GetMyHealthData

April 15, 2016

Dr. Karen DeSalvo, M.D., M.P.H., M.Sc.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW
Washington, D.C. 20024

Re: Request for Information on Updates to the ONC Model Privacy Notice

Dear Dr. DeSalvo:

Thank you for the opportunity to share the consumer perspective on an updated version of the Model Privacy Notice. We agree with ONC that the Model Notice is a valuable tool, and that updates are appropriate given the diversity of electronic tools and information now available to consumers.

GetMyHealthData is a national campaign designed to help patients gain access to their health information in electronic, computable formats.[1] We provide patients with information, tips and other resources that help them understand how to get their health data from providers and other data holders, and we help them troubleshoot and overcome obstacles along the way.

The current way we as a nation educate consumers on privacy policies is not very effective. GetMyHealthData has examined many privacy policies of entities like health apps in our work to help consumers get and use their health data, and we have found that policies are long and complicated, they vary widely in what they cover, and some inappropriately use the same policy for their app as their regular website.

To try and make sense of these policies for consumers, we developed our own **survey of health apps** focused on the services, policies, practices and costs of any app that voluntarily completes our assessment.[2] Our survey also includes whether or not the developer uses the Model Privacy Notice because we believe that **consumers are more likely to absorb the salient points of a notice that is displayed in a digestible way, instead of clicking "accept" without reading** dense legal text filled with technical terms and jargon. A Model Notice helps enable consumers to make truly informed choices about the platforms they use, the data they share and the devices they connect to.

There is no question **patients want to know how their health information is collected and used**; almost nine in 10 consider it important.[3] Information about privacy practices is vital as consumers increasingly manage their health data using smartphone apps and other electronic platforms that are not covered by HIPAA.

INFORMATION PRACTICES DISCLOSED

---

[1] Coordinated by the National Partnership for Women & Families, a non-profit consumer organization, collaborators include AHIMA, the Alliance for Nursing Informatics, Amida, Code for America, Flip the Clinic, the Genetic Alliance, Health Data Consortium, NATE and other individual thought leaders/experts.

[2] GetMyHealthData has created a list of health apps which openly shared information with us about their policies and practices, services and costs. We do not endorse any single product**,** nor do we have any financial relationships with these organizations; instead, we provide individuals with clear information so they can make the best choice for them. https://getmyhealthdata.org/home/using-your-data/

[3] National Partnership for Women & Families, *Engaging Patients and Families: How Consumers Value and Use Health IT* (Dec. 2014), available at http://www.nationalpartnership.org/research-library/health-care/HIT/engaging-patients-and-families.pdf.

The guiding principle for the development and implementation of the Model Privacy Notice must be equipping patients with information that is accessible and understandable so they may make meaningful choices[4] about how and where they store their personal health information. Consumers should never be surprised to learn about the uses of their data.

User scope

Both covered and non-covered entities should be encouraged to adopt the Model Privacy Notice.

- Regardless of HIPAA status, the Model Notice makes privacy policies more accessible and understandable, facilitating meaningful choice.
- For non-covered entities who lack a legal requirement to disclose privacy practices, the Model Privacy Notice format provides not only guidance about policy content, but a vehicle for disclosing practices in a meaningful, accessible way.
- Further, the Model Privacy Notice is essential for non-covered entities given that they are subject to federal policies regarding Unfair and Deceptive Trade Practices, as enforced by the Federal Trade Commission (FTC). This, we believe, is an important attribute of the Model Privacy Notice – it can be enforced by the FTC if the entity discloses data in practice in ways they say they do not.

In our experience, covered entity status can be confusing for consumers. The privacy policies of several apps we have reviewed clearly state they are "HIPAA compliant," whether they are a covered entity or not. However, HIPAA (under the Privacy Rule) allows for the disclosure of identifiable health information *without patients' consent* for the purpose of treatment, payment or operations (TPO).

