BEYOND HIPAA:

REIMAGINING HOW PRIVACY LAWS APPLY TO HEALTH DATA TO MAXIMIZE EQUITY IN THE DIGITAL AGE

epic.org
ELECTRONIC
PRIVACY
INFORMATION
CENTER

ABOUT EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for privacy, algorithmic fairness, and government accountability. Learn more at epic.org.

LEAD AUTHOR

Sara Geoghegan

CO-AUTHORS

Suzanne Bernstein
Alan Butler
Tom McBrien
Mayu Tobin-Miyaji

EDITORS

Hayden Davis
John Davisson
Caitriona Fitzgerald
Calli Schroeder

WITH THANKS TO

EPIC IPIOP Clerks Michelle Ly, Cam Marsh, and Shelby Slotter.

ACKNOWLEDGMENTS

Support for this report was provided by the Robert Wood Johnson Foundation. The views expressed here do not necessarily reflect the views of the Foundation.

CONTENT WARNING

This report discusses harms that arise from commercial surveillance that negatively affect one’s health. This report discusses suicide, self-harm, and eating disorders, and examines how these harms may affect children.

PREFACE

At the time of writing this report, I know that the health data rules and standards described herein can change at the drop of a hat—or rather, the drop of a new judicial opinion, state law, or executive order. People and providers live in a constant state of uncertainty about what is coming next regarding health privacy.

This report summarizes the current legal and technological landscape for health privacy, explains the harms of the status quo, and offers solutions to bring us closer to a more equitable world. Some of the laws and rules discussed may change in the future, but this report is inherently limited to the current landscape in January 2026.

This report has a specific focus: privacy and data protection. It does not attempt to address every facet of our society that may contribute to health inequities. Instead, it focuses on the role that a lack of privacy protections plays in causing and compounding harms to health outcomes.

Will a single unelected district court judge undo the privacy law that has safeguarded health records for nearly three decades? Will a federal agency require a state to turn over teenagers' health records? Which state will win in the battle of shield laws v. prosecutions for telehealth abortion services? Which app or company will face the next big breach affecting their users' health information? How many people will be affected as the federal government seeks to invest in AI systems instead of its people? How many more people will die from the criminalization of abortion care? How many people will forego medical care because they are undocumented?

I do not know the answers to these questions. I do know that the years ahead will bring uncertainty, chaos, and wholly avoidable harm. I also know that this harm will be most acutely felt by the most vulnerable among us. I hope this report can offer some ideas for a safer, freer, more privacy-protective future in which the wellbeing of all people is prioritized over the interests of a few powerful companies.

– Sara Geoghegan, Senior Counsel

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Unregulated digital technologies, mass surveillance, and weak privacy laws have created a health privacy crisis in which our health data is collected and used to profile us, manipulate our behavior, and charge us more for care. Commercial surveillance fuels practices that push people away from care, including criminalization, constant online tracking, unregulated use of unsafe AI systems, and massive data breaches. These privacy invasions harm certain people disproportionately and worsen inequities. We need stronger legal and technical protections for health data, especially sensitive information such as children's health data. This report provides an overview of the health privacy crisis we face, explains how it negatively impacts health equity, and proposes solutions for a better, safer, and more privacy-protective future.

Here are a few key takeaways from this report:

- A better world is possible, and these privacy breaches are not inevitable. We can build systems and improve standards to protect our health data. Health privacy abuses and breaches put vulnerable communities at risk and discourage them from seeking care; privacy protections can improve health equity and outcomes.
- Commercial surveillance and the health privacy crisis disproportionately impact marginalized communities. These invasive data practices erode trust among overpoliced groups and discourage people from seeking care. Delayed or deferred care worsens health outcomes because health conditions often become more severe when left untreated. Privacy should be baked into health systems and shouldn't be treated as a luxury good.
- When it comes to sensitive health information, policymakers and industry leaders should embrace a data minimization approach. If we limit the collection, processing, sharing, and retention of personal information to what is necessary to provide health services, we will protect privacy and promote health equity.
- One especially pernicious practice is the sale of sensitive health data. This harmful practice should be banned, and the focus of health and health-

related industries should be on providing quality care to improve health outcomes, not on harvesting and monetizing people's data.

