ConnectedHealthInitiative

February 2, 2024

Information Technology Laboratory
ATTN: AI E.O. RFI Comments
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Comments of the Connected Health Initiative to the National Institute of Standards and Technology, *Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11)* [88 FR 88368]

The Connected Health Initiative (CHI) appreciates the opportunity to submit views to the National Institute of Standards and Technology (NIST) regarding its responsibilities under the Executive order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI), including undertaking an initiative for evaluating and auditing capabilities relating to AI technologies; and to develop a variety of guidelines, including for conducting AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems.[1] CHI is the leading multistakeholder policy and legal advocacy effort driven by a consensus of thought leaders from across the connected health ecosystem. We aim to realize an environment where Americans can improve their health through policies that allow connected health technologies to enhance health outcomes and reduce costs. As part of its commitment to responsibly advance AI in healthcare, CHI assembled a Health AI Task Force consisting of a range of innovators and experts, which developed a number of recommendations for policymakers, each appended to this comment letter. We encourage NIST to consider each of these resources as it moves forward with its AI RMF:

- **CHI's Health AI Policy Principles**, a set of recommendations on the wide range of areas that should be addressed by policymakers examining AI's use in healthcare (available at https://bit.ly/3m9ZBLv);
- **CHI's Position Paper, *Why AI? Considerations for Use of Artificial Intelligence in States' Medicaid and CHIP Programs***, which maps CHI's Health AI Policy Principles to the challenges and opportunities faced at the state level (https://bit.ly/2Y2FJle);
- **CHI's *Good Machine Learning Practices for FDA-Regulated AI***, a proposed risk-based approach to benefit the Food and Drug Administration (FDA) as it addresses both locked and continuously-learning AI systems that meet the definition of a medical device (https://bit.ly/2YaYljk); and
- **CHI's *Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem***, a proposal on ways to increase the transparency of and trust in health AI tools, particularly for care teams and patients (https://bit.ly/3n36WO5).

[1] 88 FR 88368.

NIST's AI-related efforts, including those pursuant to the Executive order, as well as the efforts of numerous agencies with respect to AI policy and regulation, directly impact the digital health developer and user communities. We support NIST's efforts to accomplish its goals of (1) establishing guidelines and best practices in order to promote consensus industry standards in the development and deployment of safe, secure, and trustworthy AI systems; (2) he potential development of further science-backed standards and techniques for reducing the risk of synthetic content from AI technologies; and (3) establishing a plan for global engagement on promoting and developing AI consensus standards, cooperation, and coordination, ensuring that such efforts are guided by principles set out in the NIST AI Risk Management Framework (AIRMF) and the U.S. Government National Standards Strategy for Critical and Emerging Technology (NSSCET).

While the potential for generative AI is incredible, CHI is forthright in acknowledging that AI also has the potential to raise a variety of unique considerations for policymakers. We appreciate U.S. policymakers' efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers, and strongly encourage NIST's Executive order-related deliverables and efforts to align with CHI's comprehensive health AI policy principles (available at https://bit.ly/3m9ZBLv).

Noting our general support for NIST's efforts as discussed above, we offer the following responses to specific questions posed in NIST's request for information.

Developing Guidelines, Standards, and Best Practices for AI Safety and Security

CHI commends NIST's steps taking in this request for information to understand generative AI risk management, AI evaluation, and red-teaming, and support NIST's effort to NIST to establish guidelines and best practices to promote consensus industry standards in the development and deployment of safe, secure, and trustworthy AI systems. NIST is well-positioned to ensure that the roles and needs of the private sector, including small businesses, are appropriately considered.

We appreciate that NIST has been tasked with creating a risk management framework for generative AI, as a companion to the existing AIRMF, and urge the "companion" generative AI deliverable to build on NIST frameworks that are already widely-relied upon, including but not limited to the NIST Cybersecurity Framework, the NIST Secure Software Development Framework, and the NIST AIRMF.

CHI encourages NIST's generative AI-specific guidelines and best practices to align with CHI's policy principles for AI discussed above, the NIST AI RMF, and leading standards such as ISO/IEC 23894:2023.[2] CHI supports the development of a companion resource to the NIST RAIFW addressing the distinct risks and harms of generative AI. A companion resource elaborating on standards/norms, practical tips on improving AI risk management, and commentary/recommendations on workforce/skill issues in generative AI risk management, done in collaboration with the private sector, will be valuable resources to the CHI's unique community. This new companion should also include discussion on the benefits of generative AI to ensure that it is not perceived as a discouragement for small business engagement across generative AI opportunities.

[2] https://www.iso.org/standard/77304.html.

