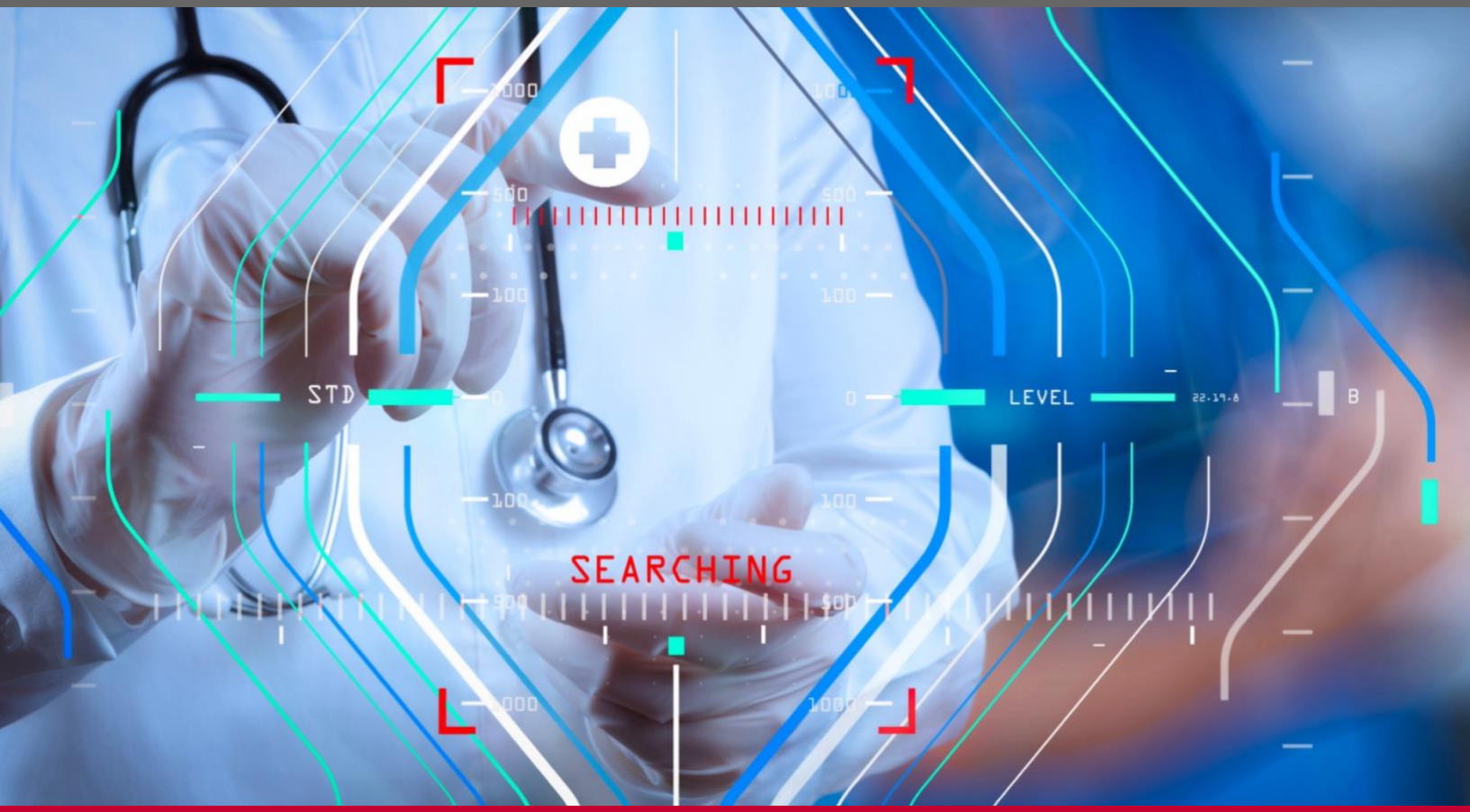
A Healthcare World Reimagined

How Big Government Threatens Healthcare AI and What to Do About It



By Rea S. Hederman Jr. and Logan Kolas

THE BUCKEYE INSTITUTE

A Healthcare World Reimagined

How Big Government Threatens Healthcare AI and What to Do About It

By Rea S. Hederman Jr. and Logan Kolas

April 1, 2024

THE BUCKEYE INSTITUTE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Artificial intelligence—commonly called AI—is a burgeoning technological tool with scores of potential applications that researchers and developers have only begun to unlock. But the new technology, even in its fledgling stage, already shows great promise for improving healthcare services for physicians, hospital systems, and their patients. Demand for healthcare continues to rise as the American population continues to age. And the supply of doctors, nurses, healthcare technicians and medical support has not kept pace with demand. AI shows the potential to be of help. It can sort, manage, and even analyze vast sums of data far faster and more accurately than humans. Its hi-powered data analysis can help doctors make better diagnoses and prognoses for patients. And by reducing the time needed for complex analytics and prognostications, AI frees doctors and nurses to spend more time consulting with patients and improving their medical visits.

To achieve these advantages, however, AI developers require access to large, accurate, and highly sensitive pools of patient data. That data must be safeguarded with security protocols in place to ensure that it is shared and stored safely. As AI improves, so do the understandable calls for enhanced data privacy. And how those calls are answered proves increasingly important.

Unfortunately, federal and state policymakers have signaled their interest in pursuing heavy-handed regulatory rules that risk short-circuiting many of the improvements that AI has to offer—particularly in healthcare. President Biden's Executive Order in late 2023 directs practically every federal agency to explore drafting new rules and regulations for AI technology. At least one federal agency is already collaborating with universities and large technology companies to create new requirements that will likely disadvantage smaller firms and reduce sector competition. Regulatory moats are rarely a good idea. And state lawmakers are actively drafting their own inconsistent patchwork of AI-stunting legislation that will favor "Big Tech" by making it more expensive, confusing, and legally treacherous for smaller, newer developers to test and bring their products to market. This paper examines several of the troubling regulatory efforts already underway in the AI and AI-healthcare related fields and suggests alternative approaches that will better support this promising new technology.

INTRODUCTION

The advent of improved AI can help address persistent challenges facing America's healthcare. The U.S. population has grown steadily older, with the median age rising from 30 years old in 1980 to 38.9 years old in 2022. As the population's median age rises so does the country's demand for healthcare services and providers.[1] And supply has not kept pace with demand, creating healthcare shortages[2] in many areas throughout the country that contribute to high medical costs that many Americans cannot afford. U.S. healthcare costs now account for between 17 and 18 percent of the nation's gross domestic product (GDP), and federal regulators expect those costs and percentages to continue to rise.[3] In addition to the high price of bringing new medical devices and treatments to market, American healthcare also labors under an expensive administrative strain. Administrative costs—those not related to medical treatment—can account for up to one-third of healthcare spending due to the complexity of and challenges associated with collecting and reporting data from patients, providers, insurers, and government overseers.[4] And finally, studies show that missed diagnoses and medical errors raise healthcare costs by up to $20 billion a year and contribute to roughly 100,000 premature deaths annually.[5] Using new and improved AI systems responsibly can help alleviate problems in each of these areas—if government policies do not interfere.

