ConnectedHealthInitiative

March 27, 2024

Mr. Travis Hall
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 Dual Use Foundation Artificial Intelligence Models With Widely Available Model Weights (Docket No. 240216-0052)

The Connected Health Initiative (CHI) appreciates the opportunity to provide input to the National Telecommunications and Information Administration (NTIA) on on the potential risks, benefits, other implications, and appropriate policy and regulatory approaches to dual-use foundation artificial intelligence (AI) models for which the model weights are widely available.[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. We encourage NTIA to consider each of these resources as it moves forward:

- **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);
- **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); and
- **CHI's Health AI Roles & Interdependencies Framework,** a proposal of clear definitions of stakeholders across the healthcare AI value chain, from development to distribution,

[1] https://www.federalregister.gov/documents/2024/02/26/2024-03763/dual-use-foundation-artificial-intelligence-models-with-widely-available-model-weights.

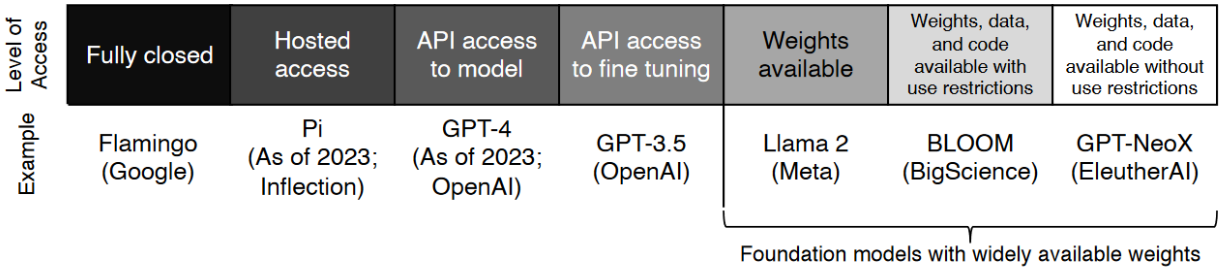
deployment, and end use; and a discussion of roles for supporting safety, ethical use, and fairness for each of these important stakeholder groups that are intended to illuminate the interdependencies between these actors, thus advancing the shared responsibility concept (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf).

CHI appreciates NTIA's discussion of open model foundations in its request for information, and agrees that open model foundations can support competition and innovation, and further transparency. Models with widely available weights can benefit from a feedback loop that includes users and developers, enabling eased feature improvements as well as identification and mitigation of risk, while spending less resources.

CHI appreciates NTIA's requesting input on how today's open source software licensing approach could inform its approach to dual use foundation models. While not analogous (because open source software licenses do not encapsulate all components and capabilities of an AI model), open source licenses can be beneficial in many scenarios by harmonizing terminology, training, deployment, weights, and documentation/monitoring. However, such licenses cannot actively prevent malfeasance. Ultimately, CHI believes that the market, not government, should organically develop open model licensing approaches.

Further, building on the above, we offer the following comments and recommendations to NTIA:

- ***Improve its categorization of foundation models:*** Categorizing foundation models as either "open" of "closed" will not reflect the important distinctions between key existing categories of foundation models. The degree of "openness" depends on a range of factors,[2] making the drawing of a hard line between "open" and "closed" arbitrary.



Level of Access	Fully closed	Hosted access	API access to model	API access to fine tuning	Weights available	Weights, data, and code available with use restrictions	Weights, data, and code available without use restrictions
Example	Flamingo (Google)	Pi (As of 2023; Inflection)	GPT-4 (As of 2023; OpenAI)	GPT-3.5 (OpenAI)	Llama 2 (Meta)	BLOOM (BigScience)	GPT-NeoX (EleutherAI)

Foundation models with widely available weights

Bommasani, Rishi, et al. "Issue Brief Considerations for Governing Open Foundation Models | Stanford HAI." Stanford University Human-Centered Artificial Intelligence, 13 Dec. 2023, https://hai.stanford.edu/issue-brief-considerations-overning-open-foundation-models.

While each of the above categories of foundation model offers its own benefits and risks. While fully closed models may be preferrable to protect intellectual property, models that make weights available (or even source code) can provide access to a feedback loop with developers or the ability for users to make improvements.

For purposes of the Executive Order, we urge NTIA to ensure that a "dual-use

[2] Bommasani, Rishi, et al. "Issue Brief Considerations for Governing Open Foundation Models | Stanford HAI." Stanford University Human-Centered Artificial Intelligence, 13 Dec. 2023, https://hai.stanford.edu/issue-brief-considerations-overning-open-foundation-models.

foundation model" is not used synonymously with "open foundation model." The Executive Order provides the following:

> "(k) The term "dual-use foundation model" means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by:
>
> > (i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;
> >
> > (ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or
> >
> > (iii) permitting the evasion of human control or oversight through means of deception or obfuscation.
>
> Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities."

