September 30, 2022

Laurie E. Locascio
Director
National Institute for Standards & Technology and
Under Secretary of Commerce for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Director Locascio:

On behalf of the Health Sector Coordinating Council (HSCC) we write in response to the National Institute for Standards and Technology's (NIST) request for comments on NIST SP 800-66r2 initial public draft, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. The SP 800-66r2 initial public draft is built upon and intended to update the existing publication NIST Special Publication 800-66 Revision 1 from October of 2008.

The HSCC is a private sector-led critical infrastructure advisory council of large, medium and small health industry stakeholders working with government partners to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to our nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents 350 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. Our members collaborate toward improving the cyber security and resiliency of the healthcare industry and patient safety.

Summary

We appreciate the opportunity to comment on this important document. Our key recommendations are summarized below and detailed in the body of our letter. Our high-level recommendations are:

1. **One Size Does Not Fit All:** While the document is well written with numerous resources, it is not well-adapted for smaller and lesser resourced healthcare entities regulated under the Health Insurance Portability and Accountability Act (HIPAA).

2. **Small and lesser-resourced entities:** Create an entirely separate document specifically for small and mid-sized entities that expresses in plain English why practicing good cyber hygiene is imperative for compliance, business operations and, ultimately care delivery and patient safety.

3. **Consistent Terminology:** Use language that better differentiates between "risk analysis" and "risk assessment."

4. **Organization:** We make several targeted recommendations around better organizing the resources contained within the document to improve the utility of this publication.

Discussion

I. Audience

According to the draft, NIST writes that the "This publication is intended to serve a diverse audience of individuals with HIPAA Security Rule 121 implementation, management, and oversight responsibilities, as well as organizations considered 122 to be a "Covered Entity" or "Business Associate" under 45 C.F.R. Sec.160.103." HSCC appreciates that NIST has attempted to create a document that can be used by a variety of entities regulated under HIPAA. The challenge, however, lies in the fact that smaller and under-resourced providers are ill-equipped to handle much of the level of detail outlined in this publication.

The document in many respects is very thorough, however, one of our chief concerns with the publication is that it is trying to be all things to all entities. Or, said another way, it takes a one size fits all approach. The HIPAA security rule is designed to be flexible, and this document could be improved if it was clearer that - like the rule - there is no single approach that will work for all entities.

II. More Resources Including Those Tailored to Smaller and Lesser Resourced Entities Including 405(d) Publications

A. Smaller / Lesser Resourced Providers

Traditionally smaller and lesser-resourced entities are typically much slower to adopt standards, best practices and technology, and meet compliance deadlines. Operating in the one of the most heavily regulated industries – if not the most regulated – presents enormous challenges to these smaller businesses and they need additional resources and support. For instance, as discussed below, smaller entities will be very challenged in conducting their own risk assessment and risk management program without additional assistance. The fact is cyber incidents among small providers are growing. Four out of five physicians, for example, have experienced some form of a cyber-attack.[1] Further, there are far more smaller healthcare providers than large ones and with all healthcare providers being target rich environments and increasingly exchanging growing volumes of data, it is critical we help these organizations, as neglecting that community poses a risk to the entire sector and to patient safety.

B. More Targeted Education and Resources are Needed

i. 405(d)

The tools developed under the 405(d) effort are directly tied to the NIST Cybersecurity Framework, a product strongly supported by our sector.

Given the intense focus and effort that has gone into developing the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) under the 405(d) Program and Task Group, NIST should focus attention on directing smaller and lesser resourced entities to these tools. The 405(d) effort with the HSCC is an outstanding example of what is possible under a joint public private partnership, and we encourage NIST to reference this resource where applicable and appropriate. These tools are designed to improve the cyber posture of organizations of different sizes and abilities to align compliance with the existing HIPAA security rule framework. The tool is scalable to guide smaller entities with a flexibility-by-design approach and without prescribing a single pathway to improving one's cyber posture.

ii. P.L. 116-321

On January 5, 2020, H.R. 7898 was signed into law as Public Law 116–321, marking an important milestone for HIPAA covered entities by offering them recognition in the form of shorter audits and fewer fines in exchange for adhering to "recognized security practices." The statute defines these as:

> *"(1) RECOGNIZED SECURITY PRACTICES.—The term 'recognized security practices' means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).*

The passage of this law moves our industry one step closer to helping healthcare entities pursue a better cyber posture by offering incentives rather than only punitive approaches. However, according to a survey published by the College of Healthcare Information Management Executives (CHIME), only 45 percent of survey respondents said they were aware of 405(d).[2] While we recognize that the P.L.116-321 pertains specifically to OCR enforcement authority rather than implementation guidance, it is nevertheless appropriate from both a policy and investment incentive perspective to recognize the statute's contextual linkage between the operational guidance in SP- 800-66r2 and two specific health sector resources: the Health Industry Cybersecurity Practices (HICP) promulgated under §405(d) and the soon-to-be-published *HPH Sector Cybersecurity Framework Implementation Guide,* produced jointly by HHS and the HSCC Cybersecurity Working Group in support of the NIST Cybersecurity Framework. Because the statute specifically references cybersecurity practices promulgated under the 405(d) program as well the NIST CSF and other "recognized security practices," the aforementioned resources and future joint publications of the HSCC and the 405(d) program constitute "recognized security

practices" under the statute and thus can help organizations meet Congressional intent by implementing the guidance contained in this NIST Special Publication.