- Our health privacy standards need to be updated to meet the moment. Technology has shifted dramatically over the last thirty years, but we don't have legal protections to keep pace. Instead, our health data is increasingly being harvested, sold, and used beyond our control, creating a health privacy crisis. Recent trends of criminalized care, Medicare cuts, and the rise of government intrusion into medical care force people to delay care, worsening their health.

- The ubiquitous tracking and profiling of consumers—which is based in part on our health data—leads to and exacerbates health inequities. Data brokers and the companies that profile us (especially for the purpose of targeted advertising) exploit our health data to manipulate us into buying more—and more expensive—products and to charge us more for care.

- Data breaches negatively impact our health because when a person's sensitive information is breached, they suffer from anxiety and stress and can lose trust in their providers. It costs time and resources to remedy a breach, so its impacts are most acutely felt by marginalized communities.

- The proliferation of artificial intelligence exacerbates the health privacy crisis. These technologies are rapidly being deployed in healthcare settings without adequate safeguards. Apps, chatbots, websites, and devices that use AI for health-related purposes typically do not meet FDA standards for medical devices. These systems are also increasingly used in medical and insurance contexts without rigorous testing for accuracy, efficacy, bias, and privacy.

- Commercial surveillance harms the health and wellbeing of minors online in unique ways. Minors are more susceptible to harms caused by chatbots, targeted advertising, profiling, addictive feeds, and engagement-maximizing platform design.

health equity

noun / as defined by the **World Health Organization**

"the absence of unfair, avoidable or remediable differences among groups of people, whether those groups are defined socially, economically, demographically, or geographically or by other dimensions of inequality (e.g. sex, gender, ethnicity, disability, or sexual orientation) [...] [h]ealth equity is achieved when everyone can attain their full potential for health and well-being."[1]

health equity

noun / as defined by the **National Cancer Institute**

a "situation in which all people are given the chance to live as healthy a life as possible regardless of their race, ethnicity, sex, sexual orientation, disability, education, job, religion, language, where they live, or other factors."[2]

health equity

noun / as defined by the **American Medical Association**

"assurance of the conditions for optimal health for all people. Achieving health equity requires valuing all individuals and populations equally, recognizing and rectifying historical injustice, and providing resources according to need."[3]

[1] *Health Equity*, World Health Organization, https://www.who.int/health-topics/health-equity.

[2] NCI Dictionary of Cancer Terms, *Health Equity*, Nat'l Cancer Inst. at the Nat'l Insts. of Health, https://www.cancer.gov/publications/dictionaries/cancer-terms/def/health-equity.

[3] *What Is Health Equity?*, AMA (July 2022), https://www.ama-assn.org/public-health/health-equity/what-health-equity quoting Dr. Camara Jones, *Systems of Power, Axes of Inequity, Parallels, Intersections, Braiding the Strands*, Medical Care (Oct. 2014), *available at* https://journals.lww.com/lww-medicalcare/Fulltext/2014/10001/Systems_of_Power,_Axes_of_Inequity___Parallels,.12.aspx.

INTRODUCTION

Privacy protections for health data promote health equity by establishing safeguards, protocols, and standards to ensure the integrity of personal information and prevent unauthorized or unintended uses. The purpose of these protections is to ensure that individuals have both the ability to control what happens with their data and the assurance that they will not be subject to unfair and invasive data practices. One example of a technical privacy protection for individuals is a web browser that prevents third-party tracking. But these protections should also include systemic safeguards, like a comprehensive data privacy law that limits the collection, use, and retention of personal data to what is necessary for the product or service a person requests.

Woven throughout these protections are societal and cultural understandings about privacy. Some people may feel more comfortable exchanging sensitive information among family members than others, and some people may distrust sharing information with law enforcement more than others. Beliefs about what and how personal information should be protected can influence how privacy protections are shaped and enforced. Big Tech has spent decades and countless millions pushing the narrative that diminished privacy is a tradeoff necessary to enjoy the benefits of new technology; that privacy stifles innovation; and that there are no downsides to companies constantly collecting and selling our information. Our understanding of what privacy protections are possible and workable has been limited by Big Tech's influence. But despite Big Tech bombarding us with this narrative, people still prefer stronger privacy protections. And we can build safer systems that are compatible with emerging technologies, that encourage innovation and competition, and that protect the basic dignity of all people.