AI can analyze data faster than humans, augment human reasoning, and quickly screen massive data sets for warning signs that a patient might be at risk. That information can be used to recommend more accurate, personalized treatments and can help reduce missed diagnoses and expensive human error. AI can also automate many healthcare jobs that require routine data entry or analysis, such as reviewing patient information and x-rays for anomalies, and screening for common illnesses and rare diseases.[6] Automated data analysis requires fewer

[1] Mark Mather and Paola Scommegna, **Fact Sheet Aging in the United States**, Population Reference Bureau, January 9, 2024.
[2] **Health Professional Shortage Areas**, data.HRSA.gov (Last visited March 27, 2024).
[3] Centers for Medicare and Medicaid Services, **National Health Expenditures 2022 Highlights**, December 23, 2023.
[4] David Cutler, ***Reducing Administrative Costs in Healthcare***, The Hamilton Project at the Brooking Institution, March 2020.
[5] Thomas L. Rodziewicz, Benjamin Houseman, and John E. Hipskind, ***Medical Error Reduction and Prevention***, (StatPearls Publishing), May 2, 2023.
[6] William Nicholson Price II, **Artificial Intelligence in the Medical System: Four Roles for Potential Transformation**, *Yale Journal of Law & Technology*, Volume 21 (2019) p. 122-132.

trained human healthcare providers to diagnosis and treat medical conditions and may even challenge the conventional wisdom in medical research.[7]

Advances in AI can help medical staff use their time more effectively and efficiently by swiftly reviewing patient data, flagging potential problems, suggesting treatment protocols, and performing routine administrative tasks. Doctors can spend more time considering treatment options[8] and working on health issues that require more cognitive thought or personal attention. Automating notetaking and administrative functions can increase physician and support staff job satisfaction, lower administrative overhead costs, and reduce redundant bureaucracies within the profession.[9]

Most importantly, AI is already helping reduce error rates, improve mortality rates, tailor treatment options, and make medical discoveries. AI programs can warn doctors of sepsis risks faster than human diagnosticians, and those early alerts have raised patient survival rates.[10] Similar artificial intelligence programs have flagged errors in drug prescriptions before it was too late.[11] AI can predict how treatments will affect specific patients and suggest available options accordingly.[12] One in eight men will suffer prostate cancer and AI recently helped doctors discover that prostate cancer is actually two diseases, not one. That discovery holds significant ramifications for cancer treatment and research.[13] AI will not replace doctors, but it can help them treat more patients more efficiently and effectively.

Risks to these advantages understandably include patient privacy and data breeches that could expose sensitive, highly personal information. Healthcare providers, patients, insurers, and government regulators are right to look for ways

---

[7] Yogesh Kumar, Apeksha Koul, Ruchi Singla and Muhammed Fazal Ijaz, **Artificial Intelligence in Disease Diagnosis: a systematic literature review, synthesizing framework and future research agenda**, *Journal of Ambient Intelligence and Humanized Computing*, Volume 14, Issue 7 (January 2022) p. 8459-8486.

[8] Abhimanyu S. Ahuja, **The impact of Artificial Intelligence in medicine on the role of the physician**, PeerJ, October 4, 2019.

[9] Joseph Spear, Jesse M. Ehrenfeld, and Brian J. Miller, **Applications of Artificial Intelligence in Healthcare Delivery**, *Journal of Medical Systems*, Volume 47, Article Number 121 (November 2023).

[10] Roy Adams, et. al., **Prospective, multi-site study of patient outcomes after implementation of the TREWS machine learning-based early warning system for sepsis**, *Nature Medicine*, July 21, 2022.

[11] Ahmed Al Kuwait, et. al., **A Review of the role of Artificial Intelligence in Healthcare**, *Journal of Personal Medicine*, Volume 13, Issue 6 (June 2023) p. 951.

[12] William Nicholson Price II, **Artificial Intelligence in the Medical System: Four Roles for Potential Transformation**, *Yale Journal of Law & Technology*, Volume 21 (2019) p. 122-132.

[13] **AI Reveals Prostate Cancer Is Not Just One Disease**, University of Oxford, March 5, 2024.

to balance those legitimate privacy and data concerns against the benefits AI can offer modern medicine and U.S. healthcare. This paper explores the state and federal policy risks that threaten AI innovation, and it examines the regulatory patchwork and misguided calls for more government interference in this burgeoning field. It concludes by offering five policy improvements that will encourage regulatory compliance with data privacy and AI-related rules and promote a more reasonable regulatory framework in which developers can create safer, more secure artificial intelligence technologies.

MISGUIDED POLICY THREATS TO HEALTHCARE AI INNOVATION

Government regulatory action threatens artificial intelligence innovation in healthcare. At the federal level, the Biden administration has deviated from the Clinton administration's successful limited-regulatory approach that allowed the nascent internet to experiment and flourish in the late 1990s.[14] A dysfunctional Congress has done little to check the Biden administration's aggressive rulemaking and has instead punted legislative duty to unelected bureaucrats. At the state level, AI-skeptical policymakers have taken a heavy-handed approach, adopting a patchwork of laws and regulatory restrictions on everything from the underlying data needed to train artificial intelligence systems to the algorithms it produces. States have even regulated hiring decisions in the AI sector and levied taxes on related job displacements.[15] The net impact of state and federal AI regulation will not be nominal and will likely delay or negate many of the benefits that the technology offers to doctors and patients.

Prescribed Federal Regulation Will Slow AI Development

In 2023, President Biden issued Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[16] Among other things, the sweeping order made clear that the Biden administration expects federal agencies to actively direct and regulate AI innovation.

Section 4.1 directs the secretary of commerce to work with the secretary of energy, the secretary of homeland security, and "the heads of other relevant agencies" to "[e]stablish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems." Those guidelines should include companion resources to the AI Risk Management Framework and Secure Software Development Framework and should develop "an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could

[14] Ryan Hagemann, **Commemorating 20 Years of Grade-A Internet Policy**, Niskanen Center, June 30, 2017.
[15] Adam Thierer, **State and Local Meddling Threatens to Undermine the AI Revolution**, *The Hill,* January 21, 2024; Rachel Wright, ***Artificial Intelligence in the States: Emerging Legislation***, The Council of State Governments, December 6, 2023.
[16] The Federal Register, **Executive Order 14110**, October 30, 2023.

cause harm, such as in the areas of cybersecurity and biosecurity."[17] The order goes on to require "appropriate procedures and processes to enable developers of AI…to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems." These procedures must include:

> (A) coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models; and (B) in coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as to support the design, development, and deployment of associated PETs…[18]

AI testing and safeguarding will be led by agency bureaucrats, not market innovators or technology sector watchdogs.

