April 15, 2016

Karen B. DeSalvo, MD, MPH, M.Sc.
National Coordinator for Health Information Technology
Acting Assistant Secretary for Health
U.S. Department of Health and Human Services
200 Independence Avenue SW, Suite 729-D
Washington, DC 20201

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

Dear Dr. DeSalvo:

The National Association for Trusted Exchange (NATE) is pleased to submit comments on the proposed revision of the voluntary Personal Health Record (PHR) Model Privacy Notice (MPN) by the Office of the National Coordinator for Health IT (ONC).

NATE is a not-for-profit membership association focused on enabling trusted exchange among organizations and individuals with differing regulatory environments and exchange preferences. NATE brings the expertise of its membership and other stakeholders together to find common solutions that optimize the appropriate exchange of health information for greater gains in technology adoption and improvement of patient outcomes. Consistent with NATE's mission to address the legal, policy and technical barriers that inhibit health information exchange between data holders and healthcare consumers, NATE leads and participates in a number of ongoing and emerging projects focused on exchange via multiple modes of transport, including Direct secure messaging and APIs.

NATE's Blue Button for Consumers (NBB4C) Trust Bundle provides a technical solution to establishing scalable trust among organizations using Direct secure messaging to exchange protected health information between HIPAA covered entities and the consumers that they serve. The NBB4C includes the trust anchors of multiple consumer-facing applications (CFAs) that have elected to adopt a common set of policies and practices that enable consumer mediated health information exchange while upholding personal privacy preferences. Working with a broad set of stakeholders through multiple task forces, crowdsourcing and a call for public comment, the process to determine the eligibility requirements that govern the NBB4C spanned two years and included multiple pilots. Many of the CFAs that NATE works with have taken advantage of ONC's original MPN

and the NBB4C eligibility requirements in fact include an expectation that CFAs have either utilized the ONC MPN or made available to consumers something similar in nature.

NATE's comments herein include the input of multiple NATE member organizations. As requested, our contribution is correlated to the questions asked in the Request for Information (RFI) published in the Federal Register.

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?

Clearly any non-HIPAA-covered entities that create, receive, process, maintain, or transmit personal health information (PHI) should provide their consumers with the information recommended in a MPN, and this should apply to all non-covered entities, whether they are PHRs or health/fitness apps or something else entirely. However, as we look forward to likely changes in the landscape, we expect that it will become increasingly important for consumers to be able to differentiate between applications that are HIPAA-covered and those that are not, and perhaps even more importantly, understand what that difference means to them as a user.

For example, there is no reason to believe that a HIPAA-covered application would have a better security profile or that HIPAA-covered entities are adhering to what the consumer would believe are fair information sharing practices. In fact, today many consumers are surprised to learn that their data has been sold or otherwise shared by their care providers without their knowledge. It is important that HIPAA-covered entities be as transparent as non-covered entities about the information a consumer shares with them via an app (including patient generated health data [PGHD] and PHI originating from other providers).

Furthermore, there is a misconception that the HHS Office of Civil Rights (OCR) has the necessary resources to enforce the requirements of the HIPAA Privacy Rule on covered entities. We are concerned that without further transparency into the uses of data by both covered and non-covered entities, the consumer may be lulled into a false sense of confidence that their providers and payers are better stewards of their data than an entity whose only purpose is to protect their privacy and enable its sharing in a privacy preserving way.

Information Type

- What information types should be considered in and out of scope for the MPN?

All data types that could potentially be deemed as sensitive, including personally identifiable information (PII), PHI and all of the examples given in the RFI should be considered in scope for the MPN.

Information Practices

- What types of practices involving the information types listed in Question 2 above should be included in the MPN?

All of the examples given in the RFI should be included in the MPN. In addition, we suggest the following modifications:

1) Modify "researchers" to include "corporate" and not just academic and non-profit institutions
2) Modify "marketing purposes" to include "advertising and promotion"
3) Add "Reporting identifiable data to any third parties, including investors, business partners, vendors and auditors"

NATE is strongly supportive of individual data donation for research. It has been reported that data donors want to be able to differentiate between those collectors of data that is being donated for the advancement of science versus those collectors of donated data that intend to either monetize the data or use it in a closed way to create competitive advantage. There is a widespread sense in the data donation community that if there is a financial gain from the sale of a donor's information, then the donor should be included in that transaction. Further, users should be able to differentiate between research entities that make their findings broadly available to the wider research community (such as those involved with the Precision Medicine Initiative) and those that may be more reticent to do so. The revised MPN is another opportunity for ONC to provide guidance against real and perceived consternations faced by the consumer when selecting an application to manage their health information.

Sharing and Storage

- What privacy and security issues are consumers most concerned about when their information is being collected, stored, or shared?

We are concerned about the risk of conveying a mixed message to consumers with regards to their right to use insecure email as a method of receiving their data versus methods that ensure end-to-end encryption for data, whether in transit, at rest or subsequently re-shared. This concern is further compounded by the complexity of conveying relative benefits in different enhanced security practices that may be employed by those who provide consumers with health information handling tools.