A technology system that lacks robust privacy protections imposes inequitable costs on people in the system. Certain data uses can harm a specific group of people more than others. For example, a documented citizen may not worry about government access of their location information in the same way that an undocumented immigrant would. Domestic violence survivors may fear their information being sold by a data broker in ways that non-survivors do not. People of color may be harmed by digital redlining, the practice of perpetuating inequities among marginalized communities using technology and the internet. Women and girls, LGBTQ+ people, people of color, and other marginalized populations may fear cyberstalking, doxing, and harassment online more than straight, white cis men do. A data breach that exposes a queer person's sexuality may be riskier than for a straight person. Overpoliced communities may fear facial recognition technology, especially inaccurate facial recognition technology, more than others.

Moreover, these harms often hit hardest for people who lack the resources to mitigate them. For example, if a person is doxed but can easily afford a service that monitors their digital presence and removes harmful content, the harm they suffer may be less acute than for a person who cannot afford the service. If two people are charged higher prices for a medical device based on their recent search histories (a practice known as surveillance pricing), but one person is wealthy and can afford the higher price while the other person cannot, the result is inequitable: the latter person is less likely to experience favorable health outcomes due to resource disparities.

But we can build a better world. Legislators and regulators can protect our health information by enacting data minimization standards that limit the collection, disclosure, and retention of personal information to that which is strictly necessary to fulfill the product or service requested by a person. We can limit our health information from being used in harmful ways like profiling and surveillance advertising. We can restrict data brokers' access to our health data which is often used against us to charge us more for care. We can regulate emerging technologies to ensure that they are safe and that their purposes benefit us, not exploit us. We can create standards and regulations to protect our health privacy, promote trust in health services, and reduce health inequities.

This Report

This report provides background on the health privacy crisis and contains five parts that detail how it worsens health outcomes and health equity. We also suggest policy solutions to solve the health data privacy crisis and improve health equities.

Background

The Health Information Portability and Accountability Act (HIPAA) provides strong protections for a narrowly scoped category of health-related information. Today's commercial surveillance ecosystem enables the collection of vast swaths of health-related data that fall outside of the scope of HIPAA. Some state laws, like Washington's My Health My Data Act, provide strong protections for consumer health-related data that fall outside of the scope of HIPAA. But a sectoral approach to privacy falls short of adequately protecting all people.

Part 1: Direct Impacts

The U.S. Lacks Privacy Protections for Health Information, Worsening Health Outcomes and Inequities

The lack of privacy protections for health information directly leads to health inequities. While technologies that over collect, share, and process our personal information have proliferated, laws and standards to protect that information have lagged. Worse yet, federal attacks on marginalized communities and criminalization of certain forms of health care have made care more difficult to obtain. These invasions of privacy worsen health outcomes, and the harms are most acutely felt by marginalized communities.

Part 2: Profiling

Commercial Surveillance and Profiling Cause Privacy Harms, Undermine Our Autonomy, and Worsen Our Health Outcomes

Commercial surveillance is a system in which consumers are ubiquitously tracked and profiled online, based in part on our health-related information. This system leads to and exacerbates health inequities. Data brokers and the companies that profile us exploit our health data largely for the purpose of targeted advertising. This use of our health data manipulates us to buy more—and more expensive—products, which collides with our societal understanding that health is private. When our health data is implicated in this system, it can lead to digital discrimination, higher prices for care, inaccurate information and diagnoses, and a feeling of distrust from being profiled.

Part 3: Data Breach

Data Breaches Worsen Health Equity Because They Cause Fear and Mistrust in Healthcare Systems and Require Resources to Remedy

Data breach itself constitutes a negative health outcome. When a person must respond and adapt to the breach of their sensitive personal information, it can cost money and time and lead to anxiety, depression, and mistrust.

Part 4: Artificial Intelligence

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

Artificial Intelligence (AI) and generative Artificial Intelligence (GAI) systems turbocharge the harms from commercial surveillance and present special considerations. AI and GAI have changed rapidly in recent years; many people now use consumer-facing large language model systems to seek medical advice. Apps, chatbots, websites, and scientific research incorporate AI, but many of these uses have not followed the standards set for medical devices established by the Food and Drug Administration (FDA). Automated decision-making systems are deployed in medical and health insurance contexts without rigorous testing for accuracy, efficacy, bias, and privacy.