iii. Multiple Benefits Associated with Using Cybersecurity Best Practices

Employing cybersecurity best practices like the ones outlined in HICP not only can help a HIPAA covered entity or business associate comply with the HIPAA security rule, it can also help with compliance with other federal mandates such as Promoting Interoperability which requires an annual risk assessment to avoid Medicare financial penalties and the new forthcoming cyber incident report mandates from the Cybersecurity & Infrastructure Security Agency (CISA) as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). For publicly traded companies like larger healthcare covered entities there is also a new cyber reporting mandate overseen by the Securities and Exchange Commission (SEC)

Beyond meeting federal mandates, there are also practical business reasons to employ better cyber practices including averting costly breach clean-ups and being priced out of cyber insurance, as well as suffering immense reputational harm. With breaches amounting to hundreds of thousands to millions of dollars or higher, and the costs to secure cyber insurance doubling or more, taking steps to improve one's cyber posture is mission critical.

Lastly, we believe it is worth emphasizing that patient safety requires cyber safety. While a discussion of this may seem outside the scope of the NIST document, educating users of the NIST product that improving cyber hygiene can improve patient safety offers another avenue to educate around this issue – especially for smaller and under-resourced providers - around the multiple benefits and importance of making this investment. There are growing numbers of stories that depict harms – some life threatening – around cyber incidents.

iv. **Pandemic Authorities**

Given the Public Health Emergency (PHE) declared by the Secretary of HHS which has consistently been renewed every 90 days since the inception of the pandemic, we believe small providers must be prepared to handle the policy and practical implications for what this means.

During the PHE many federal healthcare policies have been relaxed to accommodate efficient delivery of healthcare, minimize the regulatory burden on an overstrained workforce and ensure patients receive the timeliest access to care. Included among these flexibilities are relaxation of policies governed by HHS' Office for Civil Rights. On March 19, 2020 OCR announced the Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency. Included in this announcement was enforcement discretion associated with the delivery of telehealth. As such, OCR – during the PHE – allows for the delivery of telehealth using modalities that may not offer the level of security typically desired for use of video telecommunications. The intention behind this was based in large part to allow all providers but particularly smaller ones to rapidly scale up their telehealth presence to safely treat patients remotely.

As the pandemic winds down, it is imperative that providers understand the importance of migrating to more secure telecommunications platforms to reduce cyber incidents and protect patients. With telehealth now an ingrained method of care delivery this piece will be increasingly relevant.

v. Medical Devices

Section 3 focuses on the importance of conducting a risk assessment to ascertain where ePHI could be at risk for disclosure or use without proper authorization. Given the cybersecurity risks posed by improperly secured medical devices we believe added attention to this is warranted. We continue to find that smaller and lesser-resourced providers share login credentials or worse yet there are no credentials. For instance, how many small providers are aware that a point of care ultrasound in an emergency room must control access with more than just the on/off button? These types of scenarios are a blind spot for small providers with many being unaware of the risks.

Recommendation: Add questions to those found on pages 25-26 under "Preparing for a Risk Assessment" and "Identify Realistic Threats" that asks users of this document to consider whether their device(s) supports individual user authentication and what process is in place to have that managed.

Recommendations:

1. NIST should develop an entirely separate product focused on helping smaller, lesser resourced entities with advice on what is needed to secure electronic protected health information (ePHI) and the implications for not doing so; and

2. Include content on the following topics:

    i. 405(d) / HCIP resources designed specifically for smaller entities.

    ii. Potential mitigation of HIPAA Breach enforcement fines and/or audits available to HIPAA healthcare entities that follow the NIST CSF, 405(d) HICP and other recognized security practices.

    iii. Benefits associated with using cybersecurity best practices including meeting compliance with other federal mandate, practical business reasons, and patient safety; and

    iv. Importance of securing video telecommunications services.

III. Terminology

We note that the terms "risk analysis" and "risk assessment" are used interchangeably throughout the publication and often are assumed to be synonymous. However, they are distinct concepts and NIST has separate definitions for them in their online glossary. NIST defines them as:

Risk Analysis = Process to comprehend the nature of risk and to determine the level of risk.

> **Risk Assessment** = The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

We believe NIST should be consistent with the use of these terms and clarify when risk analysis is meant vs risk assessment to avoid confusion.

Recommendations:

1. Clarify in the document where assessment is intended vs where analysis is meant.
2. Support NIST moving the discussion of risk assessment from the appendix of the original document to the body of the document.