CHI also supports such a resource addressing "roles that can or should be played by different AI actors for managing risks and harms of generative AI (*e.g.*, the role of AI developers vs. deployers vs. end users)." CHI notes that such roles and interdependencies may vary widely across sectors and use cases. A prime example is the healthcare sector, where unique players and roles exist across the value chain. It will be important that NIST's discussion of roles in generative AI risk management accounts for these differences.

In its efforts to create "guidance and benchmarks for evaluating and auditing AI capabilities," CHI urges NIST to first undertake a comprehensive landscape assessment to ensure that it fully understands the status of related efforts, both inside and outside of government, before moving forward. In some sectors, testing networks are only just being created, and no consensus criteria yet exists. What is certain today, however, is that, consistent with the need for risk mitigation that correlates to the known harms presented, evaluation and auditing practices should be scaled based on the unique use cases and risks presented by a given generative AI use case. Further, such criteria should not be dictated by government alone; instead, key actors in government, led by NIST, should collaborate with private sector innovators to develop criteria for evaluating and auditing AI capabilities based on where consensus can be achieved. CHI also urges NIST to consider our comments to the National Telecommunications and Information Administration on AI accountability,[3] which speak to NIST's interests in the generative AI evaluation space.

CHI notes its support for a public-private partnership approach to procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. Our community is committed to working with NIST and other policymakers to advance thoughtful AI design, as well as auditing/monitoring, best practices that will ensure deployment of safe, secure, and trustworthy systems.

With respect to NIST efforts pursuant to Section 4.1(a)(ii), we agree that red-teaming efforts are important in ensuring the safe, secure, and trustworthy systems. We urge NIST to ensure that it appropriately differentiates between AI *model* red-teaming (attempting to break the AI model to find ways to improve it) and AI *system* red-teaming (attacking the model along with its data infrastructure, user interface, etc.), as both have unique roles. Consistent with the priority discussed above for risk management practices that scale to known potential harms, the need for the type and intensity of red-teaming will need to scale. CHI also urges for careful consideration of the overlap of legal liabilities with red-teaming (for example, red-teaming efforts to address potential model harms may give rise to liabilities for creating the same). CHI also agrees that a trusted information sharing construct, similar to that used for the timely sharing of cybersecurity threat information through Information Sharing and Analysis Centers (ISACs), could be key means for the sharing best practices for generative AI, including for how to share with external parties for the purpose of AI red-teaming while protecting intellectual property, privacy, and security of an AI system. Finally, we urge NIST to be mindful of the requirement on dual-use foundation model developers to provide the results of their AI red-teaming to the Commerce Department.

Reducing the Risk of Synthetic Content

[3] Included in this comment as **Appendix A**.

CHI supports NIST's efforts to, consistent with Section 4.5(a) of the Executive Order, identify existing standards, tools, methods, and practices; and to contribute to the development of a description of the potential development of further science-backed standards and techniques for reducing the risk of synthetic content from AI technologies. We strongly encourage collaboration with our community, and others from the private sector, in reaching a consensus on the stated problem's meaning ("the risk of synthetic content from AI technologies") as well as the state of standards, tools, methods, and practices for addressing it. Collaboration on "synthetic content from AI technologies" must consider a range of angles and interests, including with respect to intellectual property questions currently being grappled with by U.S. courts. We discourage formulating recommendations on AI-created "synthetic content" under this Executive order that would short-circuit (1) voluntary approaches in development and use already and (2) established policymaking channels (e.g., the federal courts adjudicating claims of copyright infringement in the development of AI) that will determine whether today's legal frameworks can adequately address such an issue.

Advance Responsible Global Technical Standards for AI Development

CHI fully supports U.S. government's global engagement to promote and develop AI consensus standards, cooperation, and coordination; and to ensure that such are guided by principles set out in the NIST AIRFM and NSSCET. Separately, CHI has offered detailed views to NIST on ways to globally promote and implement the AIRMF[4] and we request that NIST consider those recommendations as it works to meet its goals per Section 11(b). Again, we urge for alignment with and promotion of international standards for AI development and safety, namely ISO/IEC 22989:2022. CHI also urges NIST to align its international advocacy with CHI's AI policy principles discussed above.

***

CHI appreciates NIST's consideration of the above views. We urge NIST to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Executive Director

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005

[4] CHI views are included in this comment as **Appendix B**.

