CENTER FOR DEMOCRACY & TECHNOLOGY

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, S.W.
Washington, D.C. 20024

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

Dear National Coordinator DeSalvo:

The Center for Democracy & Technology (CDT) is pleased to submit comments on updates to the ONC Voluntary Personal Health Record Model Privacy Notice (MPN). The Center for Democracy & Technology (CDT) is a nonprofit advocacy organization working to advance democratic values in the digital age including privacy, free speech, and access to information.

I currently serve as the Deputy Director of CDT's Privacy and Data Project, which focuses on developing privacy safeguards for consumers through a combination of legal, technical, and self-regulatory measures. Ensuring that services are designed in ways that preserve privacy, establishing protections that apply across the life cycle of consumers' data, and giving consumers control over how their data is used are key elements of protecting privacy in the digital age. CDT has long been involved in creating standards for notice and transparency, including a best practices guide for mobile app developers that highlights the need for effective notice and transparency to users.[1] In 2013, CDT participated in a multi-stakeholder convening organized by the National Telecommunications and Information Administration released a set of principles focused on mobile app transparency.[2] Those principles were later included in an open source privacy policy released by Lookout, a privacy and security

[1] Future of Privacy Forum and Center for Democracy & Technology, *Best Practices for Mobile Application Developers*, available at https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf.
[2] National Telecommunications and Information Administration, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

startup.[3] Relying on these resources in addition to use of the MPN can help developers and manufacturers identify what they need to communicate to users, and how to do so.

As the RFI accurately notes, data collection via consumer health technology has greatly expanded in the five years since the initial development of the MPN. The ability for consumers to understand and act on information about a company's data practices and policies has been severely compromised by the sheer amount of data being collected and shared. Consumers are increasingly using mobile phone apps and wearable devices to generate and share data on health and wellness, employing personal health record tools to access and copy health records and move them to third party platforms, and sharing health information on social networking sites. They leave digital health footprints when they conduct online searches for health information and the health data created, accessed, and shared by consumers using these and many other tools can range from detailed clinical information, such as downloads from an implantable device and details about medication regimens, to data about weight, caloric intake, and exercise logged with a smartphone app.

These developments offer a wealth of opportunities for health care and personal wellness. However, privacy questions arise due to the volume and sensitivity of health data generated by consumer-focused apps, devices, and platforms, including the potential analytics uses that can be made of such data. Transparency about data practices is essential not just as a fundamental element of privacy, but is also key to engendering consumer trust, which in turn is critical to the adoption of these services. Without trust, consumers will resist using apps or devices and the industry as a whole will suffer.

Overall, transparency practices should be guided by the principle that the consumer should not be surprised. The more unexpected or potentially objectionable a data collection or usage is, the greater the obligation to explain it to consumers.

1. User scope

Openness and transparency should be guiding principles for all consumer-facing entities that collect personal health data, and thus all communications should be created with the framework of a typical person in mind. Fundamentally, it should be clear to a consumer using a health app or wearable device 1) when data is being collected; 2) what types of data are being collected; 3) what that data is used for; 4) what third parties it is shared with (and how they use and/or share it); 5) how long the data is retained and; 6) what security measures are in place to protect it.

[3] Ric Velez, Lookout Open Sourced Its "Private Parts," You Should, Too (Mar. 12, 2014), https://blog.lookout.com/blog/2014/03/12/open-source-privacy-policy/

Due to the intrinsic sensitivity of health information, all commercial vendors, HIPAA-covered and non-covered alike, have an obligation to clearly disclose data collection practices at a time and in a manner that is likely to be seen (including those that are responsive to different languages and disabilities) and acted upon by the user. This includes new entrants in the health technology world like apps, sensors, and wearables, as well as more traditional entities like academic, government and commercial researchers, data brokers that aggregate data covered entities and their Business Associates, state registries and employee wellness programs.

Rather than serving only as the basis for user consent, MPNs should be required to use concrete, digestible information about what entities actually do with user data, using written language and visual data flows whenever possible. The FTC has made it clear that, even where a registration process obtains express user consent, which consent will be invalid and the data collection illegal if a reasonable consumer would not be likely to understand the scope of the data practices being conducted. Thus, it's possible that the ONC and FTC could collaborate on a requirement that all covered and non-covered entities use an MPN.

