July 7, 2021

Eric K. Lin
Acting Associate Director
National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Submitted electronically via sp800-66-comments@nist.gov

Dear Acting Associate Director Lin:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments in response to the update of An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule ("Resource Guide"). HIMSS strongly supports the National Institute of Standards and Technology's (NIST's) decision to update the Resource Guide to include improvements to the guide as well as increase awareness, applications, and uses for it. The twelve-plus years that have occurred since SP-800-66, Revision 1, have seen dramatic changes in technology and data usage. The Resource Guide review and update is an excellent opportunity to align the text of this document with the current state of relevant laws and regulations to educate its users and enhance best practices in the security and data privacy realm.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. Established in 1961, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 105,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations.

Overall, we applaud NIST for creating the Resource Guide to be a helpful document for any agency or stakeholder seeking to better understand how to comply with the provisions of the HIPAA Security Rule—we find real value in a resource being tailored to address and educate on HIPAA's security safeguards. However, given that this document has not been updated to the current version of HIPAA Omnibus Rule, which implements certain provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Public Law 111–5), the value of the NIST guidance

document as a compliance tool is diluted. One suggestion is that NIST seek to align the Resource Guide with the NIST Security Risk Assessment Tool to better address this shortcoming.

HIMSS also urges the guidance document be updated to include best practices in terms of dealing with today's aggressive threats, including phishing, ransomware, and insider threat risks. Where possible, we encourage NIST to cross-reference other up-to-date NIST guidance documents. The Resource Guide should also make clear that complying with HIPAA does not necessarily ensure that an organization's information will be secure. To that end, there should be an alignment as well to the NIST Cybersecurity Framework that outlines the essential steps that all organizations need to follow to achieve a better security posture.

Although NIST makes clear in the existing Resource Guide that organizations are not required to use this document, once the appropriate updates are made, we urge the agency to promote its existence and value through as many communication vehicles as possible. Focus should be placed on messaging that alerts the community to its availability, its value, and exactly how best to use it as a tool in everyday cybersecurity workflows. Greater comprehension of the context and specifics of the Resource Guide will help individuals and organizations have greater confidence that they are implementing the Security Rule appropriately.

We offer the following thoughts and recommendations for ensuring that the revisions to the Resource Guide include the valuable and necessary updates needed to promote the sharing of protected health information (PHI) while guaranteeing the confidentiality, integrity, and availability of patient data:

Updates to the Resource Guide Must Reflect References and Implications to Current Regulations Including But Not Limited to the HITECH Act and The HIPAA Omnibus Rule

Since the Resource Guide's Revision 1 was published in 2008, fundamental changes affecting security requirements have been implemented through the HITECH Act and the HIPAA Omnibus Rule that are not currently reflected in the Resource Guide. We encourage NIST to include educational materials regarding patient access rights and how components surrounding those provisions of the HIPAA Privacy Rule work hand-in-hand with the new interoperability regulations, particularly the data exchange and information blocking requirements stemming from the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS). Overall, it is important to note how privacy and security are inextricably linked and that the concerns in the cybersecurity world are even more manifest with respect to privacy, HIPAA, and the interoperability regulations.

The Updates to the Resource Guide Should Include the Following Existing NIST References and Federal Resources

NIST guidance, including this resource, must be coordinated with the guidance relayed to the public by other agencies, including the Department of Health and Human Services Office of Civil Rights (OCR) and ONC. In addition, NIST must work with other

agencies to bring clarity to its users as to how the foundational privacy and security regulations function together. For example, by using this Resource Guide to accomplish that objective, we recommend referencing the crosswalk between the HIPAA Security Rule and the various cybersecurity frameworks, including the NIST Cybersecurity Framework and others (e.g., HITRUST, ISO, and COBIT).

Additionally, several NIST documents relevant to cybersecurity are up-to-date and should be incorporated by reference into this document. These documents should include:

- NIST Zero Trust Architecture (SP 800-207)
- NIST Workforce Framework for Cybersecurity (NICE Framework) (SP 800-181 Rev. 1)
- NIST Control Baselines for Information Systems and Organizations (SP 800-53B)
- NIST Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)
- NIST Cybersecurity Framework

Moreover, we suggest recent federal guidance relative to ransomware and threats, particularly from the Federal Bureau of Investigation (FBI), OCR, and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), be included. Examples of some of these resources include:

- FBI Ransomware Prevention and Response for Chief Information Security Officers (CISOs)
- OCR Fact Sheet on Ransomware and HIPAA
- DHS CISA Alert on Top 10 Routinely Exploited Vulnerabilities

Amplify Overall Awareness of this Resource to Encourage Stakeholder Engagement, Use, and Understanding of the Significance of the Updates

The HIPAA Privacy and Security Rules govern how PHI may be used and disclosed, as well as how it should be secured in terms of physical, technical, and administrative safeguards to ensure the confidentiality, integrity, and availability of information. Good cybersecurity practices help ensure that data will remain confidential, have integrity, and be available on demand. Cybersecurity, a key responsibility of data stewardship, is a necessary predicate to data privacy, access, and usage. Data should be protected, not just to preserve privacy but also to protect the patient and maintain safety.

Recognizing the value of such data, we need to have robust cybersecurity policies and corresponding practices to ensure healthcare data interoperability. People, processes, and technology must work in tandem to facilitate data privacy. Therefore, there must be a more significant push to educate potential users on the NIST Resource Guide and its content.

When finalized, we encourage NIST to join with partner federal agencies on an educational campaign to help the community understand how to make the most effective use of its updated information. The Resource Guide is an opportunity to bring together a compendium of relevant material and eliminate the need for individuals

and organizations to search in multiple areas for the information necessary to comply with current privacy, security, and cybersecurity standards.

HIMSS welcomes the opportunity to be a resource to NIST on innovative, forward-thinking steps to educate the public about the value of this Resource Guide as well as how the broader healthcare community should think about better leveraging its content.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Ashley Delosh, HIMSS Senior Manager of Government Relations, at Ashley.Delosh@himss.org , or Jeff Coughlin, HIMSS Senior Director of Government Relations, at Jeff.Coughlin@himss.org, with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO