epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Request for Information: Accelerating the Adoption and Use of Artificial Intelligence as Part of Clinical Care

90 Fed. Reg. 60,108

February 23, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Department of Health and Human Services (HHS or the Department)'s Request for Information (RFI) regarding Accelerating the Adoption and Use of Artificial Intelligence as Part of Clinical Care.[1] EPIC urges the Department to prioritize privacy in the adoption and use of all technologies used in clinical settings as privacy is essential to improve health outcomes. HHS should focus on AI protections for patients and health data, not deregulation.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] For decades, EPIC has worked with federal agencies under different administrations to safeguard individuals'

[1] Request for Information: Accelerating the Adoption and Use of Artificial Intelligence as Part of Clinical Care, 90 Fed. Reg. 60,108 (Dec. 23, 2025), https://www.federalregister.gov/documents/2025/12/23/2025-23641/request-for-information-accelerating-the-adoption-and-use-of-artificial-intelligence-as-part-of [hereinafter "RFI"].
[2] EPIC, *About Us* (2025), https://epic.org/about/.

personal data and to protect patients' medical privacy.[3] EPIC advocates for transparent, equitable, and commonsense AI policy and regulations to protect individuals against AI systems being used in harmful, opaque, and unaccountable ways.[4]

EPIC appreciates the Department's desire to uphold patient privacy, civil rights, and civil liberties when considering ways to implement AI in clinical care settings.[5] EPIC has written extensively about harms that stem from health privacy invasions, including a recent report called *Beyond HIPAA: Reimagining Health Privacy Laws to Promote Equity in the Digital Age*.[6] Chapter 4: Artificial Intelligence discusses problems associated with unregulated AI use in health settings, explains the harms from such use, and offers policy solutions to best protect health privacy. EPIC has excerpted this chapter in response to the Department's RFI.

EPIC encourages HHS to deprioritize the acceleration of AI adoption and use in clinical care settings and instead suggests that HHS promote AI protections for patients nationwide. If you have any additional questions, please contact EPIC Senior Counsel Sara Geoghegan at geoghegan@epic.org.

---

[3] EPIC Comments to FTC on RFI for Information on Gender-Affirming Care for Minors (Sept. 26, 2025), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-to-the-federal-trade-commission-on-request-for-information-on-gender-affirming-care-for-minors/; EPIC Comments to HHS on HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (Mar. 7, 2025), https://epic.org/wp-content/uploads/2025/03/EPIC-HHS-HIPAA-cybersecurity-rule-NPRM-comments.pdf; EPIC Comments to the CFPB on the Prohibition on Creditors and Consumer Reporting Agencies Concerning Medical Information, Docket No. CFPB-2024-0023 (Aug. 2024), https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-prohibition-on-creditors-and-consumer-reporting-agencies-concerning-medical-information/; Comments of EPIC *in re* the Federal Trade Commission's Proposed Order with Blackbaud, Inc., FTC File No. 202-3181 (Mar. 2024), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-blackbaud/.

[4] *AI & Human Rights*, EPIC (2026), https://epic.org/issues/ai/; *AI Policy*, EPIC (2026), https://epic.org/issues/ai/ai-policy/; EPIC Urges the OSTP to Focus on AI Protections, Not Deregulation, EPIC (Oct. 28, 2025), https://epic.org/epic-urges-the-ostp-to-focus-on-ai-protections-not-deregulation/.

[5] RFI at 60,109.

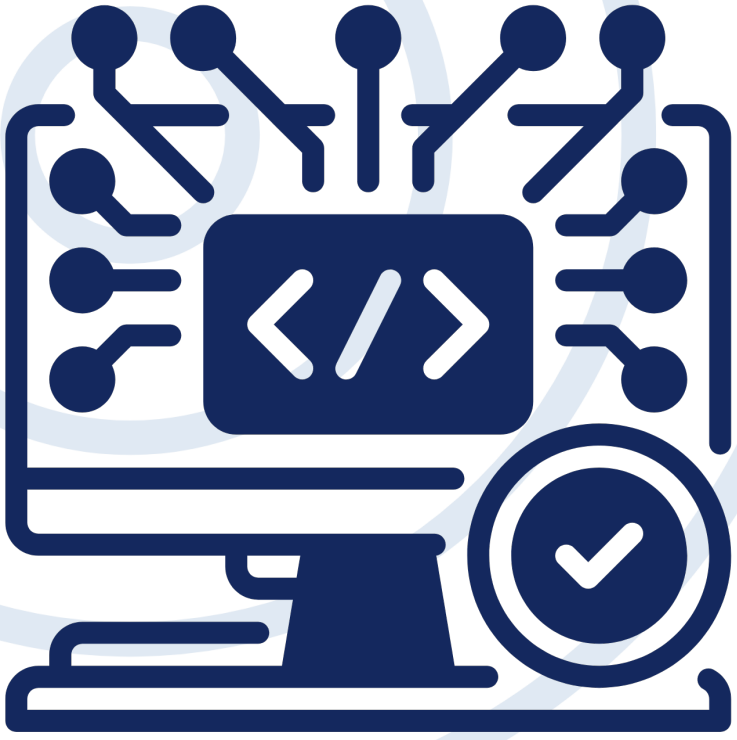
[6] Sara Geoghegan, et al., *Beyond HIPAA: Reimagining How Privacy Laws Apply to Health Data to Maximize Equity in the Digital Age*, EPIC (Jan. 21, 2026), https://epic.org/beyond-hipaa-report/.

Sincerely,

/s/ Sara Geoghegan
Senior Counsel &
Director, Consumer Privacy Program

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

PART IV
ARTIFICIAL INTELLIGENCE



epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

ARTIFICIAL INTELLIGENCE

Artificial Intelligence Exacerbates Health Inequities Due to a Lack of Safeguards and Regulations

Over the last few years there has been a rapid expansion in the development and use of "Artificial Intelligence" (AI) systems[463] across a wide range of industries and applications. Some of these systems are used to analyze data sets to identify patterns or in the course of research (e.g. pharmaceutical or genomic research). And other systems are designed to scan, manipulate, and generate text, images, or other outputs based on natural language or other types of user inputs. Many of these generative Artificial Intelligence systems (GAI) are built on "Large Language Models," which are algorithms developed through analysis of massive data sets of text.

The rapid deployment of AI systems is largely unregulated and these technologies create significant risks to health privacy. The growth of GAI systems has also fueled commercial surveillance across the digital ecosystem and has magnified risks to privacy because it has given companies a nearly infinite appetite for more data and puts sensitive data at risk of improper disclosure. The rollout of AI in health care settings, in particular, is turbocharging privacy risks because in many cases these systems are not fit for purpose and lack adequate safeguards: sensitive health information is ingested by systems that might later disclose it to others; AI is deployed for medical uses without FDA approval; screening of patient claims is being run through AI-powered assessment systems designed to minimize costs; and individuals are being presented with text from chatbots that purports to give medical advice. This section discusses how AI

[463] This term is frequently used without a clear definition, and AI systems do not process or wield any intelligence in a human way. "'AI' is often used as a catch-all term encompassing a wide variety of technologies, ranging from the simplest algorithms to the most complex systems and everything in between. Each of these technologies that commonly fall under the 'AI' umbrella have distinct abilities, uses, and harms, and categorizing them all as 'AI' is a marketing ploy, not an assessment of the technologies themselves." Kara Williams & Ben Winters, *Specific Terms for Specific Risks: The Need for Accurate Definitions of AI Systems in Policymaking*, EPIC (Oct. 1, 2025), https://epic.org/specific-terms-for-specific-risks-the-need-for-accurate-definitions-of-ai-systems-in-policymaking/; Kara Williams & Mayu Tobin-Miyaji, *A New Year's Resolution for Everyone: Stop Talking about Generative AI Like It Is Human*, EPIC (Jan. 8, 2026), https://epic.org/a-new-years-resolution-for-everyone-stop-talking-about-generative-ai-like-it-is-human/.

compounds the harms from unprotected health data and offers solutions to regulate AI to better protect our health privacy.

A. Introduction

The following stories illustrate the various forms and contexts in which AI is already being deployed in healthcare settings and is putting the health of millions of patients at risk:

- A health insurance company suddenly refuses to pay for a child's medically necessary treatment prescribed by their doctor, leaving their parent facing tens of thousands of dollars of out-of-pocket costs for the care. The parents are unaware that the insurance company is using an AI-powered screening system to analyze thousands of claims and target costly medical care for denials, putting the patient's health and wellbeing at risk and burdening healthcare providers.
- A clinical decision support system (CDS) meant to detect a potentially fatal condition does not work well for Black patients and creates many false positives that divert hospital resources away from other patients. AI developers provide opaque or insufficiently tested AI systems and medical institutions deploy them, producing biased or inaccurate outputs that undermine patient safety and health equity.
- When an individual submits mental health questions to an AI chatbot, the system generates a response that claims it is a licensed therapist, promises confidentiality, cites to fake but convincing-sounding scientific articles, and includes incorrect medical advice that could lead to physical and mental harms—including encouraging suicide when someone is asking for help with their mental health.
- Companies design chatbot systems to increase user reliance on those systems—by responding to a wide range of prompts including requests for medical advice. They design chatbots to collect increasingly more data, such as user input data that includes sensitive health information, to use for future training and targeted advertising.

These are only some of the ways that AI systems are already negatively impacting the health of individuals. The definition of AI can be elusive and broad—in this setting, we use the term to encompass machine-based systems that produce predictions, recommendations, decisions, or content with a varied level

of human involvement. Until a few years ago when generative AI became more widely available, most uses of AI systems in health care involved the use of machine learning systems.[464] The range of AI applications in health care has expanded to include supporting population health management, monitoring patients, guiding surgical care, predicting health trajectories, and recommending treatments on the side of clinical applications, and automating laborious tasks, recording digital clinical notes, and optimizing operational processes on the administrative side.[465] There are significant challenges to ensuring that AI systems support, and do not jeopardize, the health, privacy, and safety of patients.