CHI urges NTIA to recognize that not all "open foundation models" reflect the characteristics described in the Executive Order, and to ensure that the scope of foundation models addressed in its report is confined to "dual-use foundation models" as defined in the Executive Order. If the scope of NTIA's report is not carefully restrained to this scope, it may cause definitional confusion in the short term, and later improperly expose foundation models that are not "dual-use foundation models" to future policy or regulatory requirements meant to be applied this category alone.

- ***Address harms that are demonstrable and systemic.*** For purposes of this exercise under the Executive Order, NTIA should focus on high-risk scenarios (e.g., health, safety) for which there is a clear evidence base to address (in other words, policy proposals should not be based on remote edge use cases or hypotheticals).
- ***Adhere to scalable risk-based harm mitigation principles.*** As NTIA explores policy and regulatory options for dual-use foundation models, we strongly urge NTIA to, consistent with the National Institute of Standards and Technology's AI Risk Management Framework, ensure that its proposals are grounded in utilizing risk-based approaches to ensure that levels of review, assurance, and oversight are proportionate to potential harms. Building on this foundation, NTIA should discourage blanket/one-size-fits-all approaches to risk mitigation for dual-use foundation models.

  NTIA's definition of "widely available" should be similarly approached. The wide availability of a model is not necessarily an indicator of the risk(s) it may present. We urge NTIA's definition of "widely available" to reflect the harms presented by the relevant use case(s). Similarly, floating point operations do not necessarily indicate higher risks. Such definitional thresholds should primarily consider the capabilities of the model.

We urge NTIA to maintain a broad perspective in considering risk in this matter. Many other factors than weights can alter the risks and benefits for a foundation model, such as training data, evaluation metrics, and deployment guidelines.

- ***Promote shared responsibility across the AI value chain.*** Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. CHI urges NTIA's report and recommendations to reflect that all stakeholders developing and using AI have a shared responsibility for AI safety, efficacy, and transparency. AI policy frameworks, including those addressing dual-use foundation models, should ensure the appropriate distribution and mitigation of risk and liability (that those in the value chain who have the ability to minimize that risk based on their knowledge and ability to mitigate have appropriate incentives to do so).

  One way that NTIA could support shared responsibility is through proposing the creation of a mechanism for sharing best practices, and for surfacing timely threat indicators, similar to that employed by Information Security and Analysis Centers (ISACs), which foster information sharing across and between the government and private sector while avoiding liability for doing so.[3]

- ***Support, and rely on, international standards for risk management.*** CHI supports reliance on international consensus standards to develop metrics for risk, creating standards for best practices, and/or supporting or restricting the availability of foundation model weights. We believe that NIST's approach taken in its AI Risk Management Framework is optimal. Support for and deference to international standardization would also align NTIA's efforts with the U.S. Government National Standards Strategy for Critical and Emerging Technology.[4]

- ***Coordination/Alignment with Other Leading Federal Efforts.*** Consistent with the intent of the Executive Order, alignment with other key federal efforts occurring in parallel should be prioritized. As a prime example, NTIA's recommendations should be consistent with the output of the U.S. AI Safety Institute.[5]

- ***Support international harmonization.*** We urge NTIA to maintain a priority for supporting risk-based approaches to AI governance in markets abroad and through bilateral and multilateral agreements. 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 NTIA's efforts here, and the Administration's efforts broadly, discourage, or at least have a positive influence on, such mandates in other jurisdictions.

[3] https://www.nationalisacs.org/about-isacs.

[4] https://www.nist.gov/standardsgov/usg-nss.

