HIMSS™

September 22, 2023

The Honorable Bill Cassidy
Ranking Member
Committee on Health, Education, Labor and Pensions
United States Senate
Washington, DC 20510

Submitted via email to: HELPGOP_AIComments@help.senate.gov

Dear Ranking Member Cassidy:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments in response to the white paper and RFI entitled, "Exploring Congress Framework for the Future of AI: The Oversight and Legislative Role of Congress over the Integration of Artificial Intelligence in Health, Education, and Labor." We appreciate this opportunity to utilize our members' expertise in offering feedback on this discussion paper, with the goal of leveraging the iterative improvement power of AI/ML software to help realize the full health potential of every person while ensuring that patient safety is maintained. We look forward to continued dialogue with the Committee to continue the discussion on these topics.

HIMSS is a global advisor, thought leader, and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology driven by health equity. Through our innovation engine, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 125,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations. Our global headquarters is in Rotterdam, The Netherlands and our Americas headquarters is in Chicago, Illinois.

Generating trust and transparency in artificial intelligence (AI) and machine learning (ML) algorithms is core to fostering the engagement of the healthcare community, including healthcare consumers, in the use of AI/ML. Congress and federal agencies should collaborate with the AI/ML community, end users, and patients to create and educate on standardized definitions of AI and ML to ensure consistent understanding among wide-ranging applications in healthcare. As part of a framework for AI/ML oversight, legislators and regulators should ensure:

- Plain language descriptions of the logic, decision making, rules, and exceptions used by an algorithm is more easily understood by an intended user and the public.
- Access to high-quality, up-to-date, and unbiased training datasets are facilitated to bolster the responsible innovation of AI/ML technologies. Models

should be vigorously validated and revalidated on an ongoing basis with up-to-date but fully de-identified real-world data. This should be a best practice for the sector.

- o Senator Blumenthal's bipartisan framework incorporates a licensing regime administered by a separate oversight body.
- o Industry consensus and policy is needed to set appropriate requirements for validation.

- Robust research is supported to develop high-quality datasets and environments for a wide variety of AI/ML applications and to enable responsible access to good datasets and testing and training resources.
- Open-source software libraries and toolkits are leveraged to help foster AI innovation.
- Data governance and stewardship models are developed with access for secondary use of the data for healthcare research in mind. Notwithstanding this, rigorous de-identification of the data should be performed, in line with HIPAA requirements.
- That to the best extent practicable, AI/ML platforms are devoid of bias. Such biases can be introduced not only in algorithms, but also in the training data and oversight of AI/ML platforms (whether in the development or implementation phase).
- Policymakers consistently collaborate with public and private sector organizations, including non-profit entities, to ensure there is consensus around reasonable best practices and standards for the responsible innovation, use, and deployment of AI/ML technologies.

Supporting Medical Innovation and FDA Oversight

The FDA has an important role for regulating AI/ML for health and safety. In the public discourse regarding AI/ML oversight, the term "artificial intelligence" serves to mean something different to a variety of stakeholders in the health information and technology community. It is important to acknowledge these areas where terminology and definitions may differ among stakeholders. There are two distinct groups of AI – locked AI that incorporates the same model to calculate recommendations, and adaptive AI that learns as different data is fed into the model. There are also different data sets – the "training data set", which is the data set utilized to validate the model and initiate its operations, and the "production data set, which is the end-user data that is fed into the models in the setting of care. Finally, at a high level, there are AI/MLs that create recommendations for qualified intermediaries, and then there are automated AI/MLs.

HIMSS recommends FDA provide more distinct examples of both locked and adaptive AI/ML to improve clarity on what mitigation requirements are in place for manufacturers in terms of any proposed regulatory framework. Furthermore, FDA and other regulatory bodies need to promote the consistent revalidation of AI/ML models as an industry-wide best practice, as many models, as they are fed data, can "drift" away from the comparable and consistent calculations created during the manufacturer validation process. Finally, any risk-based framework for determining if an AI/ML model needs post-market surveillance, or both post-market surveillance and pre-market approval should also factor in whether the intended use for the model requires a qualified intermediary to turn the model recommendations into action.

FDA has an important role to play for regulating AI/ML for health and safety and has already started taking some of these actions. For example, to reinforce that AI/ML models need to be validated and revalidated on an ongoing basis with real-world data from the end user that is using the data, FDA has started communicating with the healthcare community to start sharing performance data on AI/ML models over time.