Part 5: Minors' Health Privacy

Social Media and Other Digital Platforms Harm Minors' Health and Wellbeing in Unique Ways

Commercial surveillance and the general lack of privacy protections for health data can adversely affect minors' physical and mental health in different and more acute ways. Minors have unique vulnerabilities to certain technologies as they progress through different developmental stages. Chatbots, targeted advertising, addictive feeds, and engagement-maximizing platforms have an outsized impact on minors and can lead to psychological harms, eating disorders, self-harm, discrimination, and difficulty developing a sense of autonomy and personality.

Each part in this report includes: (1) examples of how the privacy harms discussed impact people, worsen their health outcomes, or contribute to health inequity; (2) descriptions of the legal and technological changes that have given rise to today's health privacy crisis; (3) an exploration of how this status quo undermines health equity; and (4) proposed solutions to mitigate harms, build a more privacy-protective future, and promote health equity.

BACKGROUND

epic.org
ELECTRONIC
PRIVACY
INFORMATION
CENTER

BACKGROUND

Unregulated Technologies, Mass Surveillance, and Weak Privacy Laws Have Created a Health Privacy Crisis

As technology has evolved (and the law has stagnated) over the last three decades, our health data has been increasingly exposed and put at risk. This erosion of privacy protection has created significant health inequities. The digitization of records and rapid expansion in network capacity over this period have delivered a data ecosystem that is larger than the most expansive predictions in the pre-digital era. And most of the data collection in these system falls outside of the narrow privacy regulations created in the 1980s and 90s.

When Congress enacted the seminal health privacy law to address the digitization of health records in the late 90s, the Health Insurance Portability and Accountability Act (HIPAA), it sought to address some issues related to the digital transition of traditional medical records (including privacy). But HIPAA was not drafted to address issues raised by the widespread collection of health-related data by myriad devices today—smartphones, wearables, and the internet have generated vast amounts of data that can reveal our health information, most of which is not covered by HIPAA. Indeed, most of the information collected online today falls outside of the scope of *any* federal data privacy law. Some states, like Washington, have passed laws to protect the privacy of individuals' health information—largely in response to the onslaught of harms from unraveling privacy protections at the federal level.

The background of this report contains two sections: (1) Key Concepts and (2) Legal Landscape. The Key Concepts explain that patient privacy is an ancient concept, describe how unregulated commercial surveillance has created a health privacy crisis, illustrate why this crisis is urgent, and propose a data minimization standard to address this crisis. The Legal Landscape section discusses HIPAA, HIPAA's limitations, and state laws that affect health privacy and explain how these laws have not protected our health privacy sufficiently.

A. Key Concepts

i. *Patient Privacy is an Ancient Concept*

It has been a bedrock assumption for centuries that health privacy is necessary to the proper furnishing of healthcare services. Patient-provider confidentiality illustrates this understanding. In the medical setting, confidentiality is "the principle of keeping secure and secret from others, information given by or about an individual in the course of a professional relationship," and every patient has this right.[4] The core tenet of patient privacy and confidentiality in health care is ancient. In the Fifth Century B.C., Ancient Greek physicians pledged:

> What I may see or hear in the course of the treatment or even outside the treatment in regard to the life of men, which on no account one must spread abroad. I will keep to myself holding such things shameful to be spoken about.[5]

The notion that patient privacy is essential persists today. Failing to protect a patient's confidentiality undermines their trust and may prevent a person from seeking needed help.[6] Indeed, "[c]onfidentiality preserves individual dignity, prevents information misuse, and protects autonomous decision making by the patient."[7] When a person feels safe in sharing sensitive health information with a provider, the provider is able to give them a more accurate assessment. Facilitated by the secure exchange of information, a provider may identify a potential problem before it worsens and reach a diagnosis with ample time for treatment. Providers may also help to prevent diseases and disorders before they develop when a patient is able to share their health information more fully.

Consider a (hypothetical) college freshman named Justin. He has recently come out of the closet to his closest friends and begins dating men. When he goes home for fall break, he sees his doctor—a family friend—for his annual checkup. The doctor asks if he is sexually active, with whom, and with how many partners. Worrying that the doctor might tell his parents, Justin responds "no." He

[4] Julius Bourke and Simon Wessely, *Confidentiality*, BMJ (Apr. 2008), https://pmc.ncbi.nlm.nih.gov/articles/PMC2323098/.