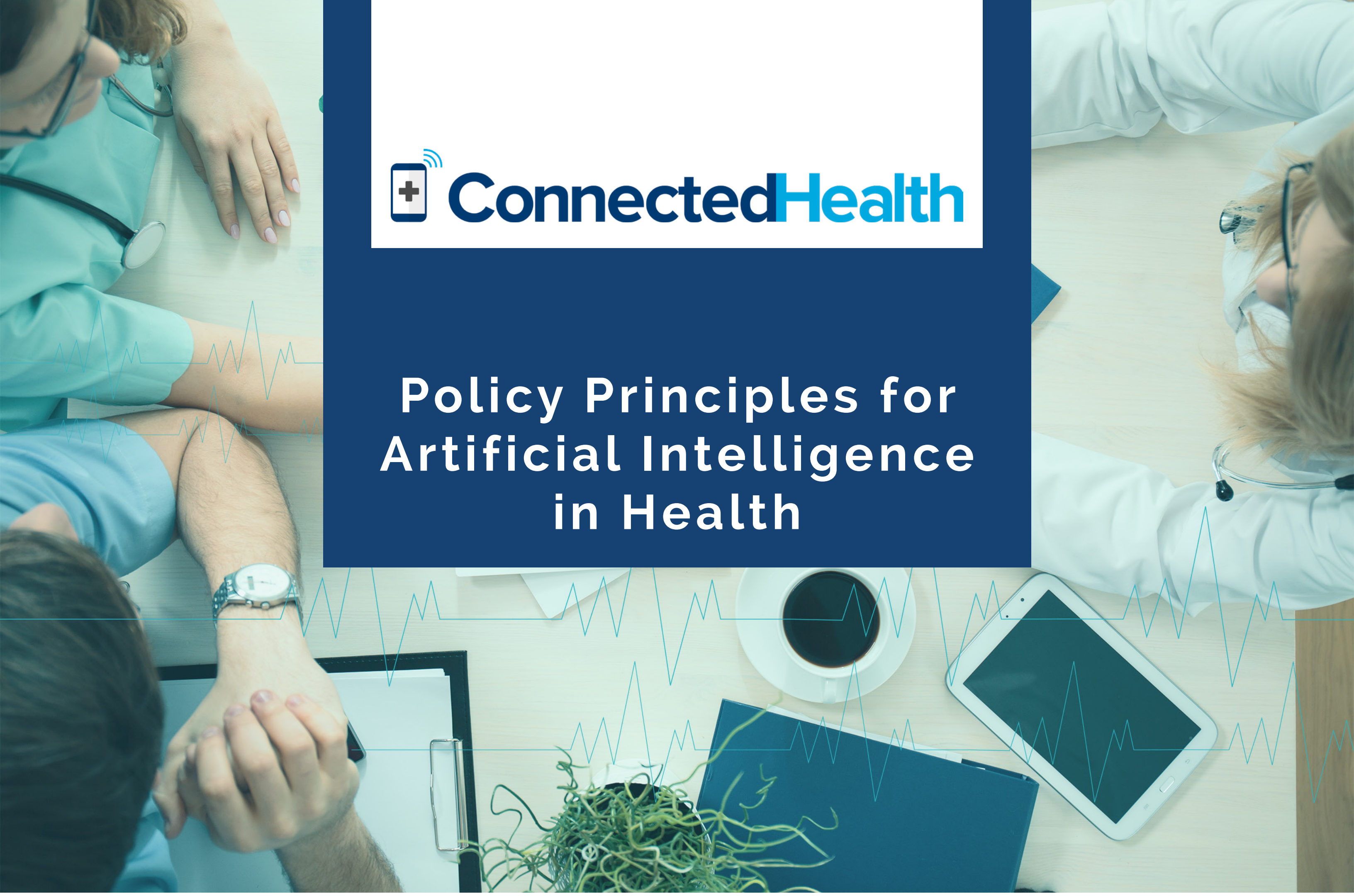
[5] https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute.

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

Sincerely,

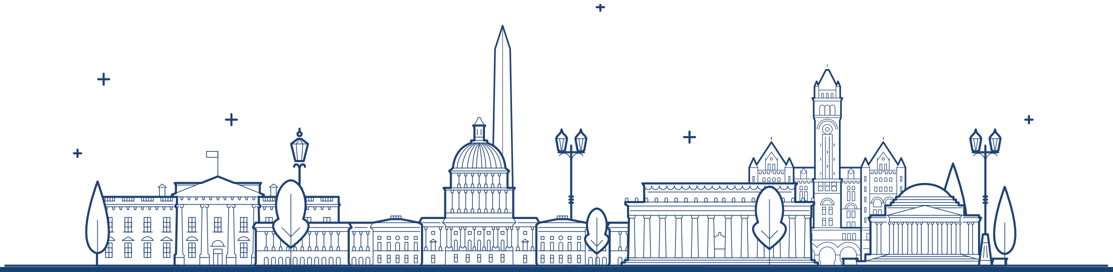
Brian Scarpelli
Executive Director

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



ConnectedHealth

Policy Principles for Artificial Intelligence in Health



Connected Health is an initiative
of ACT | The App Association

1401 K Street NW Suite 501
Washington, DC 20005

☎ 202.331.2130

connectedhi.com

#connectedhealth

/ConnectedHealthInitiative

Policy Principles for AI in Health

Today, there are already many examples of AI systems, powered by streams of data and advanced algorithms, improving healthcare by preventing hospitalizations, reducing complications, decreasing administrative burdens, and improving patient engagement. AI systems offer the promise to rapidly accelerate and scale such results and drive a fundamental transformation of the current disease-based system to one that supports prevention and health maintenance. Nonetheless, AI in healthcare has the potential to raise a variety of unique considerations for U.S. policymakers.