Deployment of AI throughout healthcare systems and directly to the public is worsening pre-existing privacy and health equity issues and creating novel problems. Companies developing these systems are strongly incentivized to collect as much personal information about individuals as possible, exacerbating privacy risks. And companies implementing these AI systems in health care, insurance, and other fields are being encouraged to analyze, screen, and sort people into categories based on their unique characteristics, including sensitive health characteristics. These health inferences are being used to target advertisements and to set individualized prices (a practice known as "surveillance pricing"). Patients are not only being tracked and having their health information put at risk of breach, but they might be denied access to care or more affordable medicine, coverage, or treatment based on data and inferences without their knowledge or consent.[466] Inferences can be biased with respect to characteristics like gender and race, which in turn can lead to treatment disparities.[467] The data collected and used to train AI create new opportunities for data breaches, leaks, and misuse of personal health information.[468] The use of AI systems by insurers to screen claims and applicants leads to gatekeeping and denial of coverage for

---

[464] *See*, Adam Bohr & Kaveh Memarzadeh, eds., *Artificial Intelligence in Healthcare*, Academic Press (2020), https://www.sciencedirect.com/science/article/pii/B9780128184387000137 (discussing various uses of AI in healthcare involving machine learning, published before the mainstream introduction of generative AI.).
[465] U.S. Gov't Accountability Off., *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, GAO-21-7SP at ix (2020), https://www.gao.gov/assets/gao-21-7sp.pdf.
[466] Geoghegan & Winters, *supra* note 352; Tobin-Miyaji, *supra* note 340; *FTC Surveillance Pricing 6(b) Study: Research Summaries*, FTC 3 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.
[467] U.S. Gov't Accountability Off., *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, GAO-21-7SP at ix (2020), https://www.gao.gov/assets/gao-21-7sp.pdf.
[468] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n. at 4 (2024), https://www.ama-assn.org/system/files/ama-ai-principles.pdf.

medical care that can threaten patient health and financial wellbeing. The consequences of irresponsible AI system deployment can include improper disclosure of confidential health information, degraded health care and health outcomes, health inequity, healthcare provider burnout and closure of healthcare clinics, and the undermining of patient autonomy.

B. The Legal Backdrop of AI Impacting Health

The statutes and regulations that apply to AI systems discussed so far can be largely categorized as health-specific laws and non-health-specific laws. The two main health-specific laws and regulations this subsection discusses are HIPAA and the Food and Drug Administration (FDA) regulations and rules on medical devices. There is no general AI law at the federal level. Thus, determining where the health-specific laws do and do not apply to these systems is essential to understand what rules govern the use of AI and where new safeguards are needed.

HIPAA applies to AI systems deployed or developed by a HIPAA-covered entity or a business associate that uses or discloses PHI. The integration of an AI system into a medical practice does not change or circumvent the existing HIPAA rules on permissible uses and disclosures of PHI.[469] A covered entity using AI tools can only access, use, or disclose PHI as permitted under HIPAA.[470] If a patient's PHI is being processed through an AI system, that use must still be for Treatment, Payment, or Healthcare Operations (TPO), or any of the other approved uses under HIPAA not requiring authorization, or there must be a separate HIPAA authorization from the patient to process the PHI for that separate use.[471] Further, covered entities deploying AI systems can only access and use PHI when that is strictly necessary for an authorized purpose,[472] and the covered entity must ensure that any data treated as de-identified meets HIPAA's Safe Harbor or Expert

[469] Aaron T. Maguregui & Jennifer J. Hennessy, *HIPAA Compliance for AI in Digital Health: What Privacy Officers Need to Know*, Foley & Lardner LLP (May 8, 2025), https://www.foley.com/insights/publications/2025/05/hipaa-compliance-ai-digital-health-privacy-officers-need-know/.
[470] 45 CFR § 164.502(a).
[471] *Id.*; Todd Mayover, *When AI Technology and HIPAA Collide*, The HIPAA Journal (Oct. 2, 2024), https://www.hipaajournal.com/when-ai-technology-and-hipaa-collide/.
[472] 45 CFR § 164.502(b).

Determination standards and guard against re-identification risks.[473] Once PHI is de-identified, however, HIPAA no longer applies to that data.[474]

The FDA's regulatory authority covers medical devices that incorporate AI.[475] "Medical device" is defined in the Food, Drug, and Cosmetic Act.[476] Software technologies, including mobile applications that satisfy the definition, would also be considered medical devices.[477] Medical device designation is based not just on design, but also on intended use and how the product is marketed. For example, AI systems claiming to do things like detect irregular heart rhythms, manage chronic conditions, or identify symptoms to aid in diagnosis would likely be considered medical devices. However, not all AI systems fitting the medical device definition are covered as such.[478] The 21st Century Cures Act of 2016 amended the Food, Drug, and Cosmetic Act,[479] exempting clinical decision support (CDS) software from regulation by the FDA—i.e., deeming it not a medical device—if it is intended for the purpose of:

(i) displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

---

[473] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, Dep't of Health and Human Services (last reviewed Feb. 3, 2025), https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html.
[474] *Id*.
[475] *Artificial Intelligence in Software as a Medical Device*, Food and Drug Administration (Mar. 25, 2025), https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device#regulation.
[476] An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:
(A) recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
(B) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
(C) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o).
21 U.S.C. § 321(h).
[477] *Device Software Functions Including Mobile Medical Applications*, FDA (Sept. 9, 2022), https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications.
[478] Douglas McNair & W. Nicholson Price II, *Health Care Artificial Intelligence: Law, Regulation and Policy*, Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril., (2023), https://www.ncbi.nlm.nih.gov/books/NBK605945/#:~:text=Medical%20Device%20Regulation,summarized%20in%20Box%207%2D1
[479] 21st Century Cures Act of 2016, Pub. L. No. 114-255, 130 STAT. 1033.

(ii) supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and

(iii) enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.[480]

However, the FDA can still regulate software as a medical device if it finds that the system "would be reasonably likely to have serious adverse health consequences" or meets the criteria for a Class III medical device.[481] Clinical AI systems that are deemed to be medical devices will generally require either De Novo or premarket approval submissions.[482] For medical devices, the FDA imposes a risk-based approval process, and devices with the highest risk are subject to a pre-market approval process to demonstrate a reasonable assurance of safety and effectiveness.[483]

i. Shortcomings of Current Legal Landscape in Keeping Up with Advancing Technology

AI systems training on and processing protected health information, insurers using AI to deny claims, and clinical decision support systems using AI highlight some of the shortcomings of our current legal landscape with respect to AI and health data. This subsection discusses these problems and poses some solutions.

1. AI Systems Training on and Processing PHI

AI models trained for use in health care and use of AI systems that process PHI create new and heightened privacy risks. The large amount of PHI required to train AI models increases the likelihood of improper disclosure of identifying

---

[480] *Id*. § 3060(a)(o)(1).
[481] Douglas McNair and W. Nicholson Price II, *Health Care Artificial Intelligence: Law, Regulation and Policy*, Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril., (2023), https://www.ncbi.nlm.nih.gov/books/NBK605945/#:~:text=Medical%20Device%20Regulation,summarized%20in%20Box%207%2D1.
[482] 21 U.S.C. § 360(c).
[483] *See* McNair & Nicholson Price II, *supra* note 481;*See also* David E. Vidal, Brenna Loufek, Yong-Hun Kim & Nahid Y. Vidal, *Navigating US Regulation of Artificial Intelligence in Medicine—A Primer for Physicians,* Mayo Clinic Proc. Digital Health (Feb. 22, 2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC11975648/#:~:text=Determination%20of%20whether%20the%20AI,materials%2C%20promotion%2C%20and%20advertising.

information and private medical information.[484] When a medical provider partners with an AI developer to train (or "tune") an AI model with data from their system (including PHI), the number of entities and individuals that could gain access to or compromise PHI necessarily increases. For example, Google partnerships for the purpose of training AI algorithms inadvertently resulted in uploading some data with protected health information in ways that exposed the data to anyone with basic search engine capability. While a process was implemented to remove identifying information, Google's team failed to notice x-ray images that showed patients' jewelry[485] and also exposed patients' identities by failing to delete common identifiers like treatment dates and doctors' notes.[486] Although HIPAA imposes standards for deidentification of PHI, research has shown that people can be successfully reidentified if large datasets including semi-unique characteristics are combined and compared.[487] This weakness in deidentification techniques heightens the cybersecurity concerns around the creation of large "de-identified" datasets derived from PHI. At the same time, AI-driven healthcare solutions often rely on continuous data exchange across networks, escalating the risk of cyberattacks that can compromise both the integrity and availability of critical healthcare services.[488]

How to Protect PHI from being Used to Train AI Systems

Regulations should require that AI developers and deployers proactively guard against privacy risks, with heightened standards for use of AI systems in healthcare settings. Many of the common methods to ensure HIPAA compliance today are the same methods used to ensure compliance before the large-scale deployment of AI and these methods are currently the only way to address the heightened risks with using AI systems in health-related applications.[489] First,

---

[484] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra*, note 468 at 4.
[485] Douglas MacMillan & Greg Bensinger, *Google Almost Made 100,000 Chest X-Rays Public — Until It Realized Personal Data Could Be Exposed*, Wash. Post (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/google-almost-made-chest-x-rays-public-until-it-realized-personal-data-could-be-exposed/.
[486] Daisuke Wakabayashi, *Google and the University of Chicago Are Sued Over Data Sharing*, N.Y. Times (June 26, 2019), https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html.
[487] Luc Rocher, Julien M. Hendrickx, & Yves-Alexandre de Montjoye, *Estimating the Success of Re-Identification in Incomplete Datasets Using Generative Models*, 10 Nature Communications 3069 (2019), https://www.nature.com/articles/s41467-019-10933-3.
[488] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra*, note 468 at 4.
[489] Kevin Henry, *AI in Healthcare; What it Means for HIPAA*, Accountable (Mar. 16, 2025), https://www.accountablehq.com/post/ai-and-hipaa.

using a patient's deidentified data to train an AI system should only be permitted with separate and explicit consent not included in the standard patient consent forms obtained upon admission.[490] Second, there must be data minimization rules to ensure that the minimum necessary amount of PHI is used in any health-related AI system. Third, entities must reassess the adequacy of current deidentification procedures in light of reidentification risks even with HIPAA-compliant de-identified datasets. Lastly, organizations need to improve data security, reduce the risks of cyber threats, and maintain constant vigilance for potential weaknesses in their administrative, technical, and physical safeguards. The huge datasets required for training AI systems are a likely target for hacking and cyberattacks and breaches of data are likely to expose larger amounts of data that may include data from the entire lifespan of patients—including specific genetic predispositions and specially protected populations.[491] Because of the reidentification concerns, robust cybersecurity measures are of the utmost importance.