2. Information type

The information types listed by the ONC for the MPN are fairly comprehensive though the list omits the use of data by the app itself for marketing and other purposes as well as the *sharing* of identifiable data. The data types listed include government access but this should include any collection by the government for public health or open data initiatives. Information from apps and devices that capture clinical data or biometric information that is then used in a clinical setting or health program should be included as a part of a MPN.

ONC should consider all personal health data that moves through the commercial space to be in scope if the MPN is to carry meaning. But if the goal of the MPN is *comprehension*, rather than comprehensiveness, a laundry list of data types will likely be indecipherable and not useful to most people. Though the concept of following HIPAA's distinctions between data types makes some sense from a legal compliance standpoint, it is does not make sense from a user standpoint. Additionally, as technology evolves in the health and wellness space, so too will the different data types; thus, we believe that determining the information types on an MPN should mostly depend on the context of the commercial entity's relationship with the consumer.

Companies have an obligation to explain any collection of data types that may not be contextually obvious (like a glucose monitor collecting glucose information) as, increasingly, it

will be possible for companies with *no relationship* with a consumer to collect health information in public spaces. For example, it's possible now that a sensor could be set up on a street corner to monitor the heart rates of passers-by in order to conduct a study of the general population or potentially to target hypertension ads to relevant consumers. The potential for a service to collect information, when it is unexpected and/or outside of the context of a consumer relationship, should also inform which data types are listed on the MPN.

3. Information practices

We believe it's worthwhile to use a framework of identifiability, expectation, and measure of harm or impact on an individual to determine which information practices must be included. For example, due to the sensitivity of personal health information, we believe that it would not be appropriate to collect health information that could be tied back to an individual or a device used by an individual without having a relationship with that individual; therefore, *any* information practices that are outside of this direct relationship should be included on an MPN. Likewise, given the sensitivity of health data, it should be paramount for a company to include any information practice that would fundamentally alter an individual's experience (such as the advertising she receives) due to observed health information that was not deliberately provided. Even de-identified data or data exempted by HIPAA should be accounted for by a MPN to uphold true transparency.

4. *Sharing and storage*

Consumers need to know that their data is being secured at the highest level possible, that it is not being shared with outside parties without a similar assurance of privacy and security protection, that their permission is required before their data is shared or used outside of the context of their relationship with the company, and that their data will be deleted when it no longer serves the specified purpose. Additionally, it's critical for consumers to know how their data will be protected from security breaches and, if they are exposed, how the company will notify them and mitigate any harm that is created by the breach.

5. *Security and encryption*

Consumers need to feel confident that their data is being protected at the highest possible level and companies must be held accountable to their security practices. The communication of encryption types or levels is probably less helpful to consumers than the assurance that their information is being adequately protected by both security measures like encryption and through robust internal access controls.

6. *Access to other device information*

Commercial privacy policies must be improved to introduce greater accountability for actual practices. These policies should contain detailed information about what data is collected, for what purposes, with whom the data is shared, and how long that data is retained, including any that it is able to access on a smartphone or computer. Companies should also communicate to consumers in simple, clear terms at the time that an app is installed, or when a device is activated, what information, including other device information, is being collected about the user and for what purpose. How detailed that notice should be depends on the context of the relationship with the user. In no event should the reasonable user be surprised by any data collection and use.

7. *Format*
Company's collecting personal health data should be required to list security practices but it seems doubtful that in-depth details about the methods used, like anonymization or other forms of de-identification, would be helpful to an individual. Rather, consumers want to know if they are sharing their data, regardless of the format, and with whom. From a developer standpoint, HITRUST's De-Identification Framework provides useful technical standards as well as methods for communicating them to consumers, as does NIST's published standards on de-identification.

8. *Information portability*
Fundamentally, we believe that consumers should be considered owners of their information, particularly when it comes to sensitive information like health data. In practice, this means that any device or application should disclose early on whether or not a consumer can download, share, transmit, or delete their information or account to communicate the company's views on ownership and control. This information should be presented in a way that allows immediate, unimpeded action for the consumer (rather than pointing a link that has restrictions or other rules about these options). If a company retains some of the consumer's data, charges for account deletion, or will sell data from deleted accounts, this should be spelled out in a clear, unequivocal way in the MPN upfront.

Thank you for the opportunity to comment on the MPN. Please do not hesitate to get in touch with me with questions or to schedule a follow-up meeting at mdemooy@cdt.org or 202.407.8831.

Sincerely,

Michelle De Mooy
Deputy Director, Privacy and Data Project