Many organizations are taking steps to proactively address adoption and integration of AI into health care and how it should be approached by clinicians, technologists, patients and consumers, policymakers, and other stakeholders, such as the Partnership for AI, Xavier Health, the American Medical Association, and the Association for the Advancement of Medical Instrumentation and BSI. Building on these important efforts, the Connected Health Initiative's (CHI) Health AI Task Force is taking the next step to address the role of AI in healthcare.

First, AI systems deployed in healthcare must advance the "quadruple aim" by improving population health; improving patient health outcomes and satisfaction; increasing value by lowering overall costs; and improving clinician and healthcare team well-being. Second, AI systems should:

- Enhance access to health care.
- Empower patients and consumers to manage and optimize their health.
- Facilitate and strengthen the relationship and communication that individuals have with their health care team.
- Reduce administrative and cognitive burdens for patients and their health care team.

To guide policymakers, we recommend the following principles to guide action:

- **National Health AI Strategy:** Many of the policy issues raised below involve significant work and changes that will impact a range of stakeholders. The cultural, workforce training and education, data access, and technology-related changes will require strong guidance and coordination. Given the significant role of the government in the regulation, delivery, and payment of healthcare, as well as its role as steward of significant amounts of patient data, a federal healthcare AI strategy incorporating guidance on the issues below will be vital to achieving the promise that AI offers to patients and the healthcare sector. Other countries have begun to take similar steps (e.g., The UK's Initial Code of Conduct for Data Driven Care and Technology) and it is critical that U.S. policymakers collaborate with provider organizations, other civil society organizations, and private sector stakeholders to begin similar work.

- **Research:** Policy frameworks should support and facilitate research and development of AI in healthcare by prioritizing and providing sufficient funding while also ensuring adequate incentives (e.g., streamlined availability of data to developers, tax credits) are in place to encourage private and non-profit sector research. Clinical validation and transparency research should be prioritized and involve collaboration among all affected stakeholders who must responsibly address the ethical, social, economic, and legal implications that may result from AI applications in healthcare. Further, public funding and incentives should be conditioned on promoting the medical commons in order to advance shared knowledge, access, and innovation.

- **Quality Assurance and Oversight:** Policy frameworks should utilize risk-based approaches to ensure that the use of AI in healthcare aligns with recognized standards of safety, efficacy, and equity. Providers, technology developers and vendors, health systems, insurers, and other stakeholders all benefit from understanding the distribution of risk and liability in building, testing, and using healthcare AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, 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. Some recommended guidelines include:

  - Ensuring AI in healthcare is safe, efficacious, and equitable.

  - Ensuring algorithms, datasets, and decisions are auditable and when applied to medical care (such as screening, diagnosis, or treatment) are clinically validated and explainable.

  - AI developers should consistently utilize rigorous procedures and must be able to document their methods and results.

  - Those developing, offering, or testing healthcare AI systems should be required to provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.

  - Adverse events should be timely reported to relevant oversight bodies for appropriate investigation and action.

- **Thoughtful Design:** Policy frameworks should require design of AI systems in health care that are informed by real-world workflow, human-centered design and usability principles, and end-user needs. Also, AI systems should help patients, providers, and other care team members overcome the current fragmentation and dysfunctions of the healthcare system. AI systems solutions should facilitate a transition to changes in care delivery that advance the quadruple aim. The design, development, and success of AI in healthcare should leverage collaboration and dialogue between caregivers, AI technology developers, and other healthcare stakeholders in order to have all perspectives reflected in AI solutions.

- **Access and Affordability:** Policy frameworks should ensure AI systems in health care are accessible and affordable. Significant resources may be required to scale systems in health care and policy-makers must take steps to remedy the uneven distribution of resources and access. There are varied applications of AI systems in health care such as research, health administration and operations, population health, practice delivery improvement, and direct clinical care. Payment and incentive policies must be in place to invest in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining AI system with an eye toward ensuring value. While AI systems should help transition to value-based delivery models by providing essential population health tools and providing enhanced scalability and patient support, in the interim payment policies must incentivize a pathway for the voluntary adoption and integration of AI systems into clinical practice as well as other applications under existing payment models.

- **Ethics:** Given the longstanding, deeply rooted, and well-developed body of medical and biomedical ethics, it will be critical to promote many of the existing and emerging ethical norms of the medical community for broader adherence by technologists, innovators, computer scientists, and those who use such systems. Healthcare AI will only succeed if it is used ethically to protect patients and consumers. Policy frameworks should:Ensuring AI in healthcare is safe, efficacious, and equitable.

    - Ensure that healthcare AI solutions align with all relevant ethical obligations, from design to development to use.

    - Encourage the development of new ethical guidelines to address emerging issues with the use of AI in healthcare, as needed.

    - Ensure consistency with international conventions on human rights.

    - Ensure that AI for health is inclusive such that AI solutions beneficial to patients are developed across socioeconomic, age, gender, geographic origin, and other groupings.