Beyond testing and safety protocols, the executive order mandates AI-industry reporting requirements and recordkeeping. Section 4.2 directs the secretary of commerce to require

> (i) Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records regarding…(A) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats; (B) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and (C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing…, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security.[19]

[17] **Executive Order 14110**, Sec. 4(a)(i)(C).
[18] **Executive Order 14110**, Sec. 4(a)(ii)(A-B).
[19] **Executive Order 14110**, Sec. 4.2(i)(A-C).

Furthermore, the Commerce Department shall require "(ii) Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster."[20]

Once implemented, these federal mandates and government-sponsored protocols will do little to foster the market-driven innovation that the order itself purports to champion. Instead, bureaucratic red-tape will do to AI development what it does to every other sector it sticks to—strangle it. Government regulations restrict innovation and competition and reduce economic growth by two percent annually.[21] Time and resources spent complying with government mandates are time and resources not spent researching, coding, or marketing a product. And time and resource considerations are especially significant to start-ups and smaller firms without the financial means to comply efficiently, which means that regulatory burdens tend to benefit larger companies with lawyers and lobbyists at-the-ready.

AI-development in the healthcare sector looks no different. Section 8 of Executive Order 14110 anticipates advances in healthcare-related AI and lays the foundation for a heavy, regulatory structure. "To help ensure the safe, responsible deployment and use of AI in the healthcare, public-health, and human-services sectors," President Biden directs the secretary of health and human services to

> establish an HHS AI Task Force [to] develop a strategic plan that includes policies and frameworks—possibly including regulatory action, as appropriate—on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health), and identify appropriate guidance and resources to promote that deployment…[22]

A long list of soon-to-be regulated healthcare subsectors follows that directive. And that does not bode well for fledgling AI initiatives.

[20] **Executive Order 14110**, Sec. 4.2(ii).
[21] Patrick A. McLaughlin, Nita Ghei and Michael Wilt, **Regulatory Accumulation and Its Costs**, Mercatus Center at George Mason University, May 4, 2016.
[22] **Executive Order 14110**, Sec. 8(b)(i).

Neither does the federal meddling in healthcare-related AI development already underway at the Food and Drug Administration (FDA),[23] which is encouraging partnerships between universities and large technology companies to create "assurance laboratories"—many funded with public tax dollars—to monitor AI.[24] Universities and their Big Tech lab partners will approve AI technology as they see fit and help regulators assess each new technology's usefulness. Smaller businesses not invited to the assurance laboratory assessment sessions are understandably concerned that they will face unfair competition from and higher regulatory barriers than the larger, more established companies that will be helping the government write the rules.[25]

State Regulations Run Rampant

Consumer data is part-and-parcel to the development of artificial intelligence, which makes data privacy laws that impose onerous and complicated restrictions on data access a direct threat to responsible AI development. In fact, since data privacy laws govern how input data can be collected, used, and stored, state data privacy laws already regulate how AI can be used and developed. Credit, employment, insurance and housing evaluations using artificial intelligence, for example, are already regulated under the Fair Credit Reporting Act, the Equal Credit Opportunity Act, and certain state specific data privacy laws, and many state-specific laws govern general data rights like the ability to access, use, and delete information.[26] Tellingly, most AI laws going into effect in 2023 were amendments or changes to already existing data privacy laws, with 10 states including AI regulatory language in laws passed or going into effect in 2023.[27] In other words, data privacy policy is now also AI policy.

Nevertheless, some regulatory advocates wrongly suggest that AI technologies have advanced in an unregulated environment. More accurately, states have been regulating artificial intelligence development for several years. According to The Software Alliance, for example, AI-related legislation rose more than 400 percent

[23] General Accounting Office, ***Federal Regulation, Selected Emerging Technologies Highlight the need for Legislative Analysis and Enhanced Coordination***, January 2024.
[24] Robert M. Califf, commissioner, U.S. Food and Drug Administration, **Remarks to the Coalition for Health AI (CHAI)**, March 4, 2024.
[25] Ruth Reader, **Startups oppose tech giants and health systems' plan to lead on AI regulation**, Politico, March 11, 2024.
[26] Brian Hengesbaugh, **How Existing Data Privacy Laws May Already Regulate Data-related Aspects of AI**, International Association of Privacy Professionals, June 7, 2023.
[27] Katrina Zhu, **The State of State AI Laws: 2023**, Electronic Privacy Information Center, August 3, 2023.

from September 2022 to September 2023,[28] ranging from innocuous study groups to pernicious "robot taxes" and over-broad algorithmic regulations.[29] In 2023, 25 states, Puerto Rico, and the District of Columbia introduced more than 150 AI proposals,[30] with New York and California accounting for 36 of them.[31] Only 10 states even have full-time legislatures, but in 2024 more than a quarter of U.S. state legislatures are considering more than 400 pieces of AI legislation.[32]

Lawmakers can and should form study groups to assess the impacts and risks of artificial intelligence, but taxes and strict new rules will do more harm than good; and a patchwork of unwieldy state laws may prove no less damaging than federal agencies. Even before the breakthrough in generative AI tools, an Information Technology & Innovation Foundation study estimated that if all states passed their own data privacy laws, that regulatory patchwork of state data privacy laws could cost $98 billion to $112 billion annually in out-of-state costs alone.[33]

State-level AI regulations threaten bureaucratic licensing requirements, age restrictions, auditing and transparency mandates, innovation permission slips, and even new regulatory agencies specifically designed to "oversee" AI development.[34] That must change.

Robot Taxes Discourage Life-Saving Technologies

Many Americans worry that AI advancement—especially AI automation—will displace jobs.[35] Responding to this concern, state and federal lawmakers may propose curbing AI automation through so-called "robot taxes" on employers

[28] Adam Thierer, **State and Local Meddling Threatens to Undermine the AI Revolution**, *The Hill,* January 21, 2024; BSA-The Software Alliance, **2023 State AI Legislation Summary**, September 22, 2023.
[29] Christopher Stevens and Jenny Holmes, **Complying with New York City's Bias Audit Law**, Nixon Peabody, November 13, 2023.
[30] **Artificial Intelligence of 2023**, National Conference of State Legislatures, January 12, 2024.
[31] *Ibid.*
[32] **States With a Full-time Legislature**, Ballotpedia (Last visited March 27, 2024); Owen Davis and David Strauss, **A Look at Proposed U.S. State Privacy Sector AI Legislation**, International Association of Privacy Professionals, February 28, 2024; Jesse Bedayn, **States Target AI's Hidden Hand in Americans' Lives**, Associated Press, March 5, 2022.
[33] Logan Kolas, ***A Federalism Opportunity in a Congressional Failure***, The Buckeye Institute, August 10, 2023; Daniel Castro, Luke Dascoli, and Gillian Diebold, **The Looming Cost of a Patchwork of State Privacy Laws**, Information Technology and Innovation Foundation, January 24, 2022.
[34] Adam Thierer, **Blumenthal-Hawley AI Regulatory Framework Escalates the War on Computation**, Medium, September 13, 2023.
[35] Taylor Barkley, **A New Pool Reveals What Americans Fear About AI Taking Their Jobs**, The Center for Growth and Opportunity at Utah State University, August 10, 2023.

suspected of displacing workers with algorithms, even if the technology complements workers rather than replacing them.[36] In healthcare, robot taxes would tax life-saving medical innovations and time-saving technologies that would allow doctors to spend more time treating patients. And those taxes would discourage those technologies and AI advances that U.S. healthcare desperately needs just to keep pace with medical data. In the 1980s, medical information doubled roughly every seven years. Today, it doubles every 73 days.[37] Doctors and medical staff simply cannot keep up with that kind of exponential growth. But AI algorithms can, and they can augment human capabilities, help medical professionals interpret and use data to treat patients, and improve health outcomes across the globe. Taxing those algorithms in the name of "job security" treats the problem with a short-sighted bandage at the expense of long-term cure.