Perhaps we can borrow a consumer friendly tool from the automotive safety industry – such as their Five Star Safety rating but instead maybe it is a three star security rating. We would recommend setting insecure email at zero stars and make very clear demarcations where one star, two star and three star ratings occur. For example, as we are currently at a stage where second factor authentication is starting to become more common but is far from ubiquitous. This could be what is required to go from a two star to a three star rating. With regards to the Direct mode of exchange, participation in a trust community such as NATE or DirectTrust may differentiate

applications from two star and one star, where finally secure messaging of any type may get a single star rating.

Further, in this time of heightened attention on data breaches in healthcare, consumers should be clearly informed as to the obligations of the operator of the CFA should a breach occur (FTC breach notification reporting requirements compared to HIPAA breach notification requirements). If the operator conveys that they will provide post-breach services to support the consumer in the event of a breach, it may be important to ensure that consumers have a way to compare these offerings as well. We anticipate the emergence of such differentiators being offered and consumers may benefit from guidance regarding these services in the future as well. We want to ensure that consumers are informed of the relative value of differing identity protection/repair services if they are promoted as a feature of consumer health apps.

Security and Encryption

- What information should the MPN convey to the consumer regarding specific security practices?
- What level of detail is appropriate for a consumer to understand?
- How can information about various security practices, often technical in nature, be presented in a way that is understandable for the consumer?

Encryption of data at rest and in transit, and encryption on the device and in the cloud are easily understandable by consumers and would be appropriate in a revised MPN. Details such as encryption standards (AES 128/256, etc.) or even "compliance with government standards" may be too technical for the general consumer audience. However, knowing whether an entity has a security program that is audited by a third party is helpful information that consumers would understand.

NATE's NBB4C eligibility requirements include attestations that the CFA perform periodic network security audits, regular network intrusion detection, regular web application security scanning/testing (applicable to web-based apps) and periodic third-party penetration testing. If explained in plain language, these are concepts that would be of interest to the consumer.

The NBB4C eligibility requirements also call out a current technology best practice that is not in fact consumer-friendly: the use of multi-tenant digital certificates. Using one certificate for multiple applications puts the information in all of those applications at risk. Again, if explained in plain language, this is a concept that would be of concern to a consumer.

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?

This is an important question but should be clarified as far as it relates to the revised MPN. The consumer should be able to distinguish between whether the application is "able to access" versus whether it actually "accesses" the data. In addition to covering Data Release and Data Security, the MPN should also specifically identify Data Access, listing each of the types of content available and whether it is "able to access" and/or "accesses" that content.

Further, the consumer should be made aware of their options for allowing such access. For example, they should know whether they can turn on/off access to information such as location, which can pose a potential safety risk to the user, or to phone calls and text messages, which may be considered especially sensitive.

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?

It may be simpler to explain and easier for the average consumer to understand if the MPN identifies and defines just two categories of data:

1) Personal Data
    a. e.g., PII, PHI, and data with any other personal identifiers

2) Statistical Data
    a. Personal identifiers removed or grouped so personal identification cannot be made without significant effort

For each category, the revised MPN should convey the risk of loss of that data. It should be clear to the user that while "statistical data" is considered to be of lower risk than "personal data," there is still the possibility that their information will be re-identified using other factors, including those perhaps obtained through a non-related application.

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?

With regard to download/transmission of health information, we suggest labeling the functions as "receive, transmit and save to a personal device."

With regard to the consumer's ability to retrieve or move their data when terminating the relationship, we suggest the following:

1) "Account Termination: Obtaining Data" + "Terminated by Consumer: <Describe Method and Timing for obtaining data.>"
2) "Account Termination: Obtaining Data" + "Terminated by Service Provider: <Describe Method and Timing for obtaining data.>"

This is a critical concern for consumers and one that is echoed in the NATE NBB4C evaluation criteria. The NBB4C eligibility requirements specifically state that a "CFA shall ensure that an end-user is able to terminate their participation in the CFA and be able to request that their data be expunged in its entirety from the application and any data stores controlled by the CFA that may contain the end-user's PHI."

Further, it should be obvious to the consumer whether the service provider plans to re-issue the Direct address assigned to that user during the time that consumer was a user of the app. The NATE NBB4C eligibility requirements make it clear that not only should only unique Direct addresses ever be active at any given time, but that once a Direct address is inactivated, it may never be reused again. This is a critical concern given that best practice includes the patient's name in their Direct address, yet we have a significant issue across the industry with ensuring accurate patient identification in cases where patients share the same name.

In addition to our comments above, we suggest that Notification of a Change in Privacy Practices also be part of the revised MPN. It should be clear to the consumer at the time they review the MPN how they will be notified if those expectations should change.

Once the MPN has been revised, we suggest that ONC produce an online tool that can create the MPN in HTML format after needed input from the developer. Input from current users of the ONC MPN indicates that the current PDF format is not as useful as it could be, as it cannot be presented on mobile screens.

Finally, we suggest that the revised MPN should be aligned with European Union (EU) and other international standards and practices to the extent possible. Many CFA developers, including some participating in the NATE NBB4C, are often developing solutions for use beyond the United States and would appreciate the attempt at conformity.

On behalf of NATE and its members and trust bundle participants, thank you for the opportunity to provide feedback on this important RFI. We appreciate that ONC took the effort to create the Voluntary PHR MPN in 2011 and are gratified to see the level of effort going into the proposed revision. If we can be of any more help in this process, please do not hesitate to reach out.

Sincerely,

Aaron Seib, CEO
National Association for Trusted Exchange