



1600 20th Street, NW • Washington, D.C. 20009 • 202/588-1000 • www.citizen.org

Regulating AI in Health Care

Though algorithms have been used widely within health care for years, the rise of AI has generated increased concern and awareness of potential benefits and harms. Initial concerns around the use of AI in health care, including the [automation of denials](#) in Medicare Advantage, AI for [diagnosis](#), using potentially vulnerable programs for [doctor's notes](#), and [robot-assisted](#) surgeries, represent the tip of the iceberg when it comes to possible uses. While the potential for improvements in the health care system through the use of new technologies is great, it is most important that patients are protected as these technologies are introduced.

The White House released its [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#), which included a number of health care specific charges, many for HHS specifically, that serve to create an important foundation for fostering and overseeing the use of AI in health care, public health, and human services.

However, without further action by states, the federal government and Congress to create meaningful guardrails to protect patients, providers, and the public, AI in health care may become a source of unwarranted profit for unscrupulous companies and a threat to patients just trying to get the care they need. Agencies and Congress must ensure sufficient protections for patients and help providers and institutions mitigate the risks of AI in health care.

Protecting Patients

The use of AI in health care has the potential to change the way care is delivered when it comes to screening, diagnosis, and treatment across numerous care settings. However, without adequate oversight and accountability, patients risk confusion and harm.

Policy recommendations:

- **Require Disclosure and Transparency When AI is Used:** If AI is being used in a health care process, it should be disclosed to patients and providers in a clear and understandable way.
- **Enact Guardrails to Protect Patients:** Whenever an AI system is used to make health decisions that may have an impact on a patient, the patient and their physician should have the right to an understandable explanation of the decision, the right to request human review, and the right to have the decision appealed to a human.

- **Guarantee Privacy Protections:** Companies and regulators must maintain patient privacy requirements around the development, testing, and ongoing evaluation of AI in health care.
- **Prevent Discrimination and Reduce Bias:** AI databases being used for training generative AI systems must be reflective of the patient population that it is intended to serve. AI algorithms should be focused on improving equity instead of just reproducing current patterns and biases in our health care system. Because AI systems are susceptible to [bias](#) from the data they are being trained on, it is important that federal agencies exercise care in their use of training data and continuously monitor AI systems.
- **Ensure Consumer Protections:** Patients should not have to sign away their private right of action, individually or on a class basis, to seek compensation for harms caused or confounded by AI in health care.
- **Implement Data Minimization:** Regulators should require AI tools to collect only task-necessary data and delete it promptly after use.
- **Improve Consistency of AI Use:** HHS and CMS should develop meaningful use standards for AI in Medicare, Medicaid, and other health care programs to protect patients, help providers and institutions to better use AI, and improve the opportunities for oversight and accountability. This must also include technical assistance, particularly for low-resource settings, to ensure that uptake of AI in health care is as equitable as possible.
- **Ensure Accountability for Bad Actors:** There must be clear procedures for the suspension and debarment of companies found violating an agency's rules and requirements on AI. Companies that are found to have knowingly concealed harms or significant potential harms should face felony criminal prosecution, for the company as well as top-level responsible corporate offices.
- **Require Special Scrutiny for Health-Related Generative AI Tools:** Either all consumer health-related AI tools and apps should be designated presumptively as Class III devices requiring pre-market FDA approval for safety and efficacy, including compliance with the Department of Health and Human Services [standards](#) for trustworthy AI, or a new and more stringent pre-market approval system should be created. Generative AI consumer health tools should be required to be tested and approved before being deployed.
- **Special Attention for AI Therapeutic Tools:** Chatbots and generative AI tools that claim or imply therapeutic benefit require special attention. Users must always understand that they are engaging with an AI, not a person. General purpose AI tools must state clearly that they do not provide therapy. Privacy protections and FDA approval standards should be especially stringent for therapeutic AI tools.
- **No Immunity Provisions for use of AI:** Health care providers must be liable for harms caused by their use of and reliance on AI tools, with no special "AI immunity." Similarly, companies that provide AI health care tools must also be held liable. The allocation of liability between providers and AI companies should be worked out on a case by case basis, but never at the expense of injured patients.

Ensuring Access and Public Health-Focused Innovation

AI and AI-enabled tools should be used to support R&D for medicines to meet public health needs, promote open science, and ensure accessibility.

Policy recommendations:

- **Prioritize Public Health:** AI and AI-enabled tools used in drug development must help meet public health needs, including in rare and traditionally neglected disease areas, rather than only benefit pharmaceutical company profits and disease areas with the most available data.
- **Promote Open Science:** Exclusive control of AI algorithms should be avoided to maximize its utility in promoting research, especially when developed with public support.
- **Promote Access to Publicly-Supported Therapies:** Medicines developed with AI and AI-enabled tools with federal support should be made available to the public on reasonable terms, including fair prices that reflect the public's investment.