State Data Privacy Laws: A Nuanced Trade-Off That Still Hurts Small AI Firms

Generative AI collects copious data, uses that information to engineer algorithms to establish patterns, and then turns those patterns into predictive applications. The better the data, the better the predictions. Data privacy laws reduce data access, which makes AI applications more complicated and expensive to build. But data differ and, in America, data access differs by type and by rule. U.S. law regulates data use in different sectors of the economy differently, with different statutes governing how different types of sensitive data must be protected. The Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, for example, prevent unauthorized financial data collection, disclosure, and transfers.[38] The Family Education Rights and Privacy Act protects education data, and the Children's Online Privacy Protection Act regulates sensitive data on minors.[39] The Health Insurance Portability and Accountability Act of 1996—or HIPAA—famously restricts how covered healthcare entities[40] can use and store patient data. Those

[36] John Whittaker, **'Robot Tax' on Automation Proposed**, *The Post-Journal*, December 12, 2023; **Robot Tax Act**, State of New York, October 27, 2023.
[37] Adam Thierer, **What I Learned About the Power of AI at the Cleveland Clinic**, Medium, May 6, 2022.
[38] Will Rinehart, **The Law & Economics of "Owning Your Data"**, American Action Forum, April 10, 2018; and Garry Kranz, **Gramm-Leach-Bliley Act (GLBA)**, TechTarget (Last visited March 27, 2024).
[39] **Family Educational Rights and Privacy Act (FERPA)**, U.S. Department of Education (Last visited March 27, 2024); and Clare Y. Cho, **Challenges with Identifying Minors Online**, Congressional Research Service, March 23, 2023
[40] **Health Insurance Portability and Accountability Act of 1996 (HIPPA)**, Centers for Disease Control and Prevention (Last visited March 27, 2024).

data-sharing restrictions inhibit digitalizing hospital records[41] and create a nuanced trade-off between health data protections and healthcare innovation.[42] Citizens and policymakers should understand that trade-off and seek the right balance between data privacy safeguards and the benefits of improved predictive medical applications.

State policymakers and regulators should also understand that a patchwork of similar-but-not-the-same data privacy laws, each with slightly unique reporting and compliance requirements, tends to benefit large technology firms with the financial resources to pay lawyers and compliance officers to understand the rules across dozens of jurisdictions, while simultaneously hurting smaller firms trying to compete. Regulators and lawmakers may not intend to dig a regulatory moat that protects Big Tech from competition, but they have dug that moat, nonetheless.

A regulatory briar patch requires technology firms of any size to first spend time and money learning what the rules allow. Then they must pay for software and hardware to do what the law demands. After that, firms have to hire engineers and lawyers to ensure that they remain compliant even as regulators amend the rules and legislatures enact new laws. Meeting those challenges may not be a heavy lift for firms like Google, which spent $31 billion in 2022 on AI research and development alone, but the regulatory burden hits harder for AI start-ups with an average operating budget of about $655,000 per year.[43] Consider, too, that a single data "access and deletion" request can cost a technology company $1,400.[44] A hundred of such requests may mean little financially to Google and Apple but could represent over 20 percent of a start-up's yearly budget.

Some of these expenses may be temporary and frontloaded but maintaining regulatory compliance costs last forever. Europe's data privacy regulation, for example, which has reduced profits at small technology firms by 8.1 percent and sales by 2.1 percent,[45] requires businesses to "create additional data inventory and

---

[41] Ginger Zhe Jin, ***The Economics of Artificial Intelligence: An Agenda***, National Bureau of Economic Research, (May 2019) p. 439-462; Amalia R. Miller, **Privacy of Digital Health Information**, working paper, University of Virginia, May 2023.

[42] Avi Goldfarb and Catherine Tucker, **Privacy and Innovation**, working paper, National Bureau of Economic Research, June 2011.

[43] Min Jun Jung and Nathan Lindfors, **Startups and AI Policy: How to Mitigate Risks, Seize Opportunities, and Promote Innovation**, Engine, September 8, 2023.

[44] William Rinehart, ***What Is the Cost of Privacy Legislation?***, The Center for Growth and Opportunity at Utah State University, November 17, 2022; James Spiro, **Attempting a 'Data Detox' in Today's Digital World**, Ctech, August 30, 2021.

[45] Chinchih Chen, Carl Benedikt Frey, and Glorgio Presidente, **Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally**, working paper, Oxford Martin School, University of Oxford, January 6, 2022.

mapping to accommodate access and deletion requests, create consent management systems, and update their privacy policies, all of which must be routinely updated to accommodate new privacy rules."[46] Similarly, President Biden's Executive Order 14110 called upon multiple federal agencies across virtually every economic sector to devise plans, rules, and regulations with on-going requirements that will need to be amended periodically as technology and market circumstances dictate. Those rules will not inflict one-time expenses, and neither will state data privacy regulations.[47] Even when California tried to exempt many smaller businesses from its own rule's reach, it soon found that small firms were still likely to shoulder a disproportionate burden.[48]

In fact, although most states, including California, have tried to exempt small technology firms from onerous data privacy obligations and expenses, the state of Washington made no such accommodation under its My Health, My Data law governing consumer health information. A poorly drafted statute with vague, overbroad definitions,[49] that law will ultimately set a default national standard and compel virtually every technology company that touches health data, regardless of size, market share, or operating budget to comply. Data privacy laws allow businesses to collect and use consumer data after gaining user consent through either an "opt-in" or "opt-out" framework. Opt-in systems require businesses to gain affirmative consumer consent before collecting or using any data. Opt-out systems assume implied consumer consent to use consumer data unless instructed otherwise. Washington's My Health, My Data chose the opt-in structure, which tends to restrict more data collection than the opt-out framework.[50] Countries using opt-in rules have more consumers invoke privacy rights than countries or states using opt-out rules. [51] The opt-in requirements in Europe, for example, resulted in a 12.5 percent dip in consumers,[52] while California's opt-out structure