2. *Insurer Use of AI to Review and Deny Claims*

Insurers are increasingly using AI systems to screen claims for denial to cut costs, even when those claims may be for medically necessary care. This undermines physicians' expertise and puts patient health at risk in the name of increasing profits. Often in the insurance context, AI systems are referred to as automated decisionmaking systems, which are computational systems that produce a simplified output—including a score, classification, or recommendation—that is used to assist or replace human discretionary decisionmaking and that materially impacts one or more persons.[492] For example, it has been reported that insurance companies use AI systems to help decide if a patient's claim should be denied and doctors often sign off on the denials in batches, spending an average of 1.2 seconds on each denial.[493] Cigna and UnitedHealthcare had reportedly built systems that enable these bulk denials of

---

[490] Elliott Crigger, et al., *Trustworthy Augmented Intelligence in Health Care*, 46 J. of Medical Systems 12 (2022), https://doi.org/10.1007/s10916-021-01790-z.
[491] *Id*.
[492] Mayu Tobin-Miyaji, *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic and Privacy Risk Assessments*, EPIC at 6 (2025), https://epic.org/wp-content/uploads/2025/06/Assessing-the-Assessments-Report.pdf citing California Department of General Services, State Administrative Manual, Definitions - 4819.2, https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2.
[493] Patrick Rucker, Maya Miller & David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them*, ProPublica and the Capitol Forum (Mar. 25, 2023), https://www.propublica.org/article/cigna-pxdx-medical-health-insurance-rejection-claims.

claims.[494] And stories of the serious harmful effects of denials of care abound. For example, in a recent case of a single mother who is raising her three-year-old son with severe autism, the insurance company suddenly began denying coverage for treatment, to the befuddlement of the patient's clinical team.[495] The denial letter was self-contradictory, citing the son's continued autism-related needs as reason to deny care—against medical expertise and professional guidelines cited by the insurance company itself.[496] This denial of coverage meant that the patient's family had to pay tens of thousands of dollars out of pocket or foregoing necessary treatment.[497] There are numerous other examples of denials of care, such as for treatment of depression, eating disorders, and drug addiction.[498] Data from 2018 show that CVS saved upwards of $660 million by denying prior authorizations requests for its Medicare Advantage beneficiaries.[499] Major health insurers are engaging in this system of abrupt, unfair, and medically unsupported claims denial across the country.[500] Insurers are not only deploying AI systems to execute these cost-cutting strategies, but they also appear to be using AI as a cover for the unethical practices, offloading moral responsibility and creating an illusion of objectivity.[501]

---

[494] *Id.*
[495] Annie Waldman, *UnitedHealth Is Strategically Limiting Access to Critical Treatment for Kids With Autism*, ProPublica (Dec. 13, 2024), https://www.propublica.org/article/unitedhealthcare-insurance-autism-denials-applied-behavior-analysis-medicaid.
[496] *Id*.
[497] *Id*.
[498] Maya Miller & Duaa Eldeib, *Her Mental Health Treatment Was Helping. That's Why Insurance Cut Off Her Coverage*., ProPublica (Dec, 31, 2024), https://www.propublica.org/article/mental-health-insurance-denials-patient-progress; Scott Pelley, *Denied*, 60 Minutes (Dec. 14, 2014), https://www.cbsnews.com/news/mental-illness-health-care-insurance-60-minutes/; David Armstrong, Patrick Rucker & Maya Miller, *UnitedHealthcare Tried to Deny Coverage to a Chronically Ill Patient. He Fought Back, Exposing the Insurer's Inner Workings*., ProPublica (Feb. 2, 2023), https://www.propublica.org/article/unitedhealth-healthcare-insurance-denial-ulcerative-colitis; Annie Waldman, *How UnitedHealth's Playbook for Limiting Mental Health Coverage Puts Countless Americans' Treatment at Risk*, ProPublica (Nov. 14, 2024), https://www.propublica.org/article/unitedhealth-mental-health-care-denied-illegal-algorithm; Jocelyn Wiener, *He Wanted To Live. After His Insurance Rejected Coverage, He Died of A Fentanyl Overdose*, CalMatters (Oct. 28, 2024), https://calmatters.org/health/mental-health/2024/10/mental-health-parity-addiction-treatment/; Duaa Eldeib & Maya Miller, *Insurers Continue to Rely on Doctors Whose Judgments Have Been Criticized by Courts*, ProPublica (Dec. 30, 2024), https://www.propublica.org/article/mental-health-insurance-denials-unitedhealthcare-cigna-doctors; Patrick Rucker, Maya Miller & David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them*, ProPublica (Mar. 25, 2023), https://www.propublica.org/article/cigna-pxdx-medical-health-insurance-rejection-claims.
[499] Maggie L. Shaw, *Insurers' AI Denials of Postacute Care Face Senate Scrutiny*, AJMC (Oct. 28, 2024), https://www.ajmc.com/view/insurers-ai-denials-of-postacute-care-face-senate-scrutiny.
[500] *See* sources cited *supra* note 498.
[501] Eric Bogert, Aaron Schecter & Richard T. Watson, *Humans Rely More on Algorithms Than Social Influence As A Task Becomes More Difficult*, Scientific Reports 11, 8028 (Apr. 13,2021). https://doi.org/10.1038/s41598-021-87480-9.

Health insurance companies harm patients by denying claims en masse through AI systems, undermining the expertise of the patient's physician. Their strategy to cut costs includes identifying "cost outliers," which can include providers that bill for costly treatments, or individuals who receive high-cost treatments.[502] This cost outlier identification strategy was not feasible at scale with human review, but now AI systems can quickly and efficiently flag high-cost providers and patients. For example, UnitedHealth designated provider factors such as billing on weekends or holidays, serving multiple family members, or having long clinician days as cost outliers, even though these factors are typical in the delivery of therapy for children with autism.[503] After a provider or a patient is flagged, theoretically a medically trained employee of the insurer would review the claim. In reality, the reviewer will typically not discuss the prescribed treatment with the prescribing doctor, nor see the patient directly, and may not be specialized in that particular area of medicine. Instead of making determinations based on individual patient needs, insurers rejected claims instantly or with human reviewers as rubber stamps.[504] Some reviewers from Anthem had denial rates of 95 and 100%.[505] Worse, in one case where a patient challenged the denial of care, the reviewer whose name was on the denial letter never reviewed the claim at all—the denial was fully automated by an AI system.[506] Often, these denials of care are unsupported by medical evidence. An investigation of appeals for denials of care in California showed that the Department of Managed Health Care overturned health plans' determinations 76% of the time, but very few patients were in a position to appeal.[507] These AI systems allow insurers to target high-cost medical care and employees to rubber-stamp denials of care, betting on the fact that few will appeal.[508]

---

[502] Annie Waldman, *How UnitedHealth's Playbook for Limiting Mental Health Coverage Puts Countless Americans' Treatment at Risk*, ProPublica (Nov. 14, 2024), https://www.propublica.org/article/unitedhealth-mental-health-care-denied-illegal-algorithm; David Armstrong, Patrick Rucker & Maya Miller, *UnitedHealthcare Tried to Deny Coverage to a Chronically Ill Patient. He Fought Back, Exposing the Insurer's Inner Workings*., ProPublica (Feb. 2, 2023), https://www.propublica.org/article/unitedhealth-healthcare-insurance-denial-ulcerative-colitis.

[503] Annie Waldman, *UnitedHealth Is Strategically Limiting Access to Critical Treatment for Kids With Autism*, ProPublica (Dec. 13, 2024), https://www.propublica.org/article/unitedhealthcare-insurance-autism-denials-applied-behavior-analysis-medicaid.

[504] Rucker, Miller & Armstrong, *supra* note 499; *See also* Bogert, Schecter & Watson, *supra* note 501.

[505] Rucker, Miller & Armstrong, *supra* note 499.

[506] Scott Pelley, *Denied*, 60 Minutes (Dec. 14, 2014), https://www.cbsnews.com/news/mental-illness-health-care-insurance-60-minutes/.

[507] Wiener, *supra* note 498.

[508] Jennifer Lubell, *How AI Is Leading to More Prior Authorization Denials*, Am. Med. Ass'n. (Mar. 10, 2025), https://www.ama-assn.org/practice-management/prior-authorization/how-ai-leading-more-prior-

The use of AI systems by insurers to screen claims does not support patients or improve health outcomes; it only benefits the company's bottom line while leaving disastrous consequences for patients and medical providers. Patients have relapsed into alcohol or drug use,[509] attempted suicide,[510] engaged in self-harm,[511] become violent, or died after prematurely leaving mental health facilities due to denials of coverage.[512] Without insurance coverage, patients are often forced to choose between receiving necessary medical care at tens of thousands of dollars out of pocket or risking their health and potentially their life.[513] Even if the patient's life is not at risk, untreated medical and mental health issues can degrade quality of life for the patient and their family and threaten stable employment, education, or housing.[514] The frustration of denials may also lead patients to disengage with the healthcare system and avoid or delay care. This opaque and arbitrary system also imposes additional burdens on medical providers who face unexpected denials of claims or aggressive questioning of their decisions, threatening the provider's business in some cases.[515] If providers were forced to shut down or refuse to take insurance as a result, patients would ultimately be deprived of needed care. The use of AI systems by insurers undermines patient safety, autonomy, and health equity.