ConnectedHealthInitiative

June 12, 2023

The Honorable Alan Davidson
Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: Comments of the Connected Health Initiative to the National Telecommunications and Information Administration on its AI Accountability Policy Request for Comment (NTIA–2023–0005)

Dear Assistant Secretary Davidson:

The Connected Health Initiative (CHI) appreciates the opportunity to provide input to the National Telecommunications and Information Administration (NTIA) on developing a productive artificial intelligence (AI) accountability ecosystem.[1] CHI is the leading multistakeholder policy and legal advocacy effort driven by a consensus of thought leaders from across the connected health ecosystem. We aim to realize an environment where Americans can improve their health through policies that allow connected health technologies to enhance health outcomes and reduce costs.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking, such as learning and reasoning. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML), where algorithms use data, learn from it, and apply their newly-learned lessons to make informed decisions, and deep learning, where an algorithm based on the way neurons and synapses in the brain change as they are exposed to new inputs allows for independent or assisted decision-making. AI-driven tools are having, and will continue to have, substantial direct and indirect effects on Americans in how they manage their health. Some forms of AI are already being used to improve American consumers' lives today – for example, AI is used to accomplish backend administrative functions for healthcare providers. Moving forward, AI has incredible potential to advance the Quadruple Aim; for example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of x-rays and other medical imaging. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions. It is

[1] https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment

estimated that AI technological breakthroughs will represent a $126 billion market by 2025.[2]

Nonetheless, AI's growing use raises a variety of challenges, and some new and unique considerations, for policymakers as well as those making AI operational in healthcare. CHI appreciates NTIA's exploration of policies to provide reliable guidance to stakeholders to reassure end-users that AI systems are legal, effective, ethical, safe, and otherwise trustworthy.

As part of its commitment to responsibly advance AI in healthcare, CHI has developed a number of resources for policymakers, linked to below. **Notably, CHI's policy principles for AI governance and policy address quality assurance and oversight, recommending that any AI policy framework utilize risk-based approaches to ensure that the use of AI aligns with the recognized standards of safety, efficacy, and equity; and ensure the appropriate distribution and mitigation of risk and liability by providing that those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so.** We encourage NTIA to align its next steps with each of these resources:

- CHI's *Health AI Policy Principles*,[3] a set of recommendations on the wide range of areas that should be addressed by policymakers examining AI's use in healthcare (available at https://bit.ly/3m9ZBLv);
- CHI's Position Paper, *Why AI? Considerations for Use of Artificial Intelligence in States' Medicaid and CHIP Programs*, which maps CHI's Health AI Policy Principles to the challenges and opportunities faced at the state level (https://bit.ly/2Y2FJle);
- CHI's *Good Machine Learning Practices for FDA-Regulated AI*, a proposed risk-based approach to benefit the Food and Drug Administration (FDA) as it addresses both locked and continuously-learning AI systems that meet the definition of a medical device (https://bit.ly/2YaYljk); and
- CHI's *Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem*, a proposal on ways to increase the transparency of and trust in health AI tools, particularly for care teams and patients (https://bit.ly/3n36WO5).

Further, CHI strongly urges for a coordinated effort across both executive and independent agencies. Already, numerous regulatory agencies, some cross-sectoral and others sector-specific, are considering or advancing regulatory proposals that would take starkly different approaches to AI accountability. Some of these proposals are

[2] McKinsey Global Institute, *Artificial Intelligence: The Next Digital Frontier?* (June 2017), *available at* https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.

[3] Are also included with this comment as **Appendix A**.

poised to put significant hurdles in place for the development and use of AI through one-size-fits -all approaches that have nominal public benefit at best, such as the Department of Health and Human Services Office of Civil Rights' proposed approach to preventing discriminatory outcomes in healthcare,[4] which CHI has detailed its views on publicly (and we encourage NTIA's consideration of these viewpoints as a leading example of sector-specific misalignment with other leading Administration efforts, such as that of the National Institute of Standards and Technology [NIST][5]). In some cases, such proposals are being developed based on speculative and undemonstrated harms.[6] NTIA, along with other cross-sectoral subject matter expert agencies in the federal government such as NIST, should take immediate steps to ensure a harmonized and informed approach to AI governance.

Many entities, both public and private, are actively engaging in efforts to create and enforce AI accountability frameworks, which may lead to he creation of trusted audits/assessments/certifications. While this area continues to evolve, we strongly urge for NTIA's alignment with NIST's efforts to develop a voluntary artificial intelligence risk management framework (AI RMF), which aims to help designers, developers, users, and evaluators of AI systems evolve in knowledge, awareness, and best practices to better manage risks across the AI lifecycle.[7] NIST's AI RMF is best positioned to guide federal government efforts in addressing AI due to NIST's expertise and its collaborative and open approach to developing the AI RMF, similar to NIST's Cybersecurity Framework.[8] And it is in the public's best interest that the NIST AI RMF's scaled, risk-based approach serve as a basis for both executive and independent agencies' approach to AI risk management and governance; and that NTIA take active steps to bring federal agencies into alignment with this approach.