    - Reflect that AI for health tools may reveal extremely sensitive and private information about a patient and ensure that laws protect such information from being used to discriminate against patients.

- **Modernized Privacy and Security Frameworks:** While the types of data items analyzed by AI and other technologies are not new, this analysis provides greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data. This raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development). It also offers the potential for more powerful and granular access controls for patients. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's health information is properly protected, while also allowing the flow of health information. This information is necessary to provide and promote high-quality healthcare and to protect the public's health and well-being. There are specific uses of data that require additional policy safeguards, i.e., genomic information. Given that one individual's DNA includes potentially identifying information about even distant relatives of that individual, a separate and more detailed approach may be necessary for genomic privacy. Further, enhanced protection from discrimination based on pre-existing conditions or genomic information may be needed for patients. Finally, with proper protections in place, policy frameworks should also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

- **Collaboration and Interoperability:** Policy frameworks should enable eased data access and use through creating a culture of cooperation, trust, and openness among policymakers, health AI technology developers and users, and the public.

- **Workforce Issues and AI in Healthcare:** The United States faces significant demands on the healthcare system and safety net programs due to an aging population and a wave of retirements among practicing care workers. And lower birth rates mean that fewer young people are entering the workforce. Successful creation and deployment of AI-enabled technologies which help care providers meet the needs of all patients will be an essential part of addressing this projected shortage of care workers. Policymakers and stakeholders will need to work together to create the appropriate balance between human care and decision-making and augmented capabilities from AI-enabled technologies and tools.

- **Bias:** The bias inherent in all data as well as errors will remain one of the more pressing issues with AI systems that utilize machine learning techniques in particular. In developing and using healthcare AI solutions, these data provenance and bias issues must be addressed. Policy frameworks should:

  - Require the identification, disclosure, and mitigation of bias while encouraging access to databases and promoting inclusion and diversity.

  - Ensure that data bias does not cause harm to patients or consumers.

- **Education:** Policy frameworks should support education for the advancement of AI in healthcare, promote examples that demonstrate the success of AI in healthcare, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.
    - Patients and consumers should be educated as to the use of AI in the care they are receiving.
    - Academic/medical education should include curriculum that will advance health care providers' understanding of and ability to use health AI solutions. Ongoing continuing education should also advance understanding of the safe and effective use of AI in healthcare delivery.

CHI Health AI Roles & Interdependency Framework

ConnectedHealthInitiative

Overview

Artificial Intelligence (AI), especially generative AI, is already a powerful tool in healthcare, offering amazing potential to upgrade patient care by improving care outcomes and patient experiences, reducing healthcare provider burnout by simplifying administrative tasks, and helping to lower the total cost of care. One of the most helpful ways to see the value of AI in healthcare is to view the question through the lens of the “quadruple aim” framework. Built on the Institute for Healthcare Improvement’s “triple aim,” a widely accepted compass to optimize health system performance, the quadruple aim focuses on four key areas where health systems need to be improved, all of which AI is already, and will continue to, provide value across:

- Enhancing population health.
- Improving patient experience, satisfaction, and health outcomes.
- Augmenting clinician and healthcare team experience and satisfaction.
- Lowering overall costs of healthcare.

CHI has explored the ways in which AI is supporting each of the four aims of the quadruple aim in CHI’s paper, Why Does Healthcare Need AI?

But this promising technology is not infallible, and as healthcare organizations seek opportunities to use AI, stakeholders are facing important questions about how various risks or limitations should be handled in the development, distribution, deployment, and end use chain. Many organizations involved in the creation or application of healthcare AI have started to develop Responsible AI programs aimed at managing these risks or limitations within their organization. But as we have learned from other new technologies in the past, stakeholders can benefit from a clear discussion around all the safety measures and other actions that are needed, and how those actions might be applied at different steps from creation to the operation of the tool by the end user. This discussion will help various stakeholders better determine accountability for responsible AI best practices across this chain of stakeholders.

CHI urges all stakeholders in the healthcare ecosystem that are developing and using AI to align with CHI's consensus health AI principles, which recognize the shared responsibility for AI safety, efficacy, and transparency. CHI supports (1) leveraging a risk-based approach to AI harm mitigation where the level of review, assurance, and oversight is proportionate to potential harms and (2) those in the value chain with the ability to minimize risks based on their knowledge and ability, and having appropriate responsibilities and incentives to do so.

Further, managing AI/Machine Learning (ML) risks will be more challenging for small to medium-sized organizations, depending on their capabilities and resources. Building on these general health AI principles, CHI proposes clear definitions of stakeholders across the healthcare AI value chain, from development to distribution, deployment, and end use. Then, CHI suggests roles for supporting safety, ethical use, and fairness for each of these important stakeholder groups that are intended to illuminate the interdependencies between these actors, thus advancing the shared responsibility concept. These roles and interdependencies are also mapped to the Functions defined in the National Institute of Standards and Technology's (NIST's) AI Risk Management Framework (RMF).