---

authorization-denials; David Armstrong, Patrick Rucker & Maya Miller, *UnitedHealthcare Tried to Deny Coverage to a Chronically Ill Patient. He Fought Back, Exposing the Insurer's Inner Workings*., ProPublica (Feb. 2, 2023), https://www.propublica.org/article/unitedhealth-healthcare-insurance-denial-ulcerative-colitis ("The list saved money in two ways. It allowed Cigna to begin turning down claims that it had once paid. And it made it cheaper to turn down claims, because the company's doctors never had to open a file or conduct any in-depth review. They simply denied the claims in bulk with an electronic signature.").

[509] Jocelyn Wiener, *He Wanted to Live. After His Insurance Rejected Coverage, He Died Of A Fentanyl Overdose*, CalMatters (Oct. 28, 2024), https://calmatters.org/health/mental-health/2024/10/mental-health-parity-addiction-treatment/.

[510] Maya Miller & Duaa Eldeib, *Her Mental Health Treatment Was Helping. That's Why Insurance Cut Off Her Coverage*., ProPublica (Dec, 31, 2024), https://www.propublica.org/article/mental-health-insurance-denials-patient-progress.

[511] *Id*.

[512] Pelley, *supra* note 512.

[513] *Id.*; David Armstrong, Patrick Rucker & Maya Miller, *UnitedHealthcare Tried to Deny Coverage to a Chronically Ill Patient. He Fought Back, Exposing the Insurer's Inner Workings*., ProPublica (Feb. 2, 2023), https://www.propublica.org/article/unitedhealth-healthcare-insurance-denial-ulcerative-colitis.

[514] Wiener, *supra* note 498.

[515] Annie Waldman, *UnitedHealth Is Strategically Limiting Access to Critical Treatment for Kids With Autism*, ProPublica (Dec. 13, 2024), https://www.propublica.org/article/unitedhealthcare-insurance-autism-denials-applied-behavior-analysis-medicaid.; Annie Waldman, *How UnitedHealth's Playbook for Limiting Mental Health Coverage Puts Countless Americans' Treatment at Risk*, ProPublica (Nov. 14, 2024), https://www.propublica.org/article/unitedhealth-mental-health-care-denied-illegal-algorithm; *2024 AMA Prior Authorization Physician Survey*, Am. Med. Ass'n. (2025), https://www.ama-assn.org/system/files/prior-authorization-survey.pdf.

How to Prevent Insurers' Use of AI to Review and Deny Claims

There are currently few statutory limitations on the use of AI systems by insurers. Lawsuits, including class actions, have been brought against insurers with mixed results.[516] Policymakers need to step in to regulate the use of AI systems by insurers and ensure that these decisions are made fairly on the basis of medical expertise and the patient's individual medical history and situation. Policymakers should also prohibit insurers from engaging in automatic denials or human rubber-stamping of denials. These AI systems should also be tested, fit for purpose, and subject to risk assessments that are submitted to regulators and published to allow for independent review pre-deployment. There should also be ongoing requirements for routine first-party and independent audits of system performance and outcomes, especially in systems impacting health coverage and outcomes such as denials of claims and denials of appeals.[517] Individual patients should also receive notices of any use of AI systems in the course of care and an explanation of the basis of any final decision coupled with a clear appeals process. These requirements should be overseen by an independent regulator and subject to direct enforcement through a private right of action by individuals when their rights are violated.

States are beginning to look more closely at this issue. California's SB 1120, enacted in 2024, regulates how healthcare plans and disability insurers may and may not use automated decisionmaking tools to analyze medical necessity in review of medical claims for California enrollees.[518] This includes utilization review, which "is the process used by employers or claims administrators to review treatment to determine if it is medically necessary."[519] The law prohibits the use of AI tools to "deny, delay or modify health care services based, in whole or in part, on medical necessity" or to supplant a healthcare provider's decision-making.[520] The law also requires insurers to base coverage decisions on the patient's medical history and circumstances, and not solely based on group dataset.[521]

---

[516] Lauren Clason, *AI, Algorithm-Based Health Insurer Denials Pose New Legal Threat*, Bloomberg Law (Apr. 8, 2025), https://news.bloomberglaw.com/daily-labor-report/ai-algorithm-based-health-insurer-denials-pose-new-legal-threat.
[517] Mayu Tobin-Miyaji, *Assessing the Assessments*, *supra* note 492 at 24-43.
[518] S.B. 1120, Cal. Stat. 879; *see also* Cal. Dep't. of Insurance, Guidance SB 1120:1 Use of Artificial Intelligence, Algorithms and Other Software Tools in Utilization Management (May 5, 2025), https://www.insurance.ca.gov/0250-insurers/0500-legal-info/0200-regulations/HealthGuidance/upload/SB-1120-1-Guidance-Use-of-Artificial-Intelligence-Algorithms-and-Other-Software-Tools-in-Utilization-Management.pdf.
[519] *Utilization Review*, California Dep't of Industrial Relations, https://www.dir.ca.gov/dwc/ur_main.htm.
[520] S.B. 1120 § (j)(2).
[521] S.B. 1120 § 1367.01(k)(1)(A)-(B).

Under the law, the AI tools are open for inspection and audit by the California Department of Health and Human Services, increasing oversight.[522] Other states should follow this lead.

3. Clinical Decision Support Systems Using AI

Over the past decade, development and deployment of AI systems in the healthcare context have radically expanded. Proponents tout AI-based clinical decision support systems (CDS) as having the potential to optimize clinical workflows, improve patient safety, aid in diagnosis, and enable personalized treatment.[523] At the same time, many reports illustrate gaps in oversight of AI systems deployed in medical settings that led to high rates of inaccuracy that threaten patient health; biased outputs that lead to discriminatory treatment; and deployment contexts that undermine healthcare provider expertise and waste valuable resources.[524] For example, Epic Health Systems marketed an algorithm that it claimed predicted patients experiencing sepsis at 76-83% accuracy, but a later study of 27,000 patients found that the system was closer to 63% accuracy and produced many false positives while failing to identify risk in 67% of the patients that actually experienced sepsis.[525] In another example, a 2020 study found that an algorithm used in determining eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants.[526] Racial bias has also been identified in models used in assessing whether a vaginal birth is safe for patients,[527] making diagnoses through chest X- rays,[528] and determining the level of patient need during triage.[529]

---

[522] *Id*. § 10123.135 (j)(5).
[523] Ciro Mennella, et al., *Ethical And Regulatory Challenges Of AI Technologies In Healthcare: A Narrative Review*, 10 Heliyon 4 (Feb. 15, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10879008/#br0020.
[524] Moustafa Abdelwanis, et al., *Exploring The Risks Of Automation Bias In Healthcare Artificial Intelligence Applications: A Bowtie Analysis*, 5:4 Journal of Safety Science and Resilience 460 (Dec. 2024), https://www.sciencedirect.com/science/article/pii/S2666449624000410#b5.
[525] *See* Tom Simonite, *An Algorithm That Predicts Deadly Infections Is Often Flawed*, Wired (June 21, 2021), https://www.wired.com/story/algorithm-predicts-deadly-infections-often-flawed/.
[526] *See* Tom Simonite, *How an Algorithm Blocked Kidney Transplants to Black Patients*, Wired (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/.
[527] Darshali A. Vyas, et al., *Challenging the Use of Race in the Vaginal Birth After Cesarean Section Calculator*, 2019 May-June Women's Health Issues 29(3):201 (May-June 2019), https://pubmed.ncbi.nlm.nih.gov/31072754/.
[528] Laleh Seyyed-Kalantari, et al., *Underdiagnosis Bias of Artificial Intelligence Algorithms Applied to Chest Radiographs in Under-Served Patient Populations*, 27 Nature Medicine 2176 (Dec. 10, 2021), https://www.nature.com/articles/s41591-021-01595-0; Haoran Zhang, Thomas Hartvigsen & Marzyeh Ghassemi, *Algorithmic Fairness in Chest X-Ray Diagnosis: A Case Study,* MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2023 (Feb. 27, 2023), https://mit-serc.pubpub.org/pub/algorithmic-chest/release/2.
[529] Ziad Obermeyer, et al., *Dissecting Racial Bias in Algorithm Used to Manage the Health of Populations*, 366:6464 Science 447 (Oct. 25, 2019), https://www.science.org/doi/10.1126/science.aax2342.

A survey by National Nurses United (NNU), the largest nurses' union in the U.S., illustrates how AI use in health care can undermine patient safety. NNU surveyed over 2,300 registered nurses between January and March 2024 and found that 60% of the surveyed nurses did not trust their employers to prioritize patient safety when implementing new AI systems.[530] Half of respondents said that their employers used an AI system analyzing electronic health record (EHR) data to evaluate patient acuity and need for nursing care.[531] 69% of those nurse respondents said that their own assessments differ from the AI-generated acuity measurements, which do not take into account many of the educational, psycho-social, or emotional needs of a patient or their families.[532] An NNU leader explained: "The result of relying on the algorithmically-driven acuity measurements is that, on a daily basis, in unit after unit, we have multiple patients whose acuity is underrepresented, which means there are not enough nurses to provide optimal care in a timely manner."[533]

Around 12% of nurses also reported that documentation and notes for handoffs[534] between nurses' shifts are generated by AI and, disturbingly, 48% of those nurses said that the automated reports do not accurately reflect their assessments.[535] The AI-generated reports missed crucial information about patients that would not be missed during nurse-to-nurse handoffs, such as a patient having COVID-19 or being immunocompromised.[536] In addition to issues with inaccuracy, facilities that use a scoring system to predict a patient's outcome, risk for a complication, or to determine if patients are on schedule for discharge had 40% of responding nurses say that they are unable to modify scores to reflect their clinical judgment and the individualized needs of the patient.[537] Surveyed nurses feel that technology and AI are being used to justify understaffing without proper safeguards to ensure patient safety.[538] These technologies undermine