[5] *Hippocratic Oath (Fifth Century B.C.), reprinted in Encyclopedia of Bioethics 2632*, Univ. of Minn. Human Rights Library (Warren Thomas Reich et al. eds., 1995), https://hrlibrary.umn.edu/instree/hippocratic.html.

[6] Bourke and Wessely, *supra* note 4.

[7] *Id.*

returns to school and continues to date men, having multiple sexual partners over the next few years. After college, he moves away and sees a new doctor. He is honest with the new doctor about his sexual history and the doctor prescribes him PrEP, noting that he is glad Justin is HIV negative, but explains that he should have been on the preventative drug years ago to best protect his health.

People are more honest with their healthcare providers when they trust them, and they trust providers when they know their providers will respect their privacy. Similarly, people will be able to make best use of health-related apps and services when they can trust that their data will be protected. When a person is more active in pursuing health-related services, they experience improved health outcomes.

ii. Commercial Surveillance, Lagging Privacy Laws, and Rising Authoritarianism Have Created a Health Privacy Crisis

Our technological and legal realities have created a landscape that undermines the ancient understanding that patient privacy is a core tenet of health care. The unchecked rise of commercial surveillance over the past three decades has created new risks that health information will be collected, shared, and sold outside of the context of the traditional patient-provider relationship. Apps, wearable devices, websites, smartphones, and other systems continuously collect information that can reveal health characteristics about us. Even many webpages for booking doctor's appointments are riddled with third party tracking technologies that collect information about a person without their knowledge. Data brokers trade in our information, some specifically in health data, to build profiles about us and target us with ads. In real time, entities can collect and transmit our location information—even when it reveals that we are at a medical facility. Commercial surveillance harms marginalized communities the most, increasing inequities through digital black boxes and opaque algorithms.

While these data collection practices have proliferated on a mass scale, laws have failed to keep pace to protect our health information from commercial surveillance. The bedrock principle of privacy in health care has been left behind because our lawmakers have failed to act. And recent trends have significantly exacerbated risks to health privacy. Over the last ten years we have seen alarming developments that directly threaten the privacy of health information, including: (1)

the attack on and criminalization of certain health-related activities; (2) law enforcement access and use of health information for non-health prosecutions; (3) Medicaid rollbacks, and (4) the recent federal data demands.

The federal health privacy law, the Health Information Portability and Accountability Act (HIPAA), was enacted by Congress in 1996 and is limited to information shared in the traditional patient-provider context. Accordingly, most of the health information implicated by the commercial surveillance ecosystem falls outside of its scope and remains unprotected. As a result of this mismatch, it can be very confusing to determine whether health related information is protected under current law. Some states have passed laws creating broader protections for health information while other states have criminalized health care like abortion and gender affirming care. Federal infrastructure for data sharing, research, and promoting public health has changed dramatically.

The surest way to safeguard against privacy risks and to protect people's health information from being weaponized is to establish legal privacy standards applicable to all settings and technologies. This report proposes solutions that, if adopted, would ensure that the privacy of our health data is protected by default. In turn, this will promote better health outcomes and reduce health inequities.

iii. The Health Data Privacy Crisis Is Urgent

The health privacy crisis has escalated to a breaking point. The harms are not merely hypothetical or theoretical. People experience the effects of the broken health privacy system daily. We live in a time where the rule of law hangs in the balance, and living a single court decision or executive order away from peril can cause extreme distress. Government overreach and criminalization deters people from sharing their information in ways that are meant to help them, and the law gives them inadequate protection when they do. If people don't feel protected by their government and providers, why would they share their information? Fear, stigmatization, and mistrust contribute to worse health outcomes. In a reasonable risk-reward calculation, people retreat from engaging fully in a health system out of fear. When teenagers in Florida worry that their health records will be used against them, or people's menstrual information isn't sufficiently protected by an app, people experience a breakdown of trust in the system.

Abusive data practices are particularly harmful when they implicate our most sensitive information: our health data. People can die when they are unable to obtain health care. And many people are rightfully fearful of seeking care due to criminalization and stigma that could result if their information is disclosed or leaked or breached. And these risks go beyond the doctor-patient relationship. Individuals can be charged higher prices for goods and services based on their digital history, which can lead to higher prices for medicine and health care. Communities may experience anxiety or mistrust because our systems have not been designed to protect them, and these feelings may be reproduced and reinforced over time. All of these harms