1

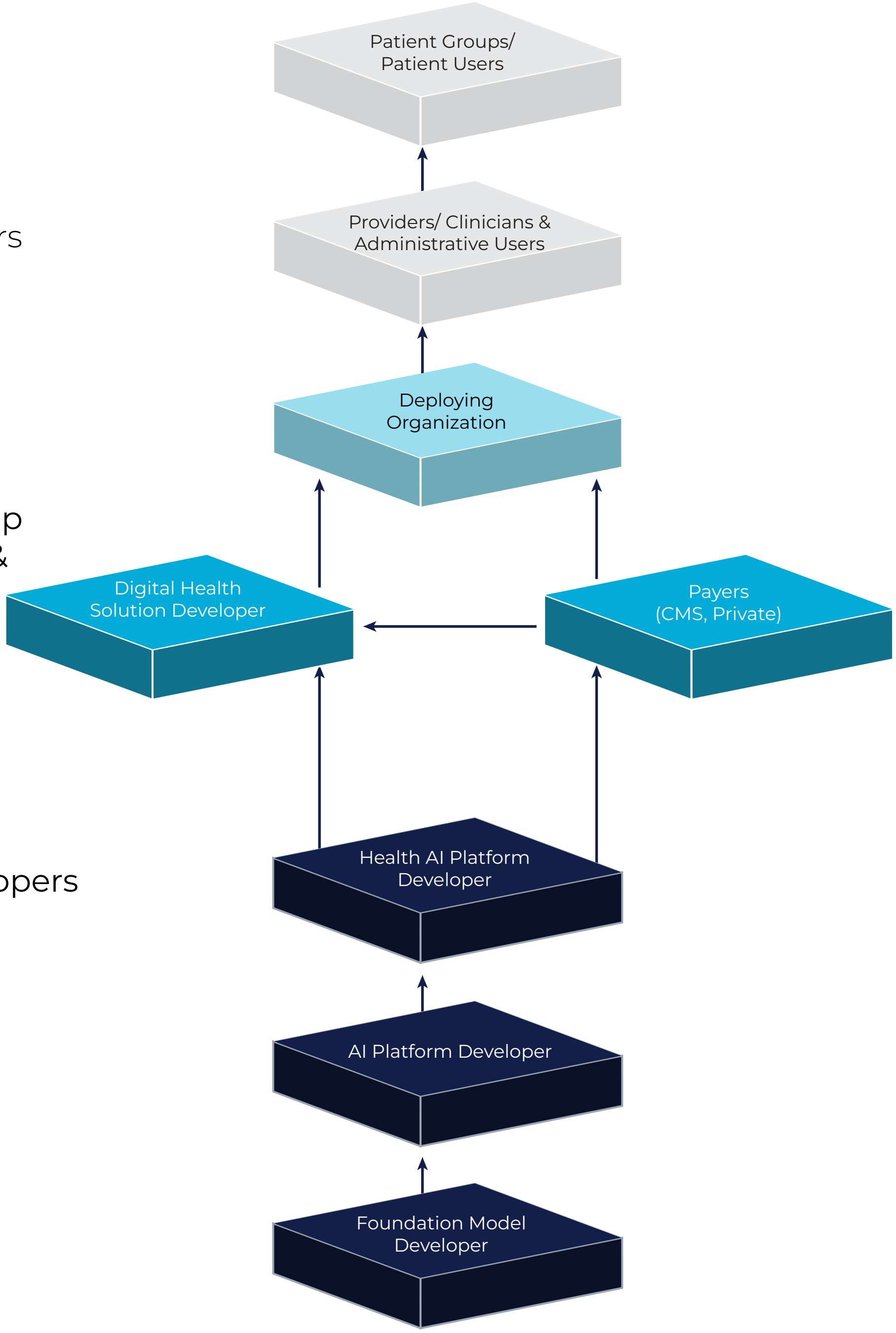
Solution Users

2

Solutions/App Developers & Deployers

3

AI/ML Developers



Patient Groups/ Patient Users

Providers/ Clinicians & Administrative Users

Deploying Organization

Digital Health Solution Developer

Payers (CMS, Private)

Health AI Platform Developer

AI Platform Developer

Foundation Model Developer

Note: Depending on the use case, some of the roles in the healthcare AI/ML value chain may be occupied by the same party; in other scenarios, some roles may not be occupied.