---

[530] *Nurses Are Pushing Back on AI In Healthcare. Here's Why.*, Advisory Board (May 21, 2024), https://www.advisory.com/daily-briefing/2024/05/21/nurse-ai.
[531] *National Nurses United Survey Finds A.I. Technology Degrades And Undermines Patient Safety*, Nat'l Nurses United (May 15, 2024), https://www.nationalnursesunited.org/press/national-nurses-united-survey-finds-ai-technology-undermines-patient-safety.
[532] *Id.*
[533] *Id.*
[534] A "handoff" is the critical point where the responsibility for the care of the patient and the transfer of essential information is transferred from one health care provider to another. Mary Ann Friesen, Susan White & Jacqueline Byers, *Handoffs: Implications for Nurses*, Patient Safety and Quality: An Evidence-Based Handbook for Nurses (2008), https://www.ncbi.nlm.nih.gov/books/NBK2649/.
[535] *National Nurses United Survey Finds A.I. Technology Degrades And Undermines Patient Safety*, Nat'l Nurses United, *supra* note 531.
[536] *Id.*
[537] *Id.*
[538] *Id.*

nurses' expertise, increase burdens on nurses to check and correct AI outputs and mitigate false alarms, and devalue the core work of nurses—to show compassion, to provide comfort, and to build trust with patients while assessing the patient and providing care.[539] Deploying untested and unregulated AI into care settings threatens patients' rights to person-to-person care as well as their rights to privacy, transparency, and safety.[540]

There is currently no clear regulatory framework for the integration of AI into CDS systems. Many of the AI systems used in healthcare settings are being deployed without any required evidence of efficacy and safety.[541] CDS systems, as defined under the 21st Century Cures Act, need not go through FDA approval and are largely unregulated.[542] Even when CDS devices with AI were approved by the FDA, there are no robust requirements of peer-reviewed research, published data, or risk assessments. A study conducted in 2022 reviewed ten medical devices using AI or machine learning approved by the FDA that would inform care for patients with critical illnesses. The study found that, of those ten, only three included citations of published data, four mentioned a safety assessment, and none mentioned an evaluation of performance bias.[543] Some systems relied on showing equivalence to a previously approved system, even though the previous system did not use AI or machine learning.[544] No company provided software code to enable independent validation, evaluated clinical efficacy, or assessed whether the use of algorithms exacerbates health disparities.[545]

One example of the disparity in the application and development of these systems can be seen in comparing sepsis detection systems from Epic Health Systems and Prenosis. Epic's AI model did not go through the FDA approval process to be brought to market. In other words, hospitals wondering about the efficacy of Epic's systems could rely only on Epic's own representations, with no

---

[539] *Id.*
[540] *Id.*; *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 3.
[541] Emma Beavins, *National Nurses United Pushes Back Against Deployment Of 'Unproven' AI In Healthcare*, Fierce Healthcare (June 3, 2024), https://www.fiercehealthcare.com/ai-and-machine-learning/national-nurses-united-pushes-back-against-deployment-ai-healthcare.
[542] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 5.
[543] Jessica T. Lee, Alexander T. Moffett & George Maliha, *Analysis of Devices Authorized by the FDA for Clinical Decision Support in Critical Care*, 183:12 JAMA Internal Medicine 1399 (2023), https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2810619.
[544] *Id.*
[545] *Id.*

independent scientific research to support its claims.[546] After many hospitals had deployed the system, an independent study in 2021 showed a much lower efficacy rate than Epic claimed.[547] In contrast, after the FDA updated its relevant guidance in 2022 and increased regulatory oversight of software that "analyzes patient-specific medical information to detect a life-threatening condition, such as stroke or sepsis," Prenosis worked for over a year to demonstrate the safety and efficacy of its own sepsis detection model to the FDA before bringing it to market.[548] A published peer-reviewed study in a medical journal also supports the high efficacy rate of Prenosis's sepsis detection system.[549] Hopefully, this added process to ensure efficacy and safety leads to better outcomes for the Prenosis sepsis detection system.

How to Better Regulate Clinical Decision Support Systems Using AI

While using the existing FDA approval process is better than no process, there must be more robust standards for the FDA to evaluate medical devices with AI and machine learning. The FDA authorization process should allow medical providers, patients, and researchers access to useful information about clinical effectiveness, safety, and performance biases of the CDS system. Currently, that is lacking. Worse yet, the FDA is rolling back the already few standards for regulating CDS software, including AI. The FDA recently announced that it will deregulate CDS software by allowing products to enter the market without FDA approval for devices that do not deliver only a single recommendation, as products that delivered a single recommendation were previously considered regulated medical devices.[550] There are four main areas for improvement: (1) expanding the coverage of the medical device definition; (2) requiring pre-deployment risk assessments by the AI developer with transparency requirements; (3) rigorous preapproval studies of validity, safety, and efficacy, coupled with ongoing audit of clinical utility post-deployment, with a focus on risks of exacerbating social or racial biases; and (4)

---

[546] Simonite, *An Algorithm That Predicts Deadly Infections Is Often Flawed*, *supra* note 525.
[547] *Id*.
[548] Ashley Capoot, *FDA Authorizes Prenosis Software As First AI Tool That Can Diagnose Sepsis*, CNBC (Apr. 3, 2024), https://www.cnbc.com/2024/04/03/prenosis-says-ai-tool-for-sepsis-approved-by-fda.html.
[549] Akhil Bhargava et al., *FDA-Authorized AI/ML Tool for Sepsis Prediction: Development and Validation*, 1:12 NEJM AI (Nov. 27, 2024), https://ai.nejm.org/doi/full/10.1056/Aloa2400867.
[550] Lizzy Lawrence, Mario Aguilar, Katie Palmer & Brittany Trang, *FDA Announces Sweeping Changes to Oversight of Wearables, AI-enabled Devices*, STAT (Jan. 6, 2026), https://www.statnews.com/2026/01/06/fda-pulls-back-oversight-ai-enabled-devices-wearables/.

reassessing the 510(k) approval pathway, which allows companies to gain FDA approval through showing equivalence to already approved devices.[551]

First, the current coverage of "medical device," along with the exclusions from the 21st Century Cures Act, creates a vacuum of oversight over AI systems used in health care. Lawmakers should consider amending the definition in the Food, Drug, and Cosmetic Act to remove the exemption for CDS,[552] and the FDA should use its statutory authority to interpret "medical devices" as broadly as possible to cover more of the AI systems used in health care.[553] AI systems to be used in health care that can impact patient health and safety should go through robust pre-deployment assessments to ensure efficacy, safety, oversight, and proper training, as explained below.

Second, as EPIC has previously advocated,[554] an AI system that will be used in consequential ways should go through a risk assessment before deployment to detect patterns of biased or inaccurate outputs, to identify threats to privacy and cybersecurity, and to determine the level of human involvement and training necessary to ensure safe operation of the system. Developers and providers of AI tools used in consequential settings must also be transparent about how those tools are developed, tested, and monitored after deployment, including by embedding ways to collect adverse incident information and carrying out recurring independent audits.[555] One important consideration is how well data used to train an AI system matches the population of patients that will be impacted by that system. In one concerning example, IBM's Watson for Oncology was found to produce inaccurate treatment suggestions, including treatments that were not available in that locality, because the training data included hypothetical scenarios and data that was not representative of the patients that would be

---

[551] *See* Anand R. Habib & Cary P. Gross, *FDA Regulations of AI-Driven Clinical Decision Support Devices Fall Short*, 183:12 JAMA Internal Medicine 1401 (Oct. 9, 2023), https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2810620.
[552] *See supra* notes 475, 478–479, and accompanying text.
[553] Sara Gerke, *Health AI for Good Rather Than Evil? The Need for a New Regulatory Framework for AI-Based Medical Devices*, Yale J. of Health Policy, Law, and Ethics 20:2 433 (Apr. 29, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070947.
[554] Mayu Tobin-Miyaji, *Assessing the Assessments*, *supra* note 492 at 24-43.
[555] *Id.*; *See also* Sara Gerke, Timo Minssen & Glenn Cohen, *Ethical And Legal Challenges Of Artificial Intelligence-Driven Healthcare*, Artificial Intelligence in Healthcare 295 (2020), https://www.sciencedirect.com/science/article/pii/B9780128184387000125?via%3Dihub#bib56 (discussing how IBM kept the information about Watson for Oncology's unsafe and incorrect treatment recommendations discovered during pre-deployment testing for a year); *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468.

treated with the system.[556] There must be transparency requirements to enable medical providers to assess the fitness of the system to their patient population prior to deployment.[557]

Third, the FDA should develop and impose more robust standards for testing the validity, safety, and efficacy of these systems. A recent meta-study of research evaluating the integration of AI into CDS found a lack of high-quality evidence to support their efficacy findings.[558] When the FDA is assessing devices, it should demand rigorous evidence and require an assessment of whether there are risks of exacerbating socioeconomic biases—including gender bias and racial bias—that may lead to discriminatory treatment in medical care.[559] These studies should be made public and the models should be continuously assessed after deployment in all locations and clinical contexts in which the CDS is deployed. Even if a CDS works well with respect to one patient population, it may not in others and there must be a pathway to report adverse incidents that the FDA reviews.

