April 25, 2022

James K. Olthoff, Ph.D.
Director
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management" Request for Information (NIST-2022-0001)

Dear Dr. Olthoff:

The Confidentiality Coalition appreciates the opportunity to provide comments on the National Institute of Standards and Technology's (NIST) request for information on, "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management."

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective patient privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Cybersecurity concerns are a significant challenge for healthcare stakeholders. In 2021, over 45 million individuals were impacted by cyber attacks on healthcare entities, a record amount.[1] Of the 16 sectors categorized as "critical infrastructure," healthcare companies reported the greatest number of ransomware attacks in 2021.[2] The Confidentiality Coalition thanks NIST and other federal agencies for their work in helping industry respond to these attacks and providing technical assistance and guidance to entities so that they can improve their cybersecurity capabilities. In particular, NIST's Cybersecurity Framework is an important resource for

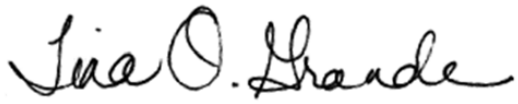
[1] Heather Landi, *Healthcare data breaches hit all-time high in 2021, impacting 45M people*, Fierce Healthcare (February 1, 2022), https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people.
[2] *Internet Crime Report 2021*, Federal Bureau of Investigation Internet Crime Complaint Center (March 23, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

stakeholders to not only develop and implement successful cybersecurity practices but respond and recover from unauthorized access into systems.

While we support developing clear guidelines to improve cyber readiness, the Coalition encourages NIST to recognize the extensive security and breach notification requirements that healthcare entities must comply with and to harmonize the Cybersecurity Framework with these regulations. In particular, the HIPAA Security Rule provides a standard for how health data must be protected by covered entities and their business associates. Failure to comply with this rule can lead to significant financial penalties. By further aligning the Cybersecurity Framework with HIPAA, healthcare stakeholders will be better equipped to leverage sophisticated cybersecurity tools while ensuring regulatory compliance. Additionally, we encourage NIST to engage with the Cybersecurity and Infrastructure Security Agency (CISA) in light of upcoming rulemaking mandating breach reporting to CISA for all critical infrastructure. The Coalition also thanks NIST for their extensive work on developing frameworks to address questions of privacy and artificial intelligence, as well. Given that many of these areas require robust cybersecurity protections as well, we encourage NIST to examine ways to further harmonize current and future frameworks to best integrate interconnected themes.

The Confidentiality Coalition looks forward to working with you on further steps to improve cybersecurity readiness. Included is a copy of the Confidentiality Coalition's principles on cyber incident reporting, which might provide insight as NIST evaluates amendments to its framework. Please contact me at tgrande@hlc.org or 202-449-3433 with any questions.

Sincerely,



Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council