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
AI/ML Developers	Someone who designs, codes, researches, or produces an AI/ML system or platform for internal use or for use by a third party. **See below for defined Subgroups of this Stakeholder Group along with recommendations specific to that Subgroup.**	• Informing deployers and users of data requirements/definitions, intended use cases/populations and applications (e.g., disclosing sufficient detail allowing providers to determine when an AI-enabled tool should reasonably apply to the individual they are treating), including whether the AI/ML tools are intended to augment human work versus automate workflows, and status of/compliance with all applicable legal and regulatory requirements. • Prioritizing safety, efficaciousness, transparency, data privacy and security, and equity from the earliest stages of design, leveraging (and, where appropriate updating) existing medical AI/ML guidelines on research and ethics, leading standards, and other resources as appropriate. • Employing algorithms that produce repeatable results and, when feasible, are auditable, and make decisions that (when applied to medical care) are clinically validated, fostering efficacy through continuous monitoring. • Utilizing risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy and security, avoid harmful outcomes due to bias, etc. • Providing information that enables those further down the value chain can assess the quality, performance, equity, and utility of AI/ML tools. • Aligning with relevant ethical obligations and international conventions on human rights and supporting the development of new ethical guidelines to address emerging issues as needed.	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight

Stakeholder SubGroup	Definition	Roles
Foundation Model Developer	Someone who creates or modifies large and generalizable machine learning models that can be used/adapted for various downstream tasks and applications, such as natural language processing, computer vision, or software development.	***Building on the cross-AI/ML Developer roles noted above:*** • Assessing what bias and safety issues might be present in its Foundation Model, and documenting steps taken to mitigate those issues in its Transparency Documentation (e.g., Transparency Notes, System Cards and product documentation). • Providing clear guidance on (1) how to use and adapt its Foundation Model for various foreseeable downstream tasks and applications, and (2) what limitations or risks may arise from doing so based on challenges discovered during testing and deployment.
AI Platform Developer	Someone who leverages existing foundation models and builds an industry-agnostic platform that enables other developers to access, customize, and deploy these models for various use cases and applications, such as natural language processing, computer vision, and/or software development.	***Building on the cross-AI/ML Developer roles noted above:*** • Testing for, identifying, and mitigating bias and safety issues that may arise from using or modifying existing foundation models for its AI Platform, and documenting these issues and steps taken to address them in its transparency documentation (e.g., transparency notes, system cards and product • documentation).
Health AI Platform Developer	Someone who creates or uses AI-powered platforms that are tailored for the healthcare domain, such as administrative efficiency, diagnostics, therapeutics, or research. These platforms may leverage foundation models (or other types of machine learning models or solutions), such as AI platforms, that are suitable for specific healthcare problems and data sources.	***Building on the cross-AI/ML Developer roles noted above:*** • Meeting specific requirements and standards of the healthcare domain, such as accuracy, efficacy, explainability, and compliance with regulations. • Testing for, identifying, and mitigating any bias and safety issues that may affect the health outcomes of patients or the performance of clinicians using the Health AI Platform, and documenting these issues and the steps it has taken to address them in its transparency documentation (e.g., transparency notes, system cards and product documentation).
Digital Health Solution Developer	Someone who creates complete digital tools and technologies to improve health and healthcare outcomes, such as providing diagnostic and administrative solutions for clinicians, patients, and healthcare organizations. They may build digital health solutions with both health AI platforms, which are specialized for the health care domain, and AI platforms, which are more general and adaptable for various use cases and applications.	***Building on the cross-AI/ML Developer roles noted above:*** • Specifying appropriate uses for its digital health solution to avoid amplifying bias or safety issues that may exist in the underlying foundation models, AI platforms, or health AI platforms. • Designing user interfaces to enable an end user to safely and effectively act upon the output of the tool, such as providing explanations, feedback mechanisms, or human oversight options, providing clear documentation to Deploying Organizations and Users to help them avoid bias and safety issues.

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
Deploying Organization (Healthcare Provider or Payor)	Someone who is a healthcare providers and health care payors that and is deploying solutions built by Digital Health Solution Developers. They may also have their own internal IT staff that use health AI platforms or general AI platforms to develop their own custom digital health solutions.	***Respecting that managing AI/ML risks will be more challenging for small to medium-sized organizations depending on their capabilities and resources:*** • Adopting AI/ML Developer instructions for use, specifying appropriate uses for Users through governance policies to avoid bias and safety issues that may exist in the underlying foundation models, AI platforms, or health AI platforms. • Developing and leveraging digital health solutions that augment efficiencies in coverage and payment automation, facilitate administrative simplification/reduce workflow burdens, and are fit for purpose. • Setting organization policy/designing workflows to reduce the likelihood that a User will act upon the output of the tool in a way that would cause fairness/bias or safety issues (tailored explanations, feedback mechanisms, and/or human oversight options). • Developing and organizational guidance on how the digital health solution should and should not be used. • Creating risk-based, tailored communications and engagement plans to enable easily understood explains to patients about how the digital health solution was developed, its performance and maintenance, and how it aligns with the latest best practices and regulatory requirements.	Assessment; Procurement; Governance and Oversight
Provider/Clinician Users and Administrative Users	Someone who directly interacts with or benefits from the digital health solutions that are built by Digital Health Solution Developers or by the internal IT staff of the Deploying Organization. They may include clinicians, such as doctors, nurses, or pharmacists, and administrative staff, such as billing, claims, or customer service personnel, in the provider and payor organizations.	***Respecting that managing AI/ML risks will be more challenging for small to medium-sized organizations depending on their capabilities and resources:*** • Taking required training and incorporating employer guidance about use of AI/ML digital health solutions. • Documenting (through automated processes or otherwise) whether AI is being used in medical records and report any issues or feedback to the developer, such as errors, vulnerabilities, biases, or harms (where AI/ML's use is known by the User). • Ensuring there is appropriate clinician review and review of the output or recommendations from each digital health solution prior to acting on it (where AI/ML's use is known by the User).	AI Deployment; Operation and Monitoring; Domain Expert; AI Impact Assessment; Procurement; Governance and Oversight

