national partnership for women & families
Because actions speak louder than words.

April 14, 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

Attn.: MPN RFI

Re: Request for Information on Updates to ONC's Voluntary Personal Health Record Model Privacy Notice

Dear National Coordinator DeSalvo:

The National Partnership for Women & Families appreciates the opportunity to comment on the Request for Information on Updates to the ONC Voluntary Personal Health Record Model Privacy Notice ("Request"). The National Partnership is a national, non-profit, non-partisan organization that, for 45 years, has worked to improve the lives of women and families. We represent individuals across the country who are the health care decision-makers for themselves and their families, who use the personal health records and apps and devices that are at the heart of ONC's request for information, and who care about the privacy and security of that health information.

We agree with the Request's observation that the consumer health technology landscape has evolved greatly since ONC published the first Model Privacy Notice in 2011, which focused on the web-based Personal Health Record. We now have a much expanded universe of smartphones and mobile applications (apps), devices, wearables and other consumer-facing applications that help to collect, send, manage and use one's health information.

According to a national survey the National Partnership released in December 2014, almost nine in ten patients report that it is important to them to know how their health information is being collected and used.[1] **The Model Privacy Notice can help** – by disclosing to consumers in plain language how the app or device will use, share and protect the privacy and security of their health information, and thus helping consumers identify the app or device that best meets their needs and preferences.

[1] 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, p. 40.

1875 connecticut avenue, nw ~ suite 650 ~ washington, dc 20009 ~ phone: 202.986.2600 ~ fax: 202.986.2539
email: info@nationalpartnership.org ~ web: www.nationalpartnership.org

1. User Scope

We recommend broad use of the Model Privacy Notice by covered and non-covered entities alike. Consumers may not track technical or legal distinctions among different types of technology developers when collecting, sending, receiving and using their health information from diverse sources; instead, the consumer may be focused on the seamless nature of the health information exchanges. Indeed, the *same* device or mobile app might or might not be subject to HIPAA's privacy and security protections depending upon whether a HIPAA-covered entity such as a provider, payer or business associate provided it to the individual. Since such distinctions may hardly be apparent to the consumer when managing her clinical health information from myriad sources, we encourage ONC to develop a Model Privacy Notice that is broadly applicable to covered and non-covered entities alike without distinction or exclusion by type of health technology developer. This is most useful to consumers.

2. Information Type

Similarly, we recommend starting with identifiable health information generally rather than asking whether discrete information types are in or out of scope. The HIPAA Privacy Rule may make legal distinctions for purposes of defining a HIPAA-designated record set or relevant identifiers for purposes of de-identification, but consumers may not be tracking or distinguishing these diverse information types when collecting, sending, receiving and using their collective health information from diverse sources. For instance, as the FTC notes, "the consumer's IP address, if maintained by a health plan's wellness app, is identifiable health information." It does not become any less so, from a consumer's practical perspective, when maintained by her commercial wellness app on her smartphone or wearable. For consumers, the simple starting point is identifiable health information collectively.

Moreover, our understanding of relevant categories of health information is evolving just as the consumer health technology landscape is evolving. Providers and policymakers increasingly appreciate that individual's non-clinical information – social determinants of health – can nonetheless be critical in health care decision-making and treatment.[2] Different information types, when combined with identifiable health information, become identifiable health information as well. Working with the collective framework of identifiable health information, rather than categorizing information types as categorically in or out of scope, allows the Model Privacy Notice to adapt with an evolving understanding of relevant and identifiable health information.

---

[2]According to Robert Wood Johnson Foundation's assessment, medical care delivery determines only an estimated 10-15 percent of health. The remaining 85-90 percent of health is determined by other factors, such as health behaviors, genetics, and the socioeconomic and physical environment (e.g., access to education and job opportunities, housing, public safety, language services, availability of places to exercise, healthy food choices, and other environmental factors). Robert Wood Johnson Foundation, Frequently asked questions about the social determinants of health (2010), available at http://www.rwjf.org/content/dam/files/rwjf-web-files/Research/2010/faqsocialdeterminants20101029.pdf

3. Information Practices

The 2011 Model Privacy Notice identifies many of the basic information practices, especially releases to third parties, that consumers would want to know. However, consumers also want to know how the company or technology itself is using one's health information. **We urge ONC to add disclosure of the company's own uses to the Model Privacy Notice.** Consumers want to know if a company is using their health information for its own medical research, its own marketing and advertising, or its own technology development, just as they want to know whether the company or technology discloses their health information to third parties for the same purposes. Consumers should be able to find the company's own uses transparently displayed as well. For simplicity, the Notice could employ the same set of information practices, whether the company uses consumers' health information for itself or shares it with a third party.

We also recommend adding "sale"[3] and "public health reporting" as information practices to be covered, and we recommend disclosing release to insurers and employers separately, so the consumer can distinguish sharing with employers from sharing with health insurers for payment or claims (a specially permitted disclosure under HIPAA).

In summary, we recommend that the Model Privacy Notice cover

- Marketing and advertising,
- Medical or pharmaceutical research,
- Reporting about our company and our customer activity, and
- Developing software applications

as disclosed information practices whether for the company's internal use or sharing with third parties, and

- Sale,
- Release to your insurer,
- Release to your employer, and
- Release for public health reporting

as disclosed information practices specific to sharing with third parties.

We encourage ONC to keep the existing format that displays whether the release of information occurs with "personal" and "statistical data" through the use of two columns. However, we recommend relabeling "statistical data" as "de-identified data" or "anonymized data." We also recommend adding a third column to disclose, "yes" or "no," whether the company and technology obtain the consumer's prior consent before any release.

[3] The HITECH Act added "sale" to a pre-existing requirement in the HIPAA Privacy Rule to disclose "marketing," illustrating that "sale" and "marketing" are different practices. HITECH Act of 2009, § 13405(d), 123 Stat. 115, 266; 78 Federal Register 5566, 5603 (Jan. 25, 2013) (discussing sale of protected health information).

4. Sharing and Storage

Consumers should have disclosure of whether the device or technology stores the data locally in the device or technology, and separately whether the company stores and retains the data in its servers. Asking whether the device or technology stores the data locally helps consumers understand the risk of local access to their information through the device or technology. Asking whether the company stores the data elsewhere helps consumers understand that other copies of the health information exist. Thus we recommend the addition of two questions:

- Is your health information stored locally in the device or app?
- Is your health information stored externally in the company's servers?

We also recommend adding two questions regarding sharing the health information with third parties:

- Does the company require each third party also to adhere to the same privacy and security policies that the company discloses in its Model Privacy Notice?
- Does the company require each third party to agree not to attempt to re-identify de-identified data?

5. Security and Encryption

The 2011 Model Privacy Notice merely includes a statement that "We have security measures that are reasonable and appropriate to protect personal information, such as PHR Data, in any form, from unauthorized access, disclosure, or use." The statement does not indicate what "reasonable and appropriate" means in practice, nor whether it is a subjective standard that might mean different things to different companies.

We therefore recommend the addition of two standard questions:

- Do the company and technology encrypt (encode) the health information wherever stored (sometimes called "encryption at rest")?
- Do the company and technology encrypt (encode) the health information whenever transmitted electronically (sometimes called "encryption in transit")?

We recognize that appropriate security and privacy require much more than encryption, such as authentication and authorization, but in a simple Model Privacy Notice, these two questions tell the consumer much about the security of her health information.

6. Access to Other Device Information

We recommend a simple question about the device's access to other consumer information stored on a smartphone or computer, such as geo-location data or social media:

- Does the technology or device access and integrate the consumer's other information external to the health application?

Just understanding that such access does or does not occur communicates much to the consumer.

7. Format

As we stated above regarding disclosure of information practices, we recommend relabeling "statistical data" as "de-identified data" or "anonymized data". We agree with the Request's implication that using an existing, standardized definition can facilitate wider understanding and consistency when applied to the Model Privacy Notice.

8. Information Portability

Consumers expect to be able to have and take their health information with them for whatever reason – choosing a different device or app, or choosing a different provider – or if the company terminates the service. The Notice should disclose whether the device or technology allows this information portability whenever the consumer wants, and whether it allows the consumer to download and share *all* data, including data contributed by the consumer as well as data incorporated from other sources, perhaps automatically. We therefore recommend the following disclosure:

- Does the device or technology allow the consumer to download and share all of the consumer's health information?

Our comments above on retention (under sharing and storage) are equally applicable here as well. If the company stores and retains the data in its servers, the consumer should know:

- Does the company return all of the consumer's data and erase all copies when the consumer or the company terminates the service?

- If not, does the company retain the data for its use or sharing with third parties?

We close with a strong recommendation that the Model Privacy Notice be available in at least the top 15 languages nationally and be accessible to people with various disabilities. According to the Census Bureau, more than 60 million Americans ages five and older, or 21 percent, spoke a language other than English at home in 2011, and more than 37 million Americans spoke Spanish alone.[4] There were 56 million Americans with a

[4] U.S. Census Bureau, *Language Use in the United States: 2011*, p. 3 (Aug. 2013), available at https://www.census.gov/prod/2013pubs/acs-22.pdf.

disability.[5] The Model Privacy Notice should be equally available and accessible to them, too.

Thank you very much for this opportunity to comment on the Model Privacy Notice. If you have any questions about our recommendations, please contact Mark Savage, Director of Health IT Policy and Programs, at MSavage@nationalpartnership.org or (202) 986-2600.

Sincerely,

[signed]

Mark Savage
Director of Health IT Policy and Programs

[5] U.S. Census Bureau, *Americans with Disabilities: 2010*, at 4, 8-9, 17-19 (2012), available at http://www.census.gov/prod/2012pubs/p70-131.pdf