Electronic Healthcare Network Accreditation Commission

www.EHNAC.org

Lee B. Barrett
Executive Director

Debra C. Hopkinson
Operations, VP

December 28, 2018

Ms. Naomi Lefkovitz,
U.S. Department of
Commerce, NIST, MS 2000, 100 Bureau
Drive, Gaithersburg, MD 20899

RE: [Docket Number 181101997–8997–01] NIST RFI Developing a Privacy Framework

To Whom It May Concern:

The Electronic Healthcare Network Accreditation Commission appreciates the opportunity to comment on this Request for Information published by the National Institute for Standards Technology on November 14, 2018. Our comments were submitted to privacyframework@nist.gov by the 5:00 PM ET deadline on December 31, 2018.

Founded in 1993, the Electronic Healthcare Network Accreditation Commission (EHNAC) is an independent, federally recognized, standards development organization and tax-exempt 501(c) (6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare. EHNAC's accreditation programs were specifically designed to support the protection of electronic health information with a focus on Protected Health Information (PHI) and Personally Identifiable Information (PII) as well as support for industry-adopted standards allowing for a more seamless information exchange between participants in health information networks. EHNAC has over 18 stakeholder-specific programs available across the industry including by not limited to Health Information Exchanges (HIE's), Health Information Service Providers (HISPs), Electronic Healthcare Networks (EHN's), Electronic Prescription of Controlled Substances (EPCS). This includes new programs under development such as one for the use of Blockchain technologies and Trusted Exchange components as set forth within the 21st Century Cures proposed TEFCA requirements.

EHNAC supports the goal of NIST to develop an enterprise Risk Management tool whereby organizations integrate general privacy concepts into their products and business development life cycles. EHNAC also agrees that the industry will benefit from additional tools and practical suggestions to bridge the gap between privacy and security initiatives. We are pleased to offer general and detailed comments as requested to the Organizational, Structural and Specific Privacy Practices set forth in the RFI.

General EHNAC Comments:

- **Address the Divide Between Privacy and Security Resources:** One of the challenges EHNAC experiences when conducting organizational reviews across the healthcare industry with many different types of HIPAA Covered Entities and Business Associates alike is that it is challenging to find both privacy and security expertise in the same individual workforce member. Not only is it typical that privacy professionals are often comprised of those with legal, compliance and business expertise, whereas, security professionals are most often trained Information Technology professionals, sometimes identical terms and definitions are used which imply entirely different meanings. It is imperative to continue to build into the workforce members who have the experience to address both privacy and security.

- **Understand The Data:** One of the areas EHNAC stresses as part of the initial self-assessment process and reinforced by the on-site Review is the emphasis on the flow of Protected Health Information. The "exercise" recommended first by the Office for Civil Rights (and stressed by the Workgroup for Electronic Data Interchange) when HIPAA Privacy implementations were first being conducted was the requirement that an organization analyze and document the type of PHI that is being handled throughout the process of delivering services (demographic data, financial data, clinical data) and determine whether or not the data is created by the organization, received from others, maintained and/or transmitted. Lastly, it should be noted whether data is in use, at rest or in transit and when possible, encryption is suggested to be documented. Defining and documenting the category of data (PHI), the flow of it throughout the business cycle from inception to destruction and then "grading or scoring" the level of data handled is an incredibly helpful exercise to the overall ongoing compliance effort.

- **Scale "Up" Privacy:** EHNAC applauds the attempt to address privacy risk absent any particular law. One can immediately become confused attempting to meet GDPR requirements when also caring for a designated record set of PHI (HIPAA). Summarizing privacy requirements into realistic (commonly understood) categories and then assigning a risk based on the level of data handled should prove a great benefit to the industry.
    - EHNAC also finds it helpful to summarize traditional HIPAA Privacy into categories: 1) Administrative Requirements; 2) Individual Rights; 3) Uses and Disclosures and 4) General Safeguards. For purposes of the NIST Privacy Framework, we recommend using this same breakdown but augmenting the Individual Rights to include other prescriptive requirements such as those set forth in GDPR and/or other specific legal requirements which may or may not include consent, authorization and opt in/out processes.