There is still an unproven assumption that AI/ML innovators can create AI/ML that is always controllable or changes in a predictable fashion, however this has a greater chance of happening if there is inconsistent oversight of AI/ML innovators. In addition, it's uncertain whether the trigger that causes the software to act is always realistic or reliable. Policies need to enforce a better understanding of the types of resource information and best practices for revalidation that commercial developers of AI models should share with the end-users of their solutions, as well as needed training and technical support to support and revalidate the models. HIMSS believes that the industry should develop consensus-based based practices, standards, and guidelines as AI/ML technology evolves.

The community also feels we need more clarification for when an AI application falls under medical device purview. AI tools deployed are once, and self-learning/self-correcting AI changes output based on new data that is consumed. As part of that oversight, FDA needs to clarify if there is a difference in the regulatory framework for AI/ML models driving automated processes, versus AI/ML models that produce recommendations that can only become action through the intervention of a competent professional intermediary.

HIMSS also recommends that the FDA add expertise to thoughtfully review how to validate and re-validate self-learning models.

Finally, there are significant consequences for not acting thoughtfully and quickly to lead the development to set global standards for the oversight of AI/ML. The longer the United States waits, the more our leadership is ceded to other governments (and potential bad actors.) The European Union AI Act has created a risk-based regulatory framework for AI. If passed as expected in the final quarter of 2023, all entities making AI-based solutions available in EU markets will have to follow the regulatory framework. AI systems that are developed and used outside of the EU, if the output of those systems is intended for use in the EU, will be subject to this framework as well. As a result, the act's extraterritorial reach is potentially expansive. Many providers and users based outside the EU, including those in the United States, will find their system outputs being used within the EU, and such entities will fall under the purview of the act. As Congress assesses FDA and other regulatory agencies roles in regulating AI/ML, HIMSS strongly recommends Congress and federal agencies consider aligning with the AI Act where appropriate and encourage European Union leaders to modify the regulatory framework to address potential problematic regulatory barriers.

Medical Ethics and Protecting Patients

As noted above, it is critical for Congress to legislate in a manner that delineates between fixed and learning AI/ML models, the types of data that feed the models, and whether or not the intended use of a model requires a competent professional intermediary in the decision-making loop. Underneath that framework, establishing the

consistent re-validation of AI/ML models as new data populates the algorithm as an industry best practice is critical.

Unfortunately, there is little consensus within the industry to identify the best framework for creating oversight for this process, and questions regarding potential liability persist. HIMSS strongly encourages Congress to convene a technical expert panel of stakeholders from manufacturers, end users, patient safety experts, and other stakeholders that would have material involvement in deployment of these models to develop recommendations for lawfully required standards for revalidation. Data collected as part of the FDA AI/ML precertification program should be incorporated into their findings.

Regarding the Committee's question on the current HIPAA framework being equipped to safeguard patient privacy in regard to AI in clinical settings, HIMSS has long advocated for Congress to adopt a unified, global approach to health cybersecurity and information privacy built upon consensus-based, and industry-led standards, guidelines, best practices, methodologies, procedures, and processes with use cases and implementation guidance that is scalable for a wide range of healthcare organizations and inclusive of all provider levels. While clinical care settings and breaches that happen within those care settings are covered by HIPAA breach notification requirements, data feeding into AI/ML models can often migrate to other settings that are potentially not covered by HIPAA.

In the summer of 2023, the Federal Trade Commission proposed modifying the breach notification responsibilities of non-HIPAA covered entities, including app developers that may encounter identifiable health information. HIMSS strongly supported the FTC proposal to ensure that all entities outside of HIPAA's purview collecting identifiable health information are covered by federal oversight and have responsibilities to protect health information, update impacted parties when a breach occurs and take appropriate action to mitigate the impact of the breach. This is critical to ensure a seamless, secure, ubiquitous and nationwide exchange of data, a careful balance must be made between the need to keep information private and secure while also remaining shareable across various environments to help ensure patient health and care is not impeded. Notwithstanding this, HIMSS advocates that Congress develop voluntary, consensus-based, and industry-led standards, guidelines, best practices, methodologies, procedures, and processes with use cases and implementation guidance. Especially in a field that is quickly growing and yet is relatively new, we strongly recommend this voluntary, but industry-focused, approach.

However, HIMSS' goal is for all identifiable patient information to be protected with the same protections and breach responsibilities. HIMSS continues to call upon Congress to construct appropriate legislative language formulating functional definitions that ensure all platforms that handle, collect, and share electronic health information have the responsibility to protect consumer health information, regardless of whether the actor is covered by HIPAA or FTC.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact David Gray, Director of Government Relations, at DGray@HIMSS.org with questions or to request more information. Thank you for your consideration.