Submitted to: HELPGOP_AIComments@help.senate.gov

September 21, 2023

Senator Bill Cassidy, M.D.
Ranking Member
U.S. Senate Committee on Health, Education, Labor and Pensions
Washington DC 20510-6300

RE: Exploring Congress’ Framework for the Future of AI

Dear Senator Cassidy:


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 health information 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.

The Confidentiality Coalition applauds your office for issuing the White Paper, which could not be more timely. We agree strongly with its premise that artificial intelligence (AI) is a transformational tool, the use of which holds enormous promise, but also presents significant risks. We support the efforts by your office and others in Congress to lay the regulatory framework to address the risks presented by the use of AI, while nurturing its promise.
We attach for your consideration the Confidentiality Coalition’s recently developed “Principles for the Responsible Development and Use of Artificial Intelligence in Health Care.” These principles touch on many of the issues raised in the White Paper, and reflect the position of the Coalition on these issues.

In addition, we would like to comment specifically on the section of the White Paper entitled “Safeguarding Patient Privacy Throughout the Health Care Lifecycle.” In that section, the White Paper notes that large data sets are a prerequisite for the development of AI tools, and raises questions regarding the protections to which this data is entitled, especially as some of it may fall outside the scope of HIPAA. We believe strongly that all personally identifiable health data should be subject to robust protections, whether that data falls within HIPAA or outside of HIPAA. For personal health information that falls outside of HIPAA, we have long supported the passage of national privacy legislation that aligns with HIPAA and provides commensurate protections. We elaborate on this important topic in response to the letter issued by your office on September 7, 2023 seeking feedback on various health privacy issues for consideration by the Senate Committee on Health, Education, Labor and Pensions (“Health Privacy RFI”).

The White Paper also points out that while AI can enhance privacy by aggregating and anonymizing data, it can also be used to re-identify previously de-identified health information. We agree with this concern. Therefore, and as discussed further in our response to the Health Privacy RFI, we recommend that the HIPAA Privacy Rule be revised to require that, as a condition for treating disclosed data as deidentified, the recipient of such data must contractually agree not to attempt to re-identify the data. This same requirement should also be incorporated into the national privacy legislation for personal health information that falls outside of HIPAA so that its deidentification standard aligns with that of HIPAA.

Thank you for your consideration of our comments. Please do not hesitate to contact me at tgrande@hlc.org or 202-306-3538 if you have any questions.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and Executive VP, Policy, Healthcare Leadership Council
Principles for the Responsible Development and Use of Artificial Intelligence in Health Care

INTRODUCTION

Perhaps no area of human endeavor stands to benefit more from the transformative power of artificial intelligence (AI)1 than health care, whether in aiding in diagnosing diseases, assisting intricate procedures, or identifying individuals who could benefit from additional health services. However, with these new capabilities come risks, and the potential for misuse and unintentional consequences. Guardrails are essential to protect against these risks while at the same time encouraging ongoing technological development. Regulators should collaborate with all stakeholders to strike the right balance between protecting individual rights and liberties, ensuring improved patient outcomes, and encouraging competition and ongoing innovation so that the full promise of AI in the health care field may be realized.

With this context in mind, we have developed the below principles to guide regulators as they consider a regulatory framework to govern the use of AI in the health care field.

PRINCIPLES

Benefits and Innovation. AI tools are already utilized in the health care industry in multiple ways to benefit society. These include tools to identify areas for intervention so as to improve health and wellness, help diagnose diseases earlier and more accurately, to provide new and personalized treatments, and automate and streamline certain tasks while retaining human oversight where appropriate, creating clinical and operational efficiencies that lower costs, reduce human error, and ultimately increase access to care and improve health outcomes. [For example, the use of AI is enabling review and translation of mammograms thirty times faster with 99% accuracy, reducing the need for unnecessary biopsies.]2 These benefits accrue with AI being used as an enhancement to existing clinician reviews, not as a substitute for them. The positive benefits represent

---

1 The term “artificial intelligence” or “AI” is defined in different ways for different purposes. The National Institute of Science and Technology (NIST) Computer Security Resource Center provides the below two definitions:

“(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.
(2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.”


only the first step of the varied ways in which AI could be deployed in the future to revolutionize health care and help individuals lead longer and healthier lives. It is only through ongoing innovation that this tremendous potential will come to fruition. It is therefore essential that regulators, stakeholders, and AI experts work together to ensure any regulatory framework takes a risk-based, patient centered approach that supports and nurtures developing AI technology to improve health care and patient outcomes.

**Risk-based Approach.** Regulatory agencies and organizations using AI applications should take a risk-based approach to the regulation and oversight of AI applications, taking into account their potential impact and possible harms. Organizations should perform risk assessments that align with, or extend beyond, consensus-based risk management frameworks such as the AI Risk Management Framework (AI RMF) developed by the National Institute of Standards and Technology (NIST). An AI Risk Assessment should identify potential risks that the AI tool could introduce, potential mitigation strategies, detailed explanations of recommended uses for the tool, and risks that could arise should the tool be used inappropriately. By focusing on a risk-based approach and regulating accordingly, regulators will allow developers and users to allocate resources appropriately and proportionate to the potential harm and nuances of their specific AI use case. Rather than having to perform risk assessments of the same type and cadence for every AI application, organizations should be able to tailor these assessments based on the nature of the application, its intended use and context, potential harms, and changes in the internal and external environment. This approach would encourage healthcare applications with the highest risk have the highest guardrails, such as requiring more frequent review or human intervention. Finally, regulators should avoid imposing duplicative compliance requirements, and consideration should be given to organizations that follow a framework such as the NIST AI RMF in the imposition of penalties.