- **Keep It Simple:** EHNAC agrees that tools for the industry should be practical, adaptable, easy to understand and scalable to small, medium and large businesses. We strive for the same scalability across our many accreditation programs.

Specific EHNAC Comments in Alignment with the Request for Information:

Organizational

1. The greatest challenges in improving organizations' privacy protections for individuals;

EHNAC believes some of the greatest challenges for organizations with respect to delivering individual privacy protections is to first know the data that is handled, and secondly to know/understand the requirements for using and disclosing that data.

2. The greatest challenges in developing a cross-sector standards- based framework for privacy;

EHNAC manages the challenges presented with its programs as they span from very small Managed Service Organizations and Billing Companies to very large and complex Health Information Exchanges and many organizations in between. Being able to recommend best practices and then to provide examples of what best practices look like in the large/complex entity versus the small, simple environment is very helpful to the industry.

3. How organizations define and assess risk generally, and privacy risk specifically;

The majority of EHNAC candidates are subject to HIPAA such that we view many organizations that have implemented risk-based security approaches and some who extend that to include the various potential threats associated with privacy risks and expectations. Again, understanding where the data resides, how it is handled, and who has access to it are of utmost importance to the process of assigning appropriate levels of risk.

4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;

It appears to be relatively common across EHNAC candidates that enterprise risk management is expanded to include privacy risks, for those organizations subject to HIPAA. EHNAC believes this model would work well for non-HIPAA subject entities also.

5. Current policies and procedures for managing privacy risk;

Policies and procedures not only need to span and address all legal and regulatory requirements, but they should also reflect that the organization understands where its data resides, who handles it and how. Implementing good formal policies is key to knowing the organization's business goals and knowledge about its data handling.

6. How senior management communicates and oversees policies and procedures for managing privacy risk;

EHNAC sometimes sees overall senior authority that spans privacy and security in an integrated manner. This provides a comprehensive and coordinated approach and seems to alleviate "placing blame" from one area to another regarding responsibility. It is more common to see separations of privacy and security areas which can create risk in itself.

7. Formal processes within organizations to address privacy risks that suddenly increase in severity;

The HITECH Breach requirements require organizations to be ready to identify and respond to a potential threat. Models of policies, procedures, training, forms and checklists for this could be expanded to cover other types of data.

8. The minimum set of attributes desired for the Privacy Framework, as described in the *Privacy Framework Development and Attributes* section of this RFI, and whether any attributes should be added, removed or clarified;

EHNAC agrees with the minimum set of attributes as set forth in this RFI (Transparency, Common Language, Adaptable to Many; Risk and Outcome Based; Readily Usable as part of Broader Initiatives and Paired with other Approaches; Living document) as EHNAC strives to meet similar goals as part of the accreditation and standard setting process it follows.

9. What an outcome-based approach to privacy would look like;

EHNAC uses a process whereby candidates are requested to document the types of information handled and further to complete a survey of the level of data handled. These exercises which are currently completed to address PHI compliance could be expanded to offer the model sought by NIST.

10. What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above;

As was mentioned earlier, EHNAC has adopted the process first set forth by the Office for Civil Rights and The Workgroup for Electronic Data Interchange where PHI is documented based on category and then an additional survey is completed to set forth the category/level of data handled by the organization.

11. How current regulatory or regulatory reporting requirements (*e.g.,* local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;

When the HITECH Breach Rule was under initial implementation, the Office for Civil Rights established the method to report via the Internet known as the "Wall of Shame". The fields required to be reported offer a summary of the type of data potentially breached and whether it was encrypted. Completing this reporting form in a proactive manner is a best practice exercise as it forces the organization to understand the types of data it handles.

12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;

EHNAC believes that requiring the documentation of the flow of data, at use, at rest and in transit, when encrypted and the level of information handled would align with other current standards, frameworks and models.

13. The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles;

EHNAC strives to work collaboratively with other standard setting bodies to minimize administrative burden and the sheer number of audits our candidate's must undergo. This was the core reason that EHNAC partnered with HITRUST in 2016 in order to allow for its EHNAC candidates who choose to adopt HITRUST complete the self-assessment and review process as easily as possible by aligning privacy and security criteria.