[46] Logan Kolas, ***Key Principles for State Data Privacy Laws***, The Buckeye Institute, October, 2023; ***The Age of Privacy: The Cost of Continuous Compliance***, DataGrail, May 2019.
[47] David Navetta and Alex Murchison, **At GDPR's One Year Mark, Continued Compliance Efforts Are Key and Can Help with CCPA Compliance**, Cooley, July 8, 2019.
[48] Berkeley Economic Advising and Research, ***Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations***, State of California Department of Justice Office of the Attorney General, August 2019.
[49] **Washington My Health My Data Act**, Washington State Legislature (Last visited March 27, 2024).
[50] Robert Bateman, **Washington's My Health My Data Act vs. California's CCPA**, Privado, July 10, 2023.
[51] Mike Hintze, **The Washington My Health My Data Act – Part 1: An Overview**, Hintze, April 10, 2023.
[52] Guy Aridor, Yeon-Koo Che, Tobias Salz, **The Effect of Privacy Regulations on the Data Industry: Empirical Evidence from GDPR**, working paper, National Bureau of Economic Research, March 2020.

has caused less than a five percent drop.[53] Washington's My Health, My Data law follows the flawed European model and will likely inflict similar results, pinching startup AI firms struggling to tailor appropriate datasets to support their models. Washington made matters worse by vesting authority to enforce My Health, My Data in private rights of action, effectively deputizing plaintiffs' attorneys and inviting an unintended wave of expensive, "gotcha" lawsuits for small technology firms to defend.[54]

Legislating for Algorithmic Bias—and Other Regulatory Mistakes

Policymakers rightly worry that AI technologies will suffer from "algorithmic bias" and skew outputs in undesirable directions against demographic classes or disfavored views—but they wrongly seek regulatory solutions to problems the private sector is already solving. Researchers have been working to correct artificial intelligence biases for years and continue to do so.[55] Dandelion Health, for example, is currently hurdling the regulatory obstacles to collect proprietary data and construct a large, de-identified dataset of more 10 million patient records, helping fill a market need for representative datasets for healthcare researchers and to clarify which algorithms are least biased.[56]

Despite being developed in "isolation from policy and civil society contexts and lack[ing] serious engagement with philosophical, political, legal, and economic theories of equality and distributive justice," generative AI systems and the rise of ChatGPT have made algorithmic regulation ripe for political pandering and legislative action—with severe consequences for healthcare.[57] Oxford University researchers found, for example, that anti-bias algorithms can remove bias in two ways: 1) with a "levelling up" process whereby algorithm developers exercise precaution and over-screen patients at the cost of accuracy; or 2) with a "levelling down" process designed to achieve "fairness" and "equality" by "bringing better performing groups down to the level of the worst off."[58] Developers, of course, initially opt for "leveling-up" systems to over-screen for diseases until reaching a

---

[53] ***IAB CCPA Benchmark Survey***, IAB.com, November 12, 2020.
[54] Mike Hintze, **The Washington My Health My Data Act – Part 1: An Overview**, Hintze, April 10, 2023.
[55] Alexandra George, **Thwarting Bias in AI Systems**, Carnegie Mellon University's College of Engineering, December 11, 2018; Miana Massey, **Maryland Researchers Working to Correct Potential Bias in Artificial Intelligence**, CBS News, February 20, 2023.
[56] Katie Jennings, **How This Startup Is Using 10 Million Patient Records to Reduce Bias in Healthcare AI**, *Forbes*, December 21, 2023.
[57] Brent Mittelstadt, Sandra Wachter, and Chris Russell, **The Unfairness of Fair Machine Learning: Levelling Down and Strict Egalitarianism by Default**, *Michigan Technology Law Review*, January 20, 2023.
[58] *Ibid.*

subjective "tipping point" at which no more accuracy can be forfeited without jeopardizing the integrity of the entire model.[59] But regulatory constraints make developers work backwards from pre-ordained outcomes, so developers may no longer achieve fairness by improving minority health outcomes and must instead achieve legislative fairness or "equal performance" by reducing model performance on more-typical patients.[60] As the researchers argued, this kind of algorithmic equality could lead to undertesting for diseases like cancer.[61] It is unlikely that state policymakers will resist the urge to regulate perceived algorithmic bias, but they should be aware of the risks and consequences of "levelling down" protocols and guard against them.

A better course would pursue reforms that make data access easier, particularly access to smaller databases, and then encourage developers to incorporate this data (especially sensitive data) into their models, which would increase secure but available data sets that accurately represent the population and thus improve model outputs and accuracy. One problem confronting AI healthcare, for example, is that billions of dollars have been distributed to algorithmic formulation even as data limitations have pushed the trial-and-error phase of algorithmic improvement into use-cases in which the model is used in healthcare decision-making processes.[62] Had more data been available before the algorithms were used, the models could have been tested and those problems could have been caught and treated before model deployment.[63] HIPAA is among the many laws that shrink the data pool further, making data collection more difficult[64] and yielding incomplete datasets that appear biased because they are incomplete.[65] Rather than regulating algorithm outputs, policymakers should first amend data privacy rules to make data access more secure and plentiful.

Even if health data can be collected accurately, it then needs to be deployed effectively through unbiased algorithms. AI bias laws, unfortunately, could unintentionally make these problems worse, not better. Algorithms have historically been trained *not* to use sensitive data in the hope of preventing

---

[59] *Ibid.*
[60] *Ibid.*
[61] **Healthcare Bias Is Dangerous. But So Are 'Fairness' Algorithms**, Wired, February 8, 2023.
[62] Katie Jennings, **How This Startup Is Using 10 Million Patient Records to Reduce Bias in Healthcare AI**, *Forbes*, December 21, 2023.
[63] *Ibid.*
[64] **Individuals' Right Under HIPAA to Access Their Health Information 45 CFR § 164.524**, U.S. Department of Health and Human Services (Last visited March 27, 2024); Walter Olson, **What HIPAA Isn't**, Cato Institute, June 2, 2021.
[65] Katie Jennings, **How This Startup Is Using 10 Million Patient Records to Reduce Bias in Healthcare AI**, *Forbes*, December 21, 2023.

discriminatory practices in healthcare, hiring decisions, loan financing, and housing applications to reduce bias and comply with America's data privacy regime.[66] By excluding sensitive information like biological sex or race in datasets, so the logic goes, bias and discrimination decline as the algorithm runs agnostic to sensitive demographic or identity information. But although that logic may work well with human screenings, applying it to AI algorithms can increase, not decrease, biases when imbalances exist between population subgroups—and, unfortunately, because healthcare access is unequal and because different demographics suffer diseases at varying probabilities, healthcare also exhibits many imbalances.[67] And understandably so, since race and gender are not relevant criteria when buying a home, securing a loan, or seeking new job opportunities—but this information can be relevant for healthcare.