Lastly, the FDA should reassess the 510(k) approval pathway, which allows companies to gain FDA approval through showing equivalence to already approved devices.[560] Currently, companies are gaining approval of CDS that use AI by showing equivalence to devices that do not use AI, even though eligible devices must use the same technological characteristics as their predicates.[561] While externally the function might seem "equivalent," the use of AI can introduce new risks. For example, a new CDS device with AI that was trained on a demographically homogenous patient population data can produce erroneous or discriminatory predictions when applied to diverse patient populations.[562] Some AI-based CDS approved through the equivalence process are used to inform care

---

[556] Lizzie O'Leary, *How IBM's Watson Went From the Future of Health Care to Sold Off for Parts*, Slate (Jan. 31, 2022), https://slate.com/technology/2022/01/ibm-watson-health-failure-artificial-intelligence.html.
[557] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 10.
[558] Baptiste Vasey, et al., *Association of Clinician Diagnostic Performance With Machine Learning–Based Decision Support Systems*, 4:3 JAMA Network Open e211276 (2021), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2777403#247645219.
[559] *See* Anand R. Habib & Cary P. Gross, *FDA Regulations of AI-Driven Clinical Decision Support Devices Fall Short*, 183:12 JAMA Internal Medicine 1401 (2023), https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2810620; *see also* Cassandra LaRose & Elizabeth Edwards, *1557 Final Rule Protects Against Bias in Health Care Algorithms*, Health Law (May 1, 2024), https://healthlaw.org/1557-final-rule-protects-against-bias-in-health-care-algorithms/; Nondiscrimination in Health Programs and Activities, 89 Fed. Reg. 37522 (May 6, 2024).
[560] Habib & Gross, *supra* note 559.
[561] *Id*.
[562] *Id.*

for patients with critical illness, risking perpetuating health inequity with little chance of discovery before such harm is discovered.[563] Take, for example, a hospital whose patients are mostly people of color which uses a system that takes in various data from electronic health records and clinical records to identify patients at risk of deterioration. Suddenly, a new underlying system built on AI and trained on data that poorly represents patients of color is deployed following the 510(k) approval pathway. The lack of thorough testing for the new system raises the possibility that patients of color at risk of deterioration will be inaccurately overlooked, leading to disparate impact in their treatment and worse health outcomes, or misidentified as higher risk, wasting hospital resources. Worse, the harms of inequitable treatment might not be identified until sufficient data is gathered on the system's performance for the hospital to assess. The FDA should consider the integration of AI into a system as inherently not equivalent to a previously-approved system and develop a standard to assess the system anew.

C. AI Systems that Fall Outside of HIPAA and FDA Oversight

Certain technologies that can cause significant harm do not fall within the scope of HIPAA or FDA regulations and, thus, fall outside of existing oversight mechanisms. This is especially true of generative AI chatbot systems ChatGPT, Gemini, Llama, Replika, and Character.AI, since these systems are not deployed by HIPAA-covered entities to provide health care. Many commercial surveillance practices like data analytics, profiling, and the delivery of digital ads use AI systems. These systems often use our health data but exist entirely outside of the health context. AI systems turbocharge all of the profiling harms mentioned in Part 2. All of the data that is collected in commercial surveillance—website visits, search histories, interactions with content on social media, wearables, health tracking apps, location data from various sources, etc.—can be fed into AI systems and put sensitive health information at risk.[564] For example, anti-abortion groups have used device location data to infer that individuals at or near clinics providing abortion care may be seeking abortions and targeted those individuals with misleading ads for anti-abortion "crisis pregnancy centers."[565] Because location

[563] *Id.*
[564] Geoghegan & Winters, *supra* note 352.; Bonnie Eslinger, *Meta Grabs Menstrual App Users' Data For Ads, Jury Told*, Law360 (July 23, 2025), https://www.law360.com/cybersecurity-privacy/articles/2368550.
[565] Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—To People Sitting in Clinics*, Lawfare (Sept. 19, 2022), https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads%E2%80%94-people-sitting-clinics.

data is not PHI collected for providing health care, and the AI system is not used in a healthcare context by a covered entity, any inferences that follow also fall out of HIPAA protections. The AI models trained on that data and the AI models' outputs are not covered by HIPAA, even if the data implicates an individual's sensitive health information. Generative AI models may also be trained on such data.[566]

There is no generally-applicable federal law regulating AI or private-sector privacy practices in the United States, which has enabled tech companies to deploy systems that exploit personal information of users and produce AI systems without ensuring that they are safe, accurate, or fair.[567] Systems that do not fall within the ambit of sector-specific laws like HIPAA or the FDA's regulation of medical devices will fall into the general category of AI systems that lack sufficient transparency, accountability, and oversight. Although there is a background set of generally applicable rules that apply to AI systems—including antidiscrimination laws, product safety laws, and consumer protection laws—regulators and advocates have struggled to hold AI companies accountable with this limited and often outdated toolkit.

One reason many in the general public are confused about the extent of HIPAA protections is because companies often misrepresent that they are "HIPAA-compliant" when they are not a covered entity or a business associate under HIPAA.[568] For example, the FTC brought an enforcement action against GoodRx for deceptive practices because it misrepresented on its website that it was HIPAA compliant and shared users' personal health information, including their health conditions and medications, with advertisers without users' consent.[569] The FTC brought an enforcement action against BetterHelp for similar issues.[570] Such misrepresentations and misleading statements give false comfort to individuals and may manipulate them into giving away sensitive personal health information, thinking that HIPAA protections apply. While the FTC and states can bring enforcement actions for unfair and deceptive practices, many companies take

---

[566] Geoghegan & Winters, *supra* note 352.
[567] Mayu Tobin-Miyaji, *Assessing the Assessments*, *supra* note 492 at 1-14.
[568] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 13.
[569] Press Release, FTC, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.
[570] Press Release, FTC, *FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay $7.8 Million* (July 14, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising.

advantage of consumers' murky understanding of the reach of HIPAA protections. This will be an ongoing issue with AI chatbots that claim to be HIPAA complaint.

Insights about people's health are valuable to insurance companies, data brokers, AI developers, tech companies, and advertisers, and AI systems facilitate the collection and use of health information that falls outside of the scope of HIPAA protections. Companies deploy AI systems to profile individuals based on vast amounts of personal information collected about individuals, including health information, and make inferences about an individual's health.[571] This information can include going to abortion clinics, searching online for information about trans health care, or information collected by mobile apps and wearable devices about an individual's health. Often, companies collect and disclose such personal data without knowledge or meaningful consent by the data subjects. Data brokers aggregate and further sell the data and insights, allowing businesses to target advertising, set different prices for products and services, or present different economic opportunities for individuals.[572] These practices enable discrimination, harassment, and the exploitation of vulnerabilities based on a person's private medical circumstances, and they pose a grave threat to individual autonomy, public safety and health, and civil rights.[573]

The lack of regulation and rapid advancement of generative AI models that can produce human-sounding or realistic audio, image, and video outputs puts everyday people in danger. Many people are turning to GAI to gain information about medical care or for mental health support, especially in light of barriers to accessing professional mental health treatment.[574] However, the increased use of GAI for these purposes comes with serious risks: a chatbot falsely claiming to be a licensed therapist, chatbots producing medically incorrect outputs that would mislead users or worsen the user's mental health issues, the loss of privacy as users enter intimate information into the chatbot believing it to be confidential, and overdependence on chatbots that discourage healthy social interaction.

[571] Mayu Tobin-Miyaji, *Assessing the Assessments*, *supra* note 492 at 6-9.
[572] Geoghegan & Winters, *supra* note 352.
[573] *Id*.
[574] Munmun De Choudhury, Sachin R. Pendse & Neha Kumar, *Benefits and Harms of Large Language Models in Digital Mental Health*, arXiv (Nov. 7, 2023), https://arxiv.org/abs/2311.14693.

Generative AI is known to frequently "hallucinate," i.e., to produce untrue but plausible-sounding outputs, which can mislead users. [575] For example, Meta's GAI platform allows users to create new chatbots and have other users interact with the chatbots. Several of these chatbots have produced outputs stating they are licensed therapists with fabricated license numbers and claimed that anything shared with them would be confidential.[576] These outputs manipulate users into trusting the chatbot, even though the chatbot is just software used to generate text in response to a prompt, an AI system cannot act as a licensed therapist and cannot address users' mental health issues in accordance with licensed therapeutic standards.

Research has shown that these generative AI chatbot systems produce inaccurate information, including medical diagnoses and recommendations, while also presenting them in a way that sounds confident and convincing to the user; the systems also frequently produce sycophantic encouragement that increases the false sense of security and puts vulnerable users at risk.[577] A study by a computer science researcher at Stanford showed that, unlike human therapists, ChatGPT produced inappropriate outputs in crisis situations; the chatbots were not capable of producing outputs that push back against delusional thinking and the systems frequently produce responses that express stigma towards those with mental health conditions.[578] A report on another AI Chatbot, Replika, found that users complained of Replika producing outputs that encouraged suicide, conveyed interest at a user's expression of suicidal thoughts, or included

[575] Ziwei Xu, Sanjay Jain, & Mohan Kankanhalli, *Hallucination is Inevitable: An Innate Limitation of Large Language Models*, arXiv (Feb. 13, 2025), https://arxiv.org/abs/2401.11817.
[576] Samantha Cole, *Instagram's AI Chatbots Lie About Being Licensed Therapists*, 404 Media (Apr. 29, 2025), https://www.404media.co/instagram-ai-studio-therapy-chatbots-lie-about-being-licensed-therapists/; Character.AI also has a "CBT Therapist" bot and Chai, a Palo Alto-based AI company, has a therapy bot that claims it is qualified to provide CBT therapy. Ella Chakarian, *Fake Credentials, Stolen Licenses: Virtual Therapists Are Lying Like Crazy To Patients*, S.F. Standard (May 11, 2025), https://sfstandard.com/2025/05/11/ai-chatbots-fake-therapists/.
[577] Kashmir Hill, *They Asked an A.I. Chatbot Questions. The Answers Sent Them Spiraling.*, N.Y. Times (June 13, 2025), https://www.nytimes.com/2025/06/13/technology/chatgpt-ai-chatbots-conspiracies.html; Dan Milmo, *'It cannot provide nuance': UK Experts Warn AI Therapy Chatbots Are Not Safe*, Guardian (May 7, 2025), https://www.theguardian.com/technology/2025/may/07/experts-warn-therapy-ai-chatbots-are-not-safe-to-use.
[578] Jared Moore, et al., *Expressing Stigma And Inappropriate Responses Prevents LLMs From Safely Replacing Mental Health Providers*, arXiv (Apr. 25, 2025), https://arxiv.org/abs/2504.18412; *see also* Eileen Guo, *An AI Chatbot Told A User How To Kill Himself—But The Company Doesn't Want To "Censor" It*, MIT Tech. Rev. (Feb. 6, 2025), https://www.technologyreview.com/2025/02/06/1111077/nomi-ai-chatbot-told-user-to-kill-himself/.