14. The international implications of a Privacy Framework on global business or in policymaking in other countries;

EHNAC believes that setting the model in a summary fashion will allow for different more prescriptive privacy requirements to fall into the Risk based NIST model. For example, both GDPR and HIPAA requirements could fit into the "Individual Rights and/or Specific Legal/Regulatory Requirements" section set forth above.

15. How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.

Because the Privacy Framework scales other more prescriptive requirements upward and uses common language, this can aid in the cross training of IT, regulatory, compliance and legal professionals. Aligning the training should allow for more resources to be taught who come from separate privacy and security backgrounds but who can learn to approach both disciplines in a similar manner. Specifically, teaching the skill of understanding the overall flow of data from beginning to end as what must be one to document a PHI Flow as described above would be helpful to bridge the gap between niche experts.

Structuring the Privacy Framework

16. Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (*i.e.,* the different stages—from collection to disposal—through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?

EHNAC requires organizations to respond by first documenting their data handling (PHI Flow and Level of PHI Survey). This includes creation, receipt, maintenance and transmission of data at rest, in use and in transit. EHNAC also requires organizations to define policies, procedures and safeguards for PHI contained on end-of-life equipment prior to disposal. Proper removal of PHI is an integral part of that process.

17. Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.

The Cybersecurity Framework is modeled very closely to the initial HIPAA Security Rule. The Administrative, Physical and Technical Safeguards and Implementation Specifications were a component of the Privacy Rule. EHNAC views these as very similar and fitting together naturally.

18. Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:

a. The information life cycle; b. Principles such as FIPPs; c. The NIST privacy engineering objectives of predictability, manageability, and dis-associability or other objectives; d. Use cases or design patterns; e. A construct similar to the Cybersecurity Framework functions, categories, and subcategories; or f. Other organizing constructs?

EHNAC stresses PHI Flow, Level of Data Handling and the full information life cycle as the initial component of its criteria. This is preferred and scales well to organizations of various shapes and sizes.

Please elaborate on the benefits or challenges of your preferred approach with respect to integration with organizational processes for managing enterprise risk and developing products or services. If you provided information about topic 10 above, please identify any supporting examples of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.

EHNAC Responded to Question 10 and refers the authors of this RFI to the Office for Civil Rights and WEDI documents regarding PHI Flow activities.

Specific Privacy Practices

In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:

De-identification; Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared; Enabling user preferences; Setting default privacy configurations; Use of cryptographic technology to achieve privacy outcomes—for example, the dis-associability privacy engineering objective; Data management, including: Tracking permissions or other types of data tracking tools; Metadata; Machine readability; Data correction and deletion; and usable design or requirements.

19. Whether the practices listed above are widely used by organizations;

EHNAC sees all of the above practices used to some degree. Typically, the more complex and mature companies use advanced data management. De-Identification is required as part of HIPAA for certain circumstances when data is being shared. Organizations have the choice of using a Safe Harbor or Statistical Method according to the HIPAA Privacy Rule, however not all organizations follow the process as established in the rule. This is an area where EHNAC stresses the importance for HIPAA covered entities to follow the prescriptive requirements set forth in the HIPAA Rule.

20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;

Response indicated above.

21. How the practices listed above or other proposed practices relate to existing international standards and best practices;

Response indicated above.

22. Which of these practices you see as being the most critical for protecting individuals' privacy;

The importance of the organization to understand how it handles its data is of utmost importance to protect the sensitive information.

23. Whether some of these practices are inapplicable for particular sectors or environments;

PHI can be expanded. Organizations can document whether the data is considered "business critical" or Personally Identifiable according to state law. Setting for the category of information and level of sensitivity is key to assessing the risk.

24. Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization;

EHNAC often sees the challenge to the organization is that finding a resource/resources who see the "big picture" of how the data is handled and protected from the beginning to the end is a challenge. This is another critical skill that could be taught to strengthen the skill set in response to question number 15.

25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence;

The exercise of documenting the Flow of Data, understanding how data is handled, documenting it and assigning risk would be beneficial whether the technology is old or new. The same concepts apply.

26. How standards or guidelines are utilized by organizations in implementing these practices.

Response indicated above.

____

EHNAC appreciates the opportunity to provide feedback on this RFI and stands available to assist with any specific questions and to participate in future endeavors.

Sincerely,

Lee Barrett, Executive Director

EHNAC