- While claiming "HIPAA compliance" may be intended to give consumers confidence with respect to security, making this claim would also permit the app to disclose identifiable data for TPO without consent, which would likely come as a surprise to consumers. That would violate the concept of meaningful choice, and undermine consumer trust.

Information type

Because the Model Notice is voluntary, its design has to be relatively easy to use for developers. Our assumption is that consumers will have already researched the types of data, generally speaking, that the technology will hold or have access to, based on the specific purpose they are considering.

- ONC could consider an extensible design where developers could add relevant data types to the Model Notice in an automated/check box way.
- It may also be wise to distinguish between broad categories of information types – such as demographic and related personal information (SSN, etc.), versus personal identifiable health information.

Information practices

While the sale of data and the use by the app for marketing purposes are important practices to disclose, we also note that consumers want to understand any circumstance under which their identifiable information is disclosed without their explicit consent. Sale and use in marketing are just two examples, but there are more, including those listed in the existing Model Privacy Notice.

- We suggest that categories of information practices distinguish whether disclosures are made with or without consumers' explicit authorization, and whether the data is identifiable or not. For instance, does the app disclose a particular category of information to a third-party without authorization? Does it access information from the user's smartphone without authorization or with the consumer's knowledge?

---

[4] Meaningful choice is based on the recommendations of the HIT Policy Committee found here. Two elements of meaningful choice (aka: meaningful consent) are particularly applicable here: Meaningful consent "Provides full transparency and education. (I.e., the individual gets a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the decision-making moment.)" It also "Is commensurate with the circumstances. (I.e., the more sensitive, personally exposing, or inscrutable the activity, the more specific the consent mechanism. Activities that depart significantly from patient reasonable expectations require greater degree of education, time to make decision, opportunity to discuss with provider, etc.)"

- We encourage ONC to keep its structure from the previous Model Privacy Notice that displays each information practice in terms of the release of identifiable data and de-identified data.

We have also found that, for developers to fill out the Model Notice accurately, it is important to **distinguish between an information practice and a function** that a user could select and voluntarily use. For example, a developer might disclose data to a researcher, but only at the consumer's request. The Model Notice must have clear instructions that delineate the two.

Information portability
We strongly agree with ONC's recognition that there should be a category showing whether users can download their data from the technology when their relationship ends. This policy is in line with GetMyHealthData's review of apps, through which we help consumers know whether or not they can ultimately take their data with them when they stop using the app, the company goes out of business, etc.

LANGUAGE USED TO DESCRIBE PRACTICES
The Model Notice needs to strike a balance between being comprehensive while still usable by both consumers and developers, and language is a key element of usability. We suggest using categories of "identifiable" and "de-identified" or "anonymous" data when categorizing information practices. Although the previous version of the Model Notice uses "personal" and "statistical" data, we find these terms confusing. We have not conducted user testing of "identifiable" and "de-identified" or "anonymous," and ONC would be wise to do so resources permitting, but we believe them to be more clearly understood than "statistical."

Explaining security practices is complex and technical. We have no data to indicate the best approach, but we suspect that describing details, such as 128-bit or 256-bit encryption, won't be meaningful for the vast majority of users. Another approach is to identify a benchmark for appropriate security practices and note compliance with that benchmark. We wonder whether the HIPAA Security Rule may suffice (provided that there is a basic definition of the Security Rule to briefly explain requirements).

Finally, it is essential to incentivize developers to use the Model Privacy Notice. It will not suffice to create a useful and usable tool; instead, there need to be efforts to encourage its widespread adoption. ONC must also make clear in its dissemination of the Model Notice that it does not mandate data sharing policies, but instead provides a voluntary way for displaying information. In our work with developers, this is greatly misunderstood.

Thank you again for the opportunity to comment on updates to the Model Privacy Notice. We look forward to working with ONC to update the Model Notice in line with consumer needs. If you have any questions about our recommendations, please contact Christine Bechtel, campaign coordinator, at Christine@getmyhealthdata.org or (202) 412-4397.

Christine Bechtel
Coordinator