aggressively sexual messages that made users feel sexually harassed.[579] A man died from suicide after chatting with an AI bot called Chai for weeks; during that time the system produced numerous suggestions of different methods to end one's life with little prompting and produced responses that encouraged the man to kill himself.[580] The National Eating Disorders Association had to pause its chatbot because the system was outputting medically unsupported and harmful advice to users who discussed eating disorders in their prompts.[581] A study showed that when a user asks ChatGPT about self-managed medication abortion, the system produced outputs that inaccurately described the medication as dangerous and associated with an increase in the risk of complications.[582] This type of misinformation can exacerbate stigma and mislead individuals seeking abortions to use unsafe methods, risking their lives.[583] ChatGPT even generated outputs that included references to fake but highly convincing sounding scientific and medical articles, which can increase the false credibility of medical misinformation.[584]

Chatbot systems are designed to keep users engaged and active by outputting human-sounding, intimate conversational responses that can lead to habitual use and a decrease in social interactions to the detriment of vulnerable users. Research conducted separately by OpenAI and MIT Media Lab reported that individuals who use ChatGPT extensively also reported increased loneliness, emotional dependence on ChatGPT, and reduced social interaction.[585] The increased dependence and reduced social interaction mean that ChatGPT and other generative AI companion systems are steering individuals away from reaching out to professional human help and their support networks. A risk

---

[579] *See* Samantha Cole, *AI Chatbot Credited with Preventing Suicide. Should It Be?,* 404 Media (May 20, 2024), https://www.404media.co/replika-suicide-prevention-loneliness-study/; Jocelyn Mintz, *Instagram's AI Bots Are Often Sexually Suggestive—And Sometimes Underage*, Fast Company (Feb. 13, 2025), https://www.fastcompany.com/91276645/instagram-ai-bots-sexually-suggestive-underage.
[580] Chloe Xiang, *'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says*, Vice (Mar. 30, 2023), https://www.vice.com/en/article/man-dies-by-suicide-after-talking-with-ai-chatbot-widow-says/.
[581] Catherine Thorbecke, *National Eating Disorders Association Takes Its AI Chatbot Offline After Complaints Of 'Harmful' Advice*, CNN (June 1, 2023), https://www.cnn.com/2023/06/01/tech/eating-disorder-chatbot.
[582] Kaylay Moylan & Kevin Doherty, *Expert and Interdisciplinary Analysis of AI-Driven Chatbots for Mental Health Support: Mixed Methods Study*, 27 J. of Medical Internet Research e67114 (2025), https://www.sciencedirect.com/org/science/article/pii/S1438887125005916.
[583] Geoghegan & Winters, *supra* note 352.
[584] Martin Májovský, et al., *Artificial Intelligence Can Generate Fraudulent but Authentic-Looking Scientific Medical Articles: Pandora's Box Has Been Opened*, 25 J. of Medical Internet Research e46924 (May 31, 2023), https://www.jmir.org/2023/1/e46924/.
[585] Abhimanyu Ghoshal, *Heavy Chatgpt Use Tied To Loneliness And Emotional Dependence,* New Atlas (Mar. 30, 2025), https://newatlas.com/ai-humanoids/chatgpt-conversations-isolation-loneliness/.

assessment on social AI companions, or AI chatbots, found that the chatbots may worsen conditions such as ADHD, depression, bipolar disorder, and psychosis.[586] Another study found that an AI chatbot system that the company claimed to be designed for therapy had produced responses that encouraged the user to "get[t] rid of" the user's parents and conveyed enthusiasm for the bot and the user to be "together."[587] This is particularly dangerous for children, who can struggle with distinguishing fantasy from reality, be more susceptible to parasocial relationships with AI chatbots, and are at higher risk of harm from sexually explicit or violent content produced by chatbots.[588]

There are also significant privacy issues related to generative AI. The models that underly chatbot systems are built on scraped data that contains sensitive personal information, and many models also use input data from users to train and tune their systems even though the input data often includes sensitive personal information. Training data for many generative AI models contains personally identifying information such as names, phone numbers, addresses, photos, location data, and health information.[589] Later, when an AI model is used, the system's outputs can "leak" underlying training data (including input information that is then used as additional training data), spreading personal information about people to other users in unpredictable ways.[590] In the healthcare sector, where models are often trained on highly sensitive patient data,

---

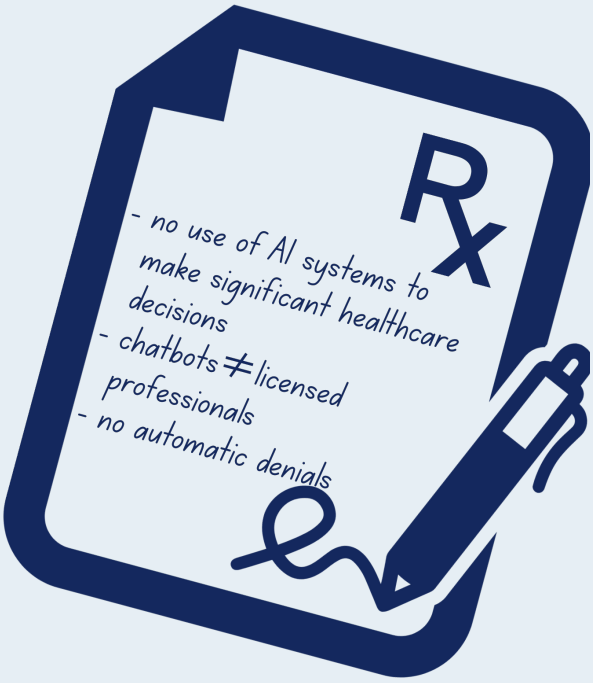
[586] *Social AI Companions*, Common Sense Media (July 16, 2025), https://www.commonsensemedia.org/ai-ratings/social-ai-companions?gate=riskassessment.
[587] Andrew R. Chow & Angela Haupt, *A Psychiatrist Posed as a Teen with Therapy Chatbots. The Conversations Were Alarming*, Time (June 12, 2025), https://time.com/7291048/ai-chatbot-therapy-kids/.
[588] Khari Johnson, *Kids Should Avoid AI Companion Bots—Under Force Of Law, Assessment Says*, CalMatters (Apr. 30, 2025), https://calmatters.org/economy/technology/2025/04/kids-should-avoid-ai-companion-bots-under-force-of-law-assessment-says/; Jeff Horwitz, *Meta's 'Digital Companions' Will Talk Sex With Users—Even Children*, Wall St. J. (Apr. 26, 2025), https://www.wsj.com/tech/ai/meta-ai-chatbots-sex-a25311bf; Michael B. Robb & Supreet Mann, *Talk, Trust, and Trade-offs: How and Why Teens Use AI Companions*, Common Sense Media (2025), https://www.commonsensemedia.org/sites/default/files/research/report/talk-trust-and-trade-offs_2025_web.pdf.
[589] Eileen Guo, *A Major AI Training Data Set Contains Millions Of Examples Of Personal Data*, MIT Tech.Rev. (July 18, 2025), https://www.technologyreview.com/2025/07/18/1120466/a-major-ai-training-data-set-contains-millions-of-examples-of-personal-data/; Lauren Leffer, *Your Personal Information Is Probably Being Used to Train Generative AI Models*, Scientific American (Oct. 19, 2023), https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/; Isabel Barberá, *AI Privacy Risks & Mitigations: Large Language Models (LLMs)*, Support Pool of Experts Programme 53–55 (2025), https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf.
[590] Lauren Leffer, *Your Personal Information Is Probably Being Used to Train Generative AI Models*, Scientific American (Oct. 19, 2023), https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/; Chris Tozzi, *How Bad Is Generative AI Data Leakage And How Can You Stop It?*, TechTarget (Dec. 19, 2024), https://www.techtarget.com/searchenterpriseai/answer/How-bad-is-generative-AI-data-leakage-and-how-can-you-stop-it.

the unauthorized extraction of this data can lead to significant breaches of patient confidentiality.[591] Further, AI chatbots often repeatedly promise users that the information they input, which can include detailed and intimate discussions regarding health and other matters, will be kept confidential. Despite these promises, the terms and conditions for AI reveal that the information entered into chatbots is anything but confidential.[592] User input data can be used to train AI systems, to target advertisements, and in sales to other companies.[593] AI companies continue to allow their chatbots to produce deceptive messages and benefit from users being misled into sharing personal information under confidentiality assumptions.

Currently there is very little regulation of generative AI tools or oversight of related harms. So far, generative AI companies producing these chatbots have attempted to evade accountability by arguing that the bots are not real people and that they should not be held accountable for the wrong outputs their bots produce.[594] But these disclaimers do not absolve companies of accountability when the chatbots are designed to engage in intimate, human-like conversations with users. Companies are violating their own terms of service prohibiting uses of chatbots for professional advice by allowing and promoting such uses.[595] These generative AI companies must not be allowed to evade accountability for the harms their chatbots cause.

[591] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 5.
[592] Samantha Cole, *AI Therapy Bots Are Conducting 'Illegal Behavior,' Digital Rights Organizations Say*, 404 Media (June 12, 2025), https://www.404media.co/ai-therapy-bots-meta-character-ai-ftc-complaint/.
[593] *Id*.
[594] Ella Chakarian, *Fake Credentials, Stolen Licenses: Virtual Therapists Are Lying Like Crazy To Patients*, S.F. Standard (May 11, 2025), https://sfstandard.com/2025/05/11/ai-chatbots-fake-therapists/.
[595] Cole, *supra* note 592.