**Federal Standards.** Any regulatory framework(s) for AI applications should be developed and applied at the federal level. A single national standard that preempts state laws in this area will avoid conflicting requirements and facilitate compliance without unduly restricting innovation.

**Privacy and Security.** Personal information used in AI should be subject to robust privacy and security protections at the federal level. This includes adhering to existing health data privacy and security protections in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for protected health information, equivalent protections for non-HIPAA health data, including that the appropriate legal authority exists for the processing of non-HIPAA personal information, including in relation to the datasets used to train, validate, and test AI models. The principles of privacy by design should be integrated into AI tools from the start. This includes, but should not be limited to, data minimization, and use limitations. Individuals should have the right to be informed about the collection and use of their personal information, and the right to access, correct and, if feasible, delete their personal information. Congress should establish a single national standard for the use of personal information not already subject to HIPAA that includes standards for the use of that information in AI applications by entities not regulated by HIPAA. Security safeguards, which may be
based on guidelines such as those provided in the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Risk Management Framework, should protect against data breaches, data poisoning, exfiltration of models or training data and other threats that could expose the data used or alter the use, behavior, or performance of an AI application.

**Harmonization.** Federal agencies such as the Office for Civil Rights (OCR), Food and Drug Administration (FDA), the U.S. Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC), among others, should collaborate to align the federal government’s approach to the regulation of AI. OCR and the FDA have worked together in the past to align (e.g., on the regulation of medical devices) as do OCR and the FTC on health information privacy. This will allow organizations subject to the authority of different federal agencies to align their approach to implementing AI applications across the enterprise, avoiding confusion, and leading to greater compliance.

While each agency may approach the technology from a different regulatory angle, whether safety, privacy, consumer protection or otherwise, they should be able to take a patient-centered approach to reach sufficient alignment so that compliance with one framework will not result in violation of, or inability to comply with, another. Failure to harmonize regulatory frameworks will not only create interpretation and compliance burdens but will slow AI development and stifle innovation by creating a regulatory patchwork that fails to account for how health care is delivered. Additionally, conflicts between federal agencies’ regulation of AI will hamper U.S. efforts to lead globally in the regulation of AI. Other countries want to adopt a framework for the regulation of AI that harmonizes across business sectors and regulatory areas, rather than having to deal with discordant or conflicting requirements.

**Accountability.** Health organizations that use AI should determine and establish a risk-based structure of accountability that extends across its partnerships to ensure that their AI uses cases are deployed in a responsible, fair, and consistent manner. This includes developing, implementing, and documenting principles, policies, procedures, as well as an internal collaborative governance structure and controls to oversee the development and use of AI applications. These controls should include quality control parameters for the data used as well as criteria against which the performance of the AI applications is monitored, evaluated, and re-evaluated, as needed, at regular intervals throughout the lifecycle. Accountability should extend to the highest levels of management and should include key elements such as risk-assessment, training, monitoring and internal sanctions.

**Transparency.** Transparency is essential to build trust in AI technology. Where appropriate, organizations should disclose when they are using AI tools, especially when these tools are used to make decisions about individuals. Organizations should not be required to reveal the inner workings of their AI systems to the public or regulatory agencies, nor is there any benefit in doing so. The detailed disclosure of either data inputs or algorithmic processes would not be meaningful to patients, providers, or payers, would force AI developers to disclose their intellectual property or proprietary technology, could create AI vulnerability risks, and may limit innovators
willingness to work with the already highly regulated healthcare industry on meaningful AI applications.

**Explainability.** Developers of AI applications for use in health care must be able explain to users how a decision is made by a high-impact AI application in a way that is sufficiently understandable to those users. Users should be able to gauge the context in which an algorithm operates and understand the implications of the outcomes. Users should in turn be able to explain the role of algorithms to individuals affected by AI-assisted decisions. Explanations should be meaningful and useful, tailored to the audience and calibrated to the level of risk.

**Addressing Adverse Bias and Discrimination.** AI applications in health care present the risk of bias as the underlying, especially historical, data sets may lack representative or accurate data. Access to high quality data sets that are as complete as possible, including sensitive personal information (e.g., data on race, ethnicity, gender, etc.), is ideal, but not always possible. Organizations should then take comprehensive steps to identify and mitigate potential sources of harmful bias across the lifecycle of their model development, and where reasonable and appropriate for specific models, align with industry-developed standards. It is important that this not be done by excluding sensitive personal data or data of vulnerable groups from AI training data so that any bias may be detected and remedied, and all patients may benefit from the advances in health care brought about by AI.