payer Claims Databases, Relationship Locator Services of HIEs), wearables, all wellness programs, implants that communicate data to a vendor for screening (e.g.: implantable cardiac defibrillators), and apps that collect health data from patients such as PHRs.

As with the nutrition labels that inspired the MPN, the use of the MPN should be mandatory, not voluntary.

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 geolocation 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.

All information that is part of the MU common clinical data set and any information that is to be associated with such information should be included. For example, a wellness program that combines blood pressure and weight (both elements of a clinical data set) with steps taken would be covered. A wearable that only collects steps and does not make claims or provide APIs that relate to aggregation with clinical data would not be required.

Come to think of it, if the MPN is voluntary, how would anything be in or out of scope?

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.

The most important information practice is transparency as in accounting for disclosures. Any uses of personal-level information, even if de-identified or exempted by HIPAA TPO, should be transparent to the person. That transparency should be as convenient as we expect with banking and internet commerce sites, meaning there is real-time online access, an available API, and notification. These transparency practices are already common outside health care because they contribute trust and because they are very important security measures. Transparency on uses of health data should be held to an even higher standard than other types of personal data.

The second most important information practice is providing access to the information first to the individual before asking for consent or authorization to share it for any other purpose. This essential "right of access" serves to keep the data holders honest because they risk patients moving their data to another data holder without notice. The MPN must highlight any asymmetry or discrepancy in what data is available through patient-directed API vs. held for use and sharing under control of the data holder.

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.

Systems of sharing and storage should be clearly labeled into one of three classes:

- Class 1: "The vendor does not see your data - all access is through a patient-controlled API." (e.g.: Apple HealthKit, ResearchKit);
- Class 2: "The vendor has access to the your data but the patient-controlled API also has full access." (e.g.: a modern email or calendar service);
- Class 3: "The vendor has access to your data and the patient has little or no API access." (e.g.: pretty much all of HIPAA CEs and most PHRs.).

Aside from the three classes of data stewardship, the actual place where data is stored may not be that important. Privacy laws in some EU countries such as Germany and Switzerland already make these locations preferable to the US. Storage in the US does not typically give users any

obvious protection or right of action beyond what is enforceable by FTC regardless of where data is stored. The jurisdiction where data is stored and/or processed should be specified.

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.

Encryption and security is way beyond the ability of any consumer to judge. Encryption should not be mentioned in the MPN in health care any more than it is mentioned in our banking relationships - which is never. Unless and until the terminology around encryption is regulated by the FTC or some other agency, including it in MPN is akin to adding undefined and unenforced terms like “natural” to a food label.

History has shown that claims of encryption and security in healthcare are vastly more often used to block access and obscure uses than to improve service or accountability (e.g.: DirectTrust).

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.

This seems like a silly question. What kind of information access on my smartphone or computer should NOT be 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 ?

Information is either stored and shared in individual or aggregated form. Any sharing of information at an individual level needs to be subject to transparency and authorization regardless of whether it’s de-identified or not. This is because consumers are not in any position to judge how likely information is to be re-identified and there is no practical enforcement mechanism for holding de-identification accountable outside of HIPAA. Even within HIPAA, the ability to audit and enforce de-identification is very limited. For example, what regulations apply to the creation of longitudinal profiles by data brokers such as IMS Health and Optum that source data from HIPAA CEs?

De-identification should be performed by entities that are under the patient’s control and separate from the service provider that collected the data. This would allow competition for good de-identification and other privacy practices and it would reduce the taking of economically valuable personal data without compensation of the patient under guise of de-identification.

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.

First, and most important, the MPN must characterize the data holder as Class 1, 2 or 3 according to their API practices as described in question 4, above. Only live APIs can reasonably ensure data portability because being presented with a "data dump" when one decides to move to a different service is almost universally impractical. The MPN needs to make clear how much of the data is NOT available live via API and whether the data that is NOT available via API is available at the termination of service in a specified standard format and at a specified cost.

Adrian Gropper, MD
CTO
Patient Privacy Rights

Deborah Peel, MD
President and Founder
Patient Privacy Rights