Federal policymakers have also staked dubious claims that threaten to undermine AI innovation. For example, Lina Kahn, commissioner of the Federal Trade Commission (FTC), announced in early 2024 that health and location data should be "off limits" to developers looking for training data to improve healthcare artificial intelligence systems.[68] A single federal data privacy law preempting all state data privacy rules may be preferrable to the state-federal data privacy split that currently governs, but only if that law is clear, concise, and carefully designed to limit arbitrary expansion by the agencies that enforce it.[69] Such a law must be designed and enacted by Congress, not drafted under rulemaking authority by unelected bureaucrats. Whether Kahn intended such a law is unclear, but unlikely, insofar as she has also pushed to use agency authority to rewrite antitrust law to target technology companies. Importantly, even if this rulemaking significantly curbs perceived privacy threats, it will come at the cost of increased bias as data pools dry up and algorithms train on less representative, more inaccurate datasets. Regardless, governments and their executive agencies are sending businesses mixed signals, increasing uncertainty and forcing businesses into a lose-lose proposition. The FTC signals for developers to avoid health data while states

[66] Stephanie Kelley, Anton Ovchinnikov, Adrienne Heinrich, and David R. Hardoon, **Removing Demographic Data Can Make AI Discrimination Worse**, *Harvard Business Review*, March 6, 2023.
[67] *Ibid.*
[68] Leah Nylen, **FTC's Khan: Health, Location and Data Should Be 'Off Limits' for AI**, Bloomberg Law, February 27, 2024; Joel Shalowitz, **The Nexus of Medical Care + Business**, HealthcareInsights.MD, March 8, 2024; Lina Kahn, chair of the Federal Trade Commission, **Remarks at RemedyFest**, February 27, 2024; Leah Nylen, **FTC's Khan: Health, Location Data Should Be 'Off Limits' for AI**, Bloomberg News, February 27, 2024.
[69] Logan Kolas, ***A Federalism Opportunity in a Congressional Failure***, The Buckeye Institute, August 10, 2023.

simultaneously pass directives requiring more data collection and processing to reduce perceived bias.

Meanwhile, the FTC typically probes significant mergers and acquisitions to prevent antitrust violations, but it recently investigated corporate investments into AI language model developer, Anthropic, a startup spun-off from ChatGPT developer OpenAI.[70] Adversarial federal investigations into AI investments have the potential to slow down—not speed up—adopting safer, better AI systems by signaling that FTC plans to meddle in artificial intelligence competition and delaying or denying investments if legal action is pursued. Technological innovation in healthcare has functioned fine without FTC meddling. Amazon acquiring the data-driven healthcare startup, One Medical, for example, likely expanded nontraditional primary care options by streamlining wait times and making it easier to book appointments.[71] By contrast, investigating spinoffs like Anthropic, widely considered one of the safest, most advanced large language model AI systems on the planet,[72] threatens technological improvements and widespread adoption of safer, better AI technologies.

[70] Kevin Roose, **Inside the White-Hot Center of A.I. Doomerism**, *The New York Times*, July 11, 2023.
[71] Jennifer Huddleston, **No, Amazon Isn't Coming for Your Medical Data**, Reason, July 27, 2022.
[72] Pascale Davies, **OpenAI Rival Anthropic Launches its Fastest and Most Powerful Chatbot Claude 3**, EuroNews, March 4, 2024.

POLICY SOLUTIONS TO PROMOTE HEALTHCARE AI

As well-intended but misguided AI regulatory restrictions bloom across the state and federal landscape, policymakers should reconsider the prevailing approach and seek ways to improve innovation and strike a more reasonable regulatory balance. State and federal policymakers can take several steps toward such improvement. First, state lawmakers can presume that a new technology is innocent until proven guilty. That is, inventors and innovators should be free to pursue new technologies before seeking the government's permission. Regulators should have the burden of proof and persuasion to show harm, rather than requiring developers to prove their invention's innocence. Second, Congress must reassert its constitutional role and regulate industry by statute, not by delegating that duty to unelected bureaucrats. Third, state and federal policymakers should rely on "soft law" incentives and protocols to guide AI policy and encourage industry behavior and outcomes. Fourth, states should construct regulatory sandboxes for AI developers to experiment with their inventions under the supervision of regulatory experts. Such sandboxes have proven effective in other sectors at encouraging innovation with less risk to consumers. And finally, states should collaborate to harmonize data privacy rules and AI-related regulations to reduce multi-state compliance costs for developers and data collectors. State compacts that resist frequent regulatory amendments will promote compliance and data privacy, and foster a more consistent, less confusing regulatory environment for developing safe AI technologies.

Presume Innovation Innocent

As technology policy scholars argued in 2017, well before AI-infused political panic, policymakers could codify a regulatory presumption that technology is innocent until proven guilty.[73] Unlike the relatively regulation-free development of the internet,[74] most new technology may not develop unless agency regulators give innovators permission to proceed. A presumption of innovation in regulatory codes would shift the burdens of proof and persuasion onto regulators trying to control technological development. Hawaii and California have already taken the

[73] Adam Thierer, **Converting Permissionless Innovation into Public Policy: 3 Reforms**, Medium, November 29, 2017.
[74] Adam D. Thierer, ***Getting AI Innovation Culture Right***, R Street Policy Study, No. 281, March 30, 2023.

opposite approach with respect to artificial intelligence. On January 19, 2024, Hawaii introduced "precautionary principle" legislation requiring AI developers to wait for the government to grant them the privilege to innovate.[75] California's similar proposal requires developers to adhere to the precautionary principle even before training their models, or self-certify and face felonious perjury charges if safety mechanisms are breached by bad actors who use the new technology to commit serious criminal activity.[76] Hawaii and California have it backwards. States should presume innovated technology innocent until regulators can prove it guilty.

Restore Congressional Oversight

Congress has over-delegated its legislative authority to executive branch agencies. Those agencies, through unelected bureaucrats, have over-regulated the AI technology sector and restricted competition with regulatory moats that unfairly favor large firms. All sector stakeholders, including small business and startups, should be at the table to discuss AI security and privacy procedures—and that discussion should be held by Congress, not agencies and their Big Tech partners. Congress should retake its regulatory mantle and in doing so understand the various benefits that AI can provide to doctors, patients, and the American healthcare system if regulators do not choke out the technology.