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
Payer Users (Centers for Medicare and Medicaid Services [CMS], State Medicaid, Private)	Someone that pays for the cost of healthcare services administered by a healthcare provider.	• Leveraging AI/ML systems that improve efficiencies in coverage and payment automation, facilitate administrative simplification, and reduce provider workflow burdens. • Aligning with medical AI/ML definitions, present-day and future AI/ML solutions, the future of AI/ML medical coding changes and trends. • Developing support mechanisms for the use of AI/ML by providers based on clinical validation, aligning with clinical decision-making processes familiar to providers, and high-quality clinical evidence. • Assuring that AI/ML systems allow for the individualized assessment of specific medical and social circumstances and provider flexibility to override automated decisions, ensuring that use of AI/ML does not improperly reduce or withhold care, or overrides the provider's clinical judgement. • Disclosing information about training and reference data to demonstrate that AI/ML systems do not create or exacerbate inequities and that protections are in place to mitigate bias. • Developing and proliferating easy to understand resources for beneficiaries and their providers that capture how and when AI/ML is being used, what information it is leveraging, and what it means to patients.	AI Deployment; Operation and Monitoring; Domain Expert; AI Impact Assessment; Procurement; Governance and Oversight
Patient Groups/ Patient Users	Someone who uses digital tools and technologies that are built by Digital Health Solution Developers or experiences their use in treatment.	• Developing and proliferating easy to understand resources that capture how AI/ML is being used and what it means to patients/patient groups, including explanations on the purpose and limitations of the digital health solutions that they use or benefit from (e.g., diagnostic, therapeutic, administrative). • Raising awareness of patients' rights and choices when using digital health solutions, such as consent, access, correction, or deletion of their personal data.	Human Factors
Standard-Setting Organizations	An organization whose primary function is developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise contributing to the usefulness of technical standards to those who employ them.	• Developing and promoting adoption of international voluntary/non-regulatory consensus standardized approaches and resources to steward a shared responsibility approach to AI.	Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
Certification Bodies & Test Beds	A certification body is a third-party organization that assures the conformity of a product, process or service to specified requirements. A test bed is a platform for conducting rigorous, transparent, and replicable testing of scientific theories, computing tools, and new technologies to a standard.	• Creating and making available transparent and reliable processes for the assurance of conformity to voluntary AI standards. • Creating and making available voluntary sandbox environments to help evaluate the usability and performance of AI/ML-based high-performance computing applications to advance the understanding of how reliable and efficacious AI, and to provide an appropriate assurance of reliability and efficacy.	Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Accrediting and Licensing Bodies, and Medical Specialty Societies and Boards	Accrediting and licensing bodies are governing authorities that establish the suitability of any participating certification body. Notably, state-level board serve this purpose for physicians, nurses, and other clinicians to standards set by each state. Medical specialty societies are organizations for physicians, research and clinical scientists who are actively involved in the study of a particular specialty.	• Based on clinical needs and expertise, developing and setting the medical standard of care and ethical guidelines to address emerging issues with the use of AI/ML in healthcare needed to advance the quadruple aim. • Identifying the most appropriate uses of AI-enabled technologies and developing and disseminating guidance and education on the responsible deployment of AI/ML in healthcare, both generally and for specialty-specific uses.	Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Academic and Medical Education Institutions	Tertiary educational institutions, professional schools, or forms a part of such institutions, that teach medicine and awards a professional degree for physicians or other clinicians.	• Developing and teaching curriculum that will advance understanding of and ability to use healthcare AI/ML solutions responsibly, which should be assisted by inclusion of non-clinicians such as data scientists and engineers as instructors. • Developing curriculum to advance the understanding of data science research to help inform ethical bodies (e.g., Institutional Review Boards that are reviewing protocols of clinical trials of AI/ML-enabled medical devices).	Human Factors; Domain Expert; AI Impact Assessment