Breach Notification Rule [7] which requires notification to affected individuals when a breach of data occurs.

We are considering creating a new version of the MPN that would expand its scope beyond PHR companies and include more types of information practices. A modernized MPN would serve as a voluntary resource for health technology developers who want to give notice of their information practices to their users in an understandable way. Therefore, ONC requests public comment from consumers, mobile and web application developers, privacy advocates, user experience and design experts, and other health technology stakeholders on any updates that should be made to the content of the MPN to make it more useful to both health technology developers and consumers.

While we encourage comments on all aspects of the MPN, ONC specifically seeks comment on the topics specified below. We note that the MPN does not recommend best practices to health technology developers, and we do not seek recommendations about best practices. Rather, ONC seeks comment concerning what information practices health technology developers should disclose to consumers and what language should be used to describe those practices in an updated MPN. Examples of information practices below are included to clarify the intent of the questions, but are not intended to be exhaustive. ONC invites commenters to discuss any examples that are relevant to the broad issues of which types of personal information and information practices should be addressed in an updated MPN.

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?

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 geo-location 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.

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.

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.

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.

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.

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? [8]

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.

ONC seeks broad input from stakeholders on updating the MPN so that the tool is useful for current health technology developers and consumers. Individuals and organizations with common interests are urged to both coordinate and consolidate their comments.

Authority: 42 U.S.C. 300jj–11; Office of the National Coordinator for Health Information Technology; Delegation of Authority (76 FR 58006, Sept. 19, 2011).

Dated: February 23, 2016.

Karen DeSalvo,

National Coordinator for Health Information Technology.

[FR Doc. 2016–04239 Filed 2–26–16; 4:15 pm]

BILLING CODE 4150–45–P

[7] 16 CFR part 318.

[8] See, *e.g.,* 45 CFR 164.514(a) (HIPAA Privacy Rule) as a potential standard for de-identification of protected health information.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

Health IT Policy Committee and Health IT Standards Committee: Schedule and Recommendations

AGENCY: Office of the National Coordinator for Health Information Technology, Department of Health and Human Services.

ACTION: Notice.

SUMMARY: This notice fulfills obligations under the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L.

111–5), which amended the Public Health Service Act (PHSA). Section 3003(b)(3) of the PHSA mandates that the Health IT Standards Committee (HITSC) develop an annual schedule for the assessment of policy recommendations developed by the Health IT Policy Committee (HITPC) and publish the schedule in the **Federal Register**. This notice fulfills the requirements of section 3003(b)(3) and updates the HITSC schedule posted in the **Federal Register** on August 10, 2015. This notice also meets the requirements under sections 3002(e) and 3003(e) for publication in the **Federal Register** of recommendations made by the HITPC and HITSC, respectively. Further, this notice serves to meet the requirements of section 3004(a)(3) for publication in the **Federal Register** of determinations by the Secretary of Health and Human Services regarding HITSC-recommended certification criteria endorsed by the National Coordinator for Health Information Technology.

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION: This notice fulfills obligations under the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5), which amended the Public Health Service Act (PHSA).

Health IT Standards Committee Schedule

Section 3003(b)(3) of the PHSA mandates that the Health IT Standards Committee (HITSC) develop an annual schedule for the assessment of policy recommendations developed by the Health IT Policy Committee (HITPC) and publish it in the **Federal Register**. The HITSC's schedule for the assessment of HITPC recommendations updates the HITSC schedule published on August 10, 2015, and is as follows:

The National Coordinator for Health Information Technology (National Coordinator) will establish priority areas based in part on recommendations received from the HITPC regarding health IT standards, implementation specifications, and/or certification criteria. Once the HITSC is informed of those priority areas, it will:

(A) Identify the best mechanism by which to organize itself in order to respond to the National Coordinator within 90 days with, at a minimum, the following:

(1) An assessment of what standards, implementation specifications, and certification criteria are currently available to meet the priority area;

(2) An assessment of where gaps exist (*i.e.,* no standard is available or harmonization is required because more than one standard exists) and identify potential organizations that have the capability to address those gaps; and

(3) A timeline, which may also account for the National Institute of Standards and Technology (NIST) testing, where appropriate, and include dates when the HITSC is expected to issue recommendations to the National Coordinator.

(B) In responding to the National Coordinator:

(1) Approve a timeline by which it will deliver recommendations to the National Coordinator; and

(2) Determine whether to establish a task force to conduct research and solicit testimony, where appropriate, and issue recommendations to the full committee in a timely manner.

(C) Advise the National Coordinator, consistent with the accepted timeline in (B)(1) and after NIST testing, where appropriate, on standards, implementation specifications, and/or certification criteria, for the National Coordinator's review and determination whether or not to endorse the recommendations, and possible adoption of the proposed recommendations by the Secretary of the Department of Health and Human Services (Secretary).

The standards and related topics which the HITSC is expected to address in 2016 include, but may not be limited to: Quality measurement; precision medicine; security; consumer-mediated information exchange; public health; technical interoperability experience in the field; and updates to the Office of the National Coordinator for Health Information Technology (ONC)'s Interoperability Standards Advisory(ies).

HITPC and HITSC Recommendations

Sections 3002(e) and 3003(e) of the PHSA provides for publication of HITPC and HITSC recommendations in the **Federal Register**. ONC will post all recommendations received from the HITPC on its Web site at: *https://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it.* ONC will post all recommendations received from the HITSC on its Web site at: *https://www.healthit.gov/facas/health-it-standards-committee/health-it-standards-committee-recommendations-national-coordinator.* All prior recommendations received from the HITPC and HITSC can be found at these respective Web site addresses.

HITSC Privacy and Security Recommendations

Section 3004(a)(3) of the PHSA provides for publication in the **Federal Register** of determinations by the Secretary regarding HITSC-recommended certification criteria endorsed by the National Coordinator.

On March 30, 2015, ONC issued a notice of proposed rulemaking with comment period for the 2015 Edition health IT certification criteria (80 FR 16804). Subsequently, on June 5, 2015, the HITSC submitted a transmittal letter to the National Coordinator which contained the HITSC recommendations for the adoption of two new certification criteria for the ONC Health IT Certification Program. The two certification criteria are:

1. A criterion for encrypting authentication credentials; and

2. A multi-factor authentication criterion for user access to health information.

The National Coordinator endorsed these recommendations for consideration by the Secretary and the Secretary has determined that it is appropriate to propose adoption of these two new certification criteria through rulemaking. Therefore, the Secretary, within a reasonable period of time, will propose adoption of the certification criteria noted above in an available and appropriate notice of proposed rulemaking.

Authority: 42 U.S.C. 300jj–11–14; Office of the National Coordinator for Health Information Technology; Delegation of Authority (74 FR 64086, Dec. 7, 2009).

Dated: February 23, 2016.

Karen DeSalvo,

National Coordinator for Health Information Technology.

[FR Doc. 2016–04238 Filed 2–26–16; 4:15 pm]

BILLING CODE 4150–45–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute on Aging; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.