Rely on "Soft Law" to Guide AI Policy

A combination of government mandates and market incentives help determine how private enterprises behave. Requirements enforced by governments—sometimes called "hard law"— regulate healthcare goods and services like pharmaceutical drugs, insurance plans, data privacy, and medical supplies. But less formal "soft law" rules have helped structure accountability and guide behavior in emerging technology for decades. Soft law takes many forms: supply chain expectations for business transactions; government procurement stipulations; behavior aligned to external expectations among peers and the media; private market certification bodies; trade association requirements; informal professional societies; liability requirements for insurance coverage; funding incentives; performance standard labeling; and competition to meet consumer demands for quality, low-cost products.[77] Soft law requirements

[75] **Hawaii Artificial Intelligence Safety and Regulation Act**, Senate Bill 2572, State of Hawaii Senate 32nd Legislature, 2024.
[76] Dean W. Ball, **California's Effort to Strangle AI**, Hyperdimensional, February 9, 2024.
[77] Gary Marchant, Lucille Tournas, and Carlos Ignacio Gutierrez, **Governing Emerging Technologies through Soft Law: Lessons for Artificial Intelligence**, *Jurimetrics* (2020) p. 1-18.

encourage responsible private market behavior without strong-arm government interference. Because artificial intelligence systems develop faster than regulators can design appropriate rules, and because the costs and benefits of AI are uncertain, the hard law approach will prove difficult, ill-fitted, and quickly obsolete.[78] Soft law, however, offers dynamic constraints flexible enough to keep pace with the technology's rapid advances.

Relying on soft law to guide privacy, technology, and healthcare policy is not new. The FDA has a long history of suggesting best-practices and issuing non-binding guidance if only to informally influence policy, recommend responsible behavior, and clarify how future regulations may emerge.[79] And given how technology has quickly integrated into healthcare and the practice of medicine, some of this guidance has removed uncertainty by clarifying FDA thinking on health technology policy, such as software functions and mobile medical applications.[80] As Kenneth A. Bamberger and Deirdre K. Mulligan detail in seminal research in the *Stanford Law Review*, the United States already has a robust, decentralized, and privately developed privacy system as privacy associations and corporate privacy officers developed best-practices for data collection and handling.[81]

Soft law is already emerging as an AI governance tool as federal policymakers contemplate legislative next steps. A nongovernmental international entity of 164 standards bodies, known as the International Organization of Standardization, is collaborating with International Electrotechnical Commission to create AI standards.[82] As John Villasenor at the Brookings Institution notes, "Algorithm Watch" maintains an AI ethics inventory of more than 150 global standards and guidelines.[83] In the United States, the National Institute for Standards and Technology (NIST) created a flexible, practical, and evolving privacy framework under authority from the U.S. Department of Commerce that has been widely and

[78] *Ibid.*
[79] **Best Practices for Convening a GRAS Panel: Guidance for Industry**, U.S. Food and Drug Administration, OMB Control No. 0910-0911, December 2022; **What Is the Difference between Laws, Regulations, and Guidance Documents?**, Melnik Legal (Last visited March 27, 2024); John Villasenor, **Soft Law as a Complement to AI Regulation**, The Brookings Institution, July 31, 2020.
[80] **Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff**, U.S. Food and Drug Administration, September 25, 2013.
[81] Kenneth A. Bamberger and Deirdre K. Mulligan, **Privacy on the Books and on the Ground**, *Stanford Law Review*, Volume 63, Issue 2 (January 2011) p. 247; Adam Thierer, **AI Governance "on the Ground" vs "on the Books"**, Medium, August 19, 2022.
[82] John Villasenor, **Soft Law as a Complement to AI Regulation**, The Brookings Institution, July 31, 2020.
[83] *Ibid.*

voluntarily used by private organizations looking to responsibly protect and use consumer data.[84] The framework has been so highly regarded that Ohio suggested (and Tennessee then adopted) using compliance with these soft law standards as an affirmative defense in court for allegations of noncompliance with the state's proposed data privacy law.

President Biden proposed something similar for artificial intelligence after NIST released its AI Risk Management Framework, but the President erred by speculatively forcing agencies to disclose dual-use AI models to the government under the Defense Production Act.[85] Still, prioritizing objective soft law measures that draw on flexible, multi-stakeholder processes is preferable to more hard law bureaucracy for innovative companies still struggling to compete in an uncertain, heavily regulated market. By prioritizing soft law over hard law, and observing how organizations respond, regulators can improve future statutory requirements. Not every unintended consequence can be foreseen and averted, but soft law allows agencies to limit some of the most avoidable unwanted collateral damage before implementing official requirements.

Build an Artificial Intelligence Regulatory Sandbox

The rapid proliferation of generative artificial technologies conflicts with traditional regulatory systems. As Will Rinehart of the American Enterprise Institute put it, "silicon innovation is colliding with jurisdictional steel."[86] Physicians using artificial intelligence software expose themselves to legal risk if they rely on AI to help make medical decisions.[87] Many physicians or practitioners may one day opt for AI liability insurance to insulate themselves from future risk just as developers and manufacturers will seek coverage for product liability.[88] And

[84] Katharina Koerner, **Standardization Landscape for Privacy: Part 1—the NIST Privacy Framework**, International Association of Privacy Professional, December 1, 2021; **Privacy Framework Perspectives and Success Stories**, National Institute for Standards and Technology, October 3, 2023.

[85] **NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence**, National Institute of Standards and Technology, January 26, 2023; Will Rinehart, **Unpacking the Executive Order on AI**, The Exformation Newsletter, November 9, 2023; Sharon Goldman, **NIST Staffers Revolt against Expected Appointment of 'Effective Altruist' AI Researcher to US AI Safety Institute**, Venture Beat, March 7, 2024.

[86] Will Rinehart, **Silicon Innovation Is Colliding with Jurisdictional Steel**, The Exformation Newsletter, August 7, 2023.

[87] W. Nicholson Price II, Sara Gerke, and I. Glenn Cohen, **Potential Liability for Physicians Using Artificial Intelligence**, *JAMA*, October 4, 2019, p. 1765-1766.

[88] Ariel Dora Stern, Avi Goldfarb, Timo Minssen, and W. Nicholson Price II, **AI Insurance: How Liability Insurance Can Drive the Responsible Adoption of Artificial Intelligence in Healthcare**, *New England Journal of Medicine Catalyst 3,* Number 4, April 2022; George Maliha,

yet new innovators in the healthcare AI space may not even know whether and how state and federal laws apply to their businesses.

Fortunately, building a regulatory sandbox for artificial intelligence technologies—at the state and federal levels—could help AI innovators and users safely develop technologies in a supervised testing environment in which risks can be confined and controlled. State regulators could create nimble regulatory arrangements under which innovators may experiment with AI technologies (and their applications) under the watchful eye of expert regulators. Unfortunately, state sandboxes have limited impact because many (but not all) restrictions slowing AI development are federal, and nearly all state sandbox commissions can only pause administrative, not statutory, restrictions. But states can align sandboxes to federal sandboxes at the Consumer Financial Protection Bureau, and commissions can research and recommend changes to laws that slow technological progress.