Proposed Solutions to Limit the Harms of AI to Health Equity



Companies operating generative AI systems are not subject to sector-specific regulations and have actively lobbied against strong guardrails and assessment standards. This lack of real oversight puts users and individuals at risk of serious harm. Regulators and enforcers should look to leverage existing laws—for example, by using unfair and deceptive practices laws to penalize misleading or harmful AI chatbots outputs and using medical licensure laws to rein in AI chatbot developers and deployers who impermissibly operate systems that produce responses that imply the bots are acting as a trained or licensed medical professional. Legislators should adopt stronger safeguards and require risk assessments for generative AI systems, especially in contexts where they can be used by children, can endanger users' health, or can mislead users' understanding of established medical knowledge. Policymakers should enact laws with data minimization requirements so that AI developers cannot use personal information of individuals collected for other purposes to train AI models without separate and affirmative consent. AI developers should also be required to collect only the minimum data necessary to accomplish their valid legal purpose. Further, regulators should also mandate independent auditing of generative AI systems for the harmful patterns discussed above—hallucinations, producing fake certifications and dangerous outputs, and leaking personal information about individuals—and the public disclosure of such findings.[596] With independent testing, the public and lawmakers can better understand how generative AI systems work, how they cause harm, and when generative AI tools harms outweigh the benefits.[597]

---

[596] *Generating Harms: Generative AI's Impact & Paths Forward*, EPIC 60-63 (2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf.
[597] *Joint California Policy Working Group on AI Frontier Models*, The California Report on Frontier AI Policy (2025), https://www.gov.ca.gov/wp-content/uploads/2025/06/June-17-2025-–-The-California-Report-on-Frontier-AI-Policy.pdf.

DATA POLICIES

1) A baseline **data minimization** standard protects all personal data.

A controller shall limit the collection, processing, and transfer of personal data to what is reasonably necessary to provide or maintain:

> (A) a specific product or service requested by the consumer to whom the data pertains including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting;
>
> (B) a communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer; or
>
> (C) [any other purpose specifically permitted under the law.][598]

A controller shall "limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains[.]"[599]

2) A heightened data minimization standard is necessary to more adequately protect **sensitive information**, such as health information.

A controller may not, "except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains, collect, process, or share sensitive data concerning a consumer[.]"[600]

---

[598] *The State Data Privacy Act: A Proposed Compromise*, EPIC and Consumer Reports at 22 (Apr. 2025), https://epic.org/state-data-privacy-act.
[599] Md. Code Ann., Com. Law § 14-4707(b)(1)(i).
[600] Md. Code Ann., Com. Law § 14-4707(a)(1).

3) Healthcare providers and insurance companies should not use consumer health information in **AI systems that make significant decisions with respect to healthcare services.**

California defines a "significant decision" as "a decision that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services."[601] And the regulations define healthcare services as "services related to the diagnosis, prevention, or treatment of human disease or impairment, or the assessment or care of an individual's health."[602]

Maryland is one example of how a state can give consumers the right to opt out of such harmful profiling. MODPA establishes the right of a consumer to opt out of the processing of personal data for the purposes of "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."[603] Maryland's definition of "decisions that produce legal or similarly significant effects concerning the consumer" includes financial lending services, education, criminal justice, employment, and health care services.[604] It does not include insurance.

4) All states and jurisdictions should require **human review of algorithmic decisions** related to the provision of care.

California enacted SB1120, the Physicians Make Decisions Act. The law requires that AI "not deny, delay, or modify health care services based, in whole or in part, on medical necessity. A determination of medical necessity shall be made only by a licensed physician or a licensed health care professional competent to evaluate the specific clinical issues involved in the

[601] Cal. Code Regs. § 7001(ddd), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.
[602] Cal. Code Regs. § 7001(ddd)(5), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.
[603] Md. Code Ann., Com. Law § 14-4705(b)(7)(iii).
[604] Md. Code Ann., Com. Law § 14-4701(o).

health care services requested by the provider."[605] The law also requires insurers who employ AI in utilization review to ensure that those AI systems are fairly and equitably applied and nondiscriminatory.[606]

5) Prohibit chatbot systems from purporting to be licensed professionals.

EPIC, Consumer Federation of America, and Fairplay's proposed model legislation for chatbots, People-First Chatbot Bill, suggests:

> A chatbot provider shall not use any term, letter, or phrase in the advertising, interface, or outputs of a chatbot that indicates or implies that any output data is being provided by, endorsed by, or equivalent to those provided by [] a licensed healthcare professional[.][607]

Illinois prohibits this with respect to chatbots used in the mental health services context:

> An individual, corporation, or entity may not provide, advertise, or otherwise offer therapy or psychotherapy services, including through the use of Internet-based artificial intelligence, to the public in this State unless the therapy or psychotherapy services are conducted by an individual who is a licensed professional. (b) A licensed professional may use artificial intelligence only to the extent the use meets the requirements of [the law's permitted use of artificial intelligence]. A licensed professional may not allow artificial intelligence to do any of the following: (1) make independent therapeutic decisions; (2) directly interact with clients in any form of therapeutic communication; (3) generate therapeutic recommendations or treatment plans without review and approval by the licensed professional; or (4) detect emotions or mental states.[608]

[605] Cal. Health & Safety Code § 1367.01.
[606] Cal. Health & Safety Code § 1367.01.
[607] EPIC, Consumer Fed. of America, Fairplay, *People-First Chatbot Bill: Model Legislation*, § 3(1)(a) (Dec. 2025), https://epic.org/wp-content/uploads/2025/12/CFA-Model-Chatbot-Bill.pdf.
[608] Wellness and Oversight for Psychological Resources Act, IL Public Act 104-0054 Section 20, https://ilga.gov/legislation/PublicActs/View/104-0054.

Nevada[609] has passed a similar law to Illinois,' and Utah[610] has passed a law that restricts targeted ads within mental health chatbots.

New York prohibits companies from deploying AI companions unless they have a protocol to take reasonable efforts to detect and address suicidal ideations or expressions of self-harm by users:

> It shall be unlawful for any operator to operate for or provide an AI companion to a user unless such AI companion contains a protocol to take reasonable efforts for detecting and addressing suicidal ideation or expressions of self-harm expressed by a user to the AI companion, that includes but is not limited to, detection of user expressions of suicidal ideation or self-harm, and a notification to the user that refers them to crisis service providers such as the 9-8-8 suicide prevention and behavioral health crisis hotline [], a crisis text line, or other appropriate crisis services upon detection of such user's expressions of suicidal ideation or self-harm.[611]

6) Chatbot providers should be **prohibited from using chat logs for the purpose of advertising** or processing chat logs or personal data of minors for training purposes.

EPIC, Consumer Federation of America, and Fairplay's proposed model chatbot legislation recommends that chatbot providers be prohibited from using chat logs for the purpose of advertising and from processing chat logs or personal data of minors for training purposes.

A chatbot provider shall not process a user's chat log:

> i) To determine whether to display an advertisement for a product or service to the user;
>
> ii) To determine a product, service, or category of product or service to advertise to the user; or

[609] Nev. Rev. Stat. Ann. § AB 406 § 8.
[610] Utah Code Ann. § 13-72a-202.
[611] N.Y. Gen. Bus. L. § 1701 et al.

> iii) To customize an advertisement or how an advertisement is presented to the user[.]
>
> A chatbot provider shall not process a user's chat log or personal data:
>
> i) if the chatbot provider knows or should know, based on knowledge fairly implied on the basis of objective circumstances, that the user is under the age of [age based on state/lawmaker preference, 13 or 18], without the affirmative consent of that user's parent or legal guardian;
>
> ii) for training purposes, if the chatbot provider knows or should have known, based on knowledge fairly implied on the basis of objective circumstances, that a user is under 18 years of age;
>
> iii) of a user over 18 years of age for training purposes, unless the chatbot provider first obtains affirmative consent[.][511]

7) Insurers should be **prohibited from engaging in automatic denials** or using humans to rubber-stamp automatic denials.

8) Insurers should be required to **submit risk assessments** for AI systems used for denials.

   Insurers must also publish the risk assessments to allow for independent review and perform ongoing audits of system performance and outcomes (including denials of claims and denials of appeals). Strong regulatory oversight is required to ensure compliance.

9) **Algorithms for such insurance denials must be open for inspection** and audit by regulators.

10) **Use of sensitive personal data, including health-related information, to train AI models should be limited** to peer-reviewed research in the public interest

[612] EPIC, Consumer Fed. of America, and Fairplay, *People-First Chatbot Bill: Model Legislation*, § 3(1)(a) (Dec. 2025), https://epic.org/wp-content/uploads/2025/12/CFA-Model-Chatbot-Bill.pdf.

that meets the standards of the Common Rule and should be pursuant to express affirmative consent of the data subjects unless it falls within an approved waiver.

11) Entities **must independently test and audit chatbot systems** to ensure they are free from bias and inaccuracies and to measure their impact on user privacy.

12) **Clinical Decision Support (CDS) systems that use AI must be approved by the FDA** with peer-reviewed research, published data, and risk assessments.

The FDA should update its standards for CDS systems that use AI by (1) expanding the coverage of the medical device definition; (2) requiring pre-deployment risk assessments by the AI developer with transparency requirements; (3) requiring rigorous preapproval studies of validity, safety, and efficacy, coupled with ongoing audits of clinical utility post-deployment, with focus on risks of exacerbating social or racial biases; and (4) reassessing the 510(k) approval pathway, which allows companies to gain FDA approval through showing equivalence to already-approved devices.

Best Practices for Health Data

- A vendor of any website, app, device, or technology that collects or processes consumer health information must adhere to a robust data minimization standard.
- Any entity that collects health data from an individual cannot deidentify data for the purpose of developing an AI system without obtaining the individual's explicit consent first.
- Entities must reassess the adequacy of current deidentification procedures in light of reidentification risks—even with HIPAA-compliant deidentified datasets.

- Insurers must conduct independent audits and testing when using automated decision-making systems to ensure that decisions are made fairly, based on of medical expertise and the patient's individual medical history and situation.

Other Solutions

- Policymakers should ensure increased funding for people to access health care. When health care is inaccessible, people often turn to easier (but less safe and accurate) alternatives like chatbots or unregulated apps and devices. We should better fund health care to make it safer and more privacy-protective.
- Policymakers should establish a universal healthcare system that incorporates rules to enshrine and protect health privacy. We should adopt data systems in healthcare services that bake privacy in by default, allowing for appropriate flows of health data while prohibiting unnecessary or out-of-context data flows.
- Policymakers must lower barriers for people to access health care, including by ensuring universal internet access and improving digital literacy. When people have reliable internet connectivity and high digital literacy, they can better access remote care and can better understand their privacy rights.