VI. Tables

Section 5

Recommendations for the table found on page 39 starting line 1014 under Section 5, "Considerations When Implementing the HIPAA Security Rule."

We offer the following revisions to this table:

1. **Section 5.1.1**, **Administrative Safeguards, Security Management Process:** Add "Develop and approve a training strategy and a plan" and include a question such as like "Are there any considerations for role-based information security training?"
2. **Section 5.2.1, Physical Safeguards, Facility Access Control:** Under item 1 add "Conduct an analysis of existing physical security vulnerabilities" and a related question, "Is there a list of employees who can access the facility after-hours via the use of keys, badge access, and knowledge of the security or alarm system?"
3. **Section 5.3.1, "Technical Safeguards, Access Control":** Add "Ensure that all system users have been assigned a unique identifier," and a question "Are audits being done to monitor system activity?"

Table 3

Table 3 - Assessment Scale for Overall Likelihood is contained on page 27 on line 735 and is designed to help an organization ascertain the likelihood of a threat successfully exploiting a vulnerability. We believe that conducting a risk assessment may be challenging for small entities. Nonetheless, we also believe it is an imperative. given increased data in circulation and the increasingly interconnected, digitized nature of healthcare.

There are existing resources developed by HHS and HSCC that smaller entities can use and should be made aware of. However, we also believe there is room for NIST to develop more products tailored to smaller healthcare entities building upon existing resources.
The focus of a new document aimed at small providers – as recommended earlier - should impart how critical it is they pay attention to risk assessment. Given the criticality associated with the aforementioned areas that pose risk to patients, business operations, compliance and more, the importance of conducting a risk assessment cannot be overstated and responsibility for this should not be simply abdicated to a consultant or vendor exclusively – stakes are simply too high.

Recommendations: Rather than pointing smaller / lesser-resourced entities to Table 3, we believe a more fruitful approach would be to:

1. Point them to the HHS' Security Risk Assessment tool;
2. Develop more tools better suited to smaller entities
3. Impart the importance of conducting a risk assessment.

Table 4

Table 4 - Security Objectives and Impacts is contained on page 28 on line 768 and is designed to help an organization determine the impact to ePHI if a threat exploits a vulnerability. From our perspective, there are items in here that are outside the scope of healthcare HIPAA covered entities and the healthcare sector.

Recommendations: Revise the table to better align with the needs of healthcare organizations and focus on patient safety by making the following changes:

1. **Loss of Confidentiality:** Remove language in Table 4, row 1 on Confidentiality that says, "The impact of an unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in the loss of public confidence, embarrassment, or legal action against the organization" and replace with "The HIPAA Privacy 391 Rule at 164.530(c)(1) states, "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."
2. **Loss of Integrity:** Change the word "information" in the first sentence, "System and data confidentiality refers to the protection of information from unauthorized disclosure..." to "ePHI".
3. We do not suggest adding "ePHI" to the other two rows (viz. Integrity and Availability") as they should be considered more broadly than just ePHI.

V. Appendix F

Appendix F found on page 141, starting line 1525: The resources listed have been carried over from the original publication and we believe this appendix could be more useful if it were better organized, contained updated information and less one-size fits all. For instance, quite a number of resources are provided and include many from US federal government repositories, including dozens of links to resources from the Office of the National Coordinator for Health IT (ONC), 405(d), HHS' HC3 cyber command center, Assistant Secretary for Preparedness and Respond (ASPR), OCR, the Food and Drug

Administration (FDA), NIST, and CISA, and a few collaborative resources from the HSCC. There is only one link to private or commercial pages - , the MITRE ATT&CK framework. Much study would be needed for an organization to get a comprehensive picture provided by all of these linked documents.
We appreciate that there's a section for small organizations which limits the topics to eight, however, we nonetheless feel this appendix would be more impactful if reorganized per below.

Recommendations:

1. Organizing the entire Appendix F into a logical progression, such as the Risk Management Framework (RMF) or CSF's several stages;
2. Moving or copying the Getting Started guides or NIST referenced documents to the head of each relevant section may also help lessen the learning curve and provide a scaffolded learning structure; and
3. Organizing the resources with descriptions on how each resource should be used.

VI. Conclusion

The HSCC appreciates the opportunity to offer our ideas on how to improve this important document and help HIPAA covered entities better fortify their systems and infrastructure, better manage the risk to the PHI they are tasked with safeguarding, reducing threats to patient safety, and meeting their compliance responsibilities. Should you have any questions regarding our comments please do not hesitate to contact Greg Garcia, Executive Director, HSCC at greg.garcia@healthsectorcouncil.org.

Sincerely,

Greg Garcia
Executive Director
Health Sector Coordinating Council Cybersecurity Working Group

---

[1] https://www.nist.gov/system/files/documents/2019/10/16/1-4-hicp-405d-chua-decker-heesters.pdf

[2] https://chimecentral.org/wp-content/uploads/2021/08/PP_infographic-v5_Handout.pdf