Promote Interstate Collaboration on Privacy Rules

States can and should collaborate to find regulatory solutions that minimize tedious and costly compliance obligations. First, states can encourage industry to comply with soft law privacy efforts. Ohio, for example, established an "affirmative defense" in data breach cases for companies that had complied with a cybersecurity program meeting certain criteria.[89] Connecticut and Utah followed suit just a few years later.[90] Similarly, Tennessee now affords an affirmative defense for firms that comply with NIST's recommended data privacy framework.[91] Critics dismiss best-practices affirmative defense provisions as giveaways to regulated businesses, but such defenses actually promote data privacy by encouraging compliance with a routinely updated framework and by lowering compliance costs if the provision is adopted in multiple states.[92] Second, states should create—and convince other states to join—voluntary, multi-state compacts with identical data privacy and AI-related statutes. Such compacts already harmonize rules in healthcare, agriculture,

---

Sara Gerke, I. Glenn Cohen, and Ravi B. Parikh, **Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation**, *The Milbank Quarterly*, Volume 99, Issue 3 (April 6, 2021) p. 629-647.

[89] **Ohio Rev. Code Ann. § 1354.02** (effective date November 2, 2018); Molly McGinnis Stine and Hannah Oswald, **"Safe Harbor" Ports in a Cybersecurity Litigation Storm**, Locke Lord, Fall 2021.

[90] Molly McGinnis Stine and Hannah Oswald, **"Safe Harbor" Ports in a Cybersecurity Litigation Storm**, Locke Lord, Fall 2021.

[91] Kaitlin R. Boeckl and Naomi B. Lefkovitz, **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0**, National Institute of Standards and Technology, January 16, 2020; and **Tenn. Code § 47-18-3314**.

[92] Logan Kolas, ***A Federalism Opportunity in a Congressional Failure***, The Buckeye Institute, August 10, 2023.

professional licensure, taxation, resource conservation, mining, and transportation—but not data privacy.[93] That should change. A critical mass of states adopting the same data privacy rules could set a more appropriate national standard rather than cede that ground to the failed regulations in California and Washington. Finally, states should pick a data privacy model and stick to it. Small, frequent statutory changes in otherwise similar laws can cause confusion and raise expensive legal questions and compliance obligations. By working collaboratively and limiting single-state amendments, compacting states can create a less fractured, more predictable regulatory environment for developing safer artificial intelligence technologies.

[93] **Occupational Licensure Compacts**, National Center for Interstate Compacts (Last visited March 27, 2024); **Chart of Interstate Compacts**, Ballotpedia (Last visited March 27, 2024); **United States—Interstate Compacts**, American Law Sources On-line (Last visited March 27, 2024); and **What Are the Nursing Compact States?**, Nursing CE Central (Last visited March 27, 2024).

Conclusion

Artificial intelligence, especially in healthcare, holds great technological promise, but the state and federal regulatory approach to AI and data privacy thus far has been flawed and risks depriving Americans of the yet-unrealized advantages that AI may offer. AI developers and software companies need broader freedom to innovate without an inconsistent, confusing threat of legal sanction. The regulatory playing field should be level and not predisposed to favor large technology firms over smaller competitors. Congress should retake its proper legislative oversight function and not cede its authority to unelected bureaucrats. And federal rule makers should tread lightly and get the lay of the technological landscape before issuing a bevy of mandates and restrictions. States should collaborate and streamline their regulatory actions, striving for consistency across state lines and jurisdictions to make it simpler and cost-effective for developers to comply. Regulators would do well to rely on soft law practices and industry standards before resorting to hard law tactics, and they should build regulatory sandboxes for agency experts to oversee AI developers safely. Artificial intelligence can help doctors, patients, and hospitals, and ease the supply-and-demand imbalance in America's healthcare—if over-zealous regulators will allow it.

ABOUT THE AUTHORS

Rea S. Hederman Jr. is executive director of the Economic Research Center and vice president of policy at The Buckeye Institute. In this role, Hederman oversees Buckeye's research and policy output.

A nationally recognized expert in healthcare policy and tax policy, Hederman has published numerous reports and papers looking at returning healthcare power to the states, the impact of policy changes on a state's economy, labor markets, and how to reform tax systems to spur economic growth.

Prior to joining Buckeye, Hederman was director, and a founding member of the Center for Data Analysis (CDA) at the Heritage Foundation, where he served as the organization's top "number cruncher." Under Hederman's leadership, the CDA provided state-of-the-art economic modeling, database products, and original studies.

While at Heritage, Hederman also oversaw the organization's technical research on taxes, healthcare, income and poverty, entitlements, energy, education, and employment, among other policy and economic issues. He was also responsible for managing Heritage's legislative statistical analysis and econometric modeling.

Hederman's commentary has been published in *The Washington Post*, *The Washington Times*, *National Affairs*, *The Hill*, National Review Online, and FoxNews.com, among others. He is regularly quoted by major newspapers and wire services, and has appeared on Fox News Channel, CNN, CNBC, and MSNBC.

Hederman graduated from Georgetown Public Policy Institute with a Master of Public Policy degree and holds a Bachelor of Arts from the University of Virginia.

Logan Kolas is an economic policy analyst with the Economic Research Center at The Buckeye Institute, where he researches and writes about state and local taxes, state-level budgets, technology and innovation policy, and labor market issues.

Kolas has conducted state-level tax modeling and budget research for states such as Iowa, Louisiana, New Hampshire, and North Carolina. He has authored policy papers, book chapters, blog posts, and op-eds on restoring Ohio's technology and innovation leadership, effective data privacy laws, the impacts of federal and state labor market policies on work, and modernizing Ohio's outdated economic system to return the Buckeye State to economic prosperity and leadership.

The author of The Buckeye Institute's three-part *Policies for More Innovation* series, Kolas authored *A Policy Primer for Emerging Technology in Ohio* and *Modernizing Ohio's Policies to Seize New Economic Opportunities*. Kolas also authored *Ohio's Global Fight for Talent*, detailing the need for Ohio to upskill and reskill its domestic workforce while attracting talent from other states and countries. Kolas' policy proposals on Ohio's workforce were praised by Governor Mike DeWine and Lt. Governor John Husted.

Kolas has testified to legislative committees on free-market policy and privacy issues. His commentary has appeared in regional and national outlets, including *The Hill,* RealClear Policy, *The Columbus Dispatch*, *The Cincinnati Enquirer*, Cleveland.com, *Crain's Cleveland Business*, *Dayton Daily News*, *The Lima News*, and *St. Louis Post Dispatch*, amongst others.

Prior to joining Buckeye, Kolas was a research associate at the Herbert A. Stiefel Center for Trade Policy Studies at the Cato Institute, where his research focused on the impact of international trade on employment, the effect of international trade taxes on state and federal government policies, and the regulatory burden imposed by the government on American businesses and families.

Kolas is a native of Cincinnati and, throughout his career, has focused on researching Ohio-related policies. He earned his Bachelor of Science in economics and political science from George Washington University and holds a Master of Science in applied economics from the University of Maryland.

A Healthcare World Reimagined: How Big Government Threatens Healthcare AI and What to Do About It

THE BUCKEYE INSTITUTE
88 East Broad Street, Suite 1300
Columbus, Ohio 43215
(614) 224-4422
BuckeyeInstitute.org