---

[4] Nondiscrimination in Health Programs and Activities, 87 FR 47824 (Aug. 4, 2022); CHI's Connected Health Initiative detailed views on this HHS OCR proposal are included in this comment as **Appendix B**.

[5] https://www.nist.gov/itl/ai-risk-management-framework.

[6] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FR 51273 (Aug. 22, 2022); CHI views provided to the Federal Trade Commission in response to its Advanced Notice of Proposed Rulemaking are included in this comment as **Appendix C**.

[7] https://www.nist.gov/itl/ai-risk-management-framework.

[8] https://www.nist.gov/cyberframework.

CHI appreciates NTIA's consideration of the above views. AI offers immense potential for widespread societal benefit, particularly in healthcare, which is why NTIA's voluntary RMF should foster investment and innovation in any way practicable. We urge NTIA to contact the undersigned with any questions or to explore ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Executive Director

Leanna Wade
Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005

ConnectedHealthInitiative

January 25, 2022

Mr. Mark Przybocki
U.S. National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Comments of the Connected Health Initiative to the National Institute of Standards and Technology on its Artificial Intelligence Risk Management Framework Concept Paper

The Connected Health Initiative (CHI) appreciates the opportunity to submit its views to the National Institute of Standards and Technology (NIST) on its Artificial Intelligence Risk Management Framework Concept Paper.[1] CHI is the leading multistakeholder policy and legal advocacy effort driven by a consensus of thought leaders from across the connected health ecosystem. We aim to realize an environment where Americans can improve their health through policies that allow connected health technologies to enhance health outcomes and reduce costs. As part of its commitment to responsibly advance AI in healthcare, CHI assembled a Health AI Task Force consisting of a range of innovators and experts, which developed a number of recommendations for policymakers, each appended to this comment letter. We encourage NIST to consider each of these resources as it moves forward with its AI RMF:

- CHI's Health AI Policy Principles, a set of recommendations on the wide range of areas that should be addressed by policymakers examining AI's use in healthcare (available at https://bit.ly/3m9ZBLv);
- CHI's Position Paper, *Why AI? Considerations for Use of Artificial Intelligence in States' Medicaid and CHIP Programs*, which maps CHI's Health AI Policy Principles to the challenges and opportunities faced at the state level (https://bit.ly/2Y2FJle);
- CHI's *Good Machine Learning Practices for FDA-Regulated AI*, a proposed risk-based approach to benefit the Food and Drug Administration (FDA) as it addresses both locked and continuously-learning AI systems that meet the definition of a medical device (https://bit.ly/2YaYljk); and

[1] https://www.nist.gov/system/files/documents/2021/12/14/AI%20RMF%20Concept%20Paper_13Dec2021_posted.pdf.

- CHI's Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem, a proposal on ways to increase the transparency of and trust in health AI tools, particularly for care teams and patients (https://bit.ly/3n36WO5).

Noting our general support for NIST's efforts to develop a voluntary prioritized, flexible, risk-based, outcome-focused, and cost-effective AI RMF, we offer the following further input:

- **NIST's AI RMF Should be Scalable, Modular, and Aligned with International Standards:** CHI supports, and urges NIST to maintain, the concept paper's positioning of the AI RMF to leverage a scalable approach to risk management, similar to the approach taken in NIST's Cybersecurity Framework. Such an approach recognizes that appropriate risk management practices reflect specific fact patterns and the unique risks posed by certain uses of AI. The AI RMF should reflect that trustworthiness is sector-dependent and that particular risk management practices develop trust—rather, the AI RMF should make clear that risk management processes assist organizations to design and develop trustworthy solutions. We support NIST's proposal to identify Core Functions (and subcategories within each Function) that will assist organizations in using the NIST AI RMF.

  Past these organizing principles, we encourage the future NIST AI RMF to map to, and rely on, international standards such as from ISO-IEC/JTC-1-SC 42, IEEE, ASTM, and SAE. We recognize, however, that international standardization for AI risk management is not yet robust. As AI standardization matures, it will be important that NIST continue to update its AI RMF periodically (ideally annually), and that its collaborators abroad do the same.

- **NIST's AI RMF Should Be Voluntary:** We strongly support maintaining the NIST AI RMF's voluntary character, much like the NIST Cybersecurity Framework. To this end, NIST should recognize that some may attempt to position the NIST AI RMF as a mandatory standard of behavior (e.g., in litigation). NIST's AI RMF should forthrightly address this concern and reinforce in the NIST AI RMF that (1) adoption of the RMF is voluntary for the private sector and (2) that the RMF is not, and is not to be offered as, a baseline for behavior norms in the context of litigation.

- **NIST's AI RMF Should Advance Thoughtful Design Principles Across AI Use Cases:** We encourage NIST to ensure that the RMF prioritizes the design of AI systems being informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems solutions should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should take advantage of collaboration and dialogue among users, AI technology developers, and other interested parties in order to have all perspectives

reflected in AI solutions. As this concept must run across sectors and AI use cases, we call on NIST to advance thoughtful design principles in the RMF.

The AI RMF should be crafted to the needs of different sectors. For example, the concept paper refers to "society-level risk," but this term is ambiguous and does not mesh well with the idea of intended use in the context of medical devices regulated by the FDA; rather than society-level risks, the medical device industry focuses on risks to patients and risks to patient populations.[2] Different industries and sectors will need to focus on other impacted stakeholder groups due to, among other requirements, regulatory requirements (as a further example, the automobile industry may need to assess risks to the vehicle driver, to other drivers on the road, or to pedestrians), which underscores that the AI RMF must not impede different sectors' unique risk management needs.

The required depth for risk analysis will also depend on established precedent. For lower risk devices (e.g., a digital thermometer), showing the device is useable and useful to the intended user is sufficient. For higher risk devices (e.g., a pacemaker), manufacturers may be asked to show a more comprehensive risk/benefit analysis in the intended context of use, or a suitable clinical study. This is to say that, even within sectors, risk analysis will depend heavily upon the purpose the device serves—another indicator that different sectors will need flexibility in risk management processes.

- **NIST's AI RMF Should Advance Ethics in AI's Development and Use:** The success of AI depends on ethical development and use, which in turn impacts user's trust and use of AI. The RMF should promote existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. We call on NIST to include a provision in its RMF providing for stakeholders' approaches to AI to duly consider ethics so that policies advance that:
    - Ensure that AI solutions align with all relevant ethical obligations, across the lifecycle of algorithms or models.
    - Encourage the development or updates of ethical guidelines to address issues emerging with the AI's use, as needed.
    - Maintain consistency with international conventions on human rights.

[2] *See* FDA, *Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions Guidance for Industry and Food and Drug Administration Staff* (Dec. 2016), *available at* https://www.fda.gov/files/medical%20devices/published/Factors-to-Consider-Regarding-Benefit-Risk-in-Medical-Device-Product-Availability--Compliance--and-Enforcement-Decisions---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf.

    - Ensure that AI is inclusive such that AI solutions beneficial to consumers are developed across socioeconomic, age, sex, gender, geographic origin, and other groupings.
    - Reflect that AI tools may reveal extremely sensitive and private information about a user or group and ensure that laws protect such information from being used to discriminate against certain consumers

- **NIST's AI RMF Should Prioritize Necessary Disclosures and Transparency:** CHI supports NIST's RMF in helping providers, technology developers and vendors, and others involved to understand the distribution of risk and liability in building, testing, deploying, and even decommissioning AI tools. The RMF should advance the appropriate distribution and mitigation of AI-related risks and liabilities. That is, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should be incentivized take reasonable steps to do so. Further, the RMF should clearly state that those developing, offering, or testing AI systems provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those impacted (as well as expected to be impacted) to use the AI solution. References to "intended use" and "context of use" as concepts is an appropriate approach for AI risk management, which encourages AI developers to identify and model to address challenges prior to algorithm development, which in turn allows developers to identify and evaluate potential threats more effectively. A focus on intended use also discourages generating solutions first and fitting those solutions to a problem second, which increases risk that possible threats, such as bias, are overlooked. Developing this aspect of the AI RMF should include consulting with consumers, as well as developers of AI and other stakeholders.
- **Harmonize the NIST AI RMF Internationally:** We urge NIST to include a priority for aligning, where appropriate, with international efforts, and upon completion, promoting the NIST AI RFM for use internationally. Already, developers of AI face top-down and one-size-fits-all mandates that substantially impede their ability to develop and utilize AI across a range of use cases. It is crucial that the NIST AI RMF be offered as an alternative to such mandates, or at least have a positive influence on mandates, from other jurisdictions.

CHI appreciates NIST's consideration of the above views. AI offers immense potential for widespread societal benefit, particularly in healthcare, which is why NIST's voluntary RMF should foster investment and innovation in any way practicable. We urge NIST to contact the undersigned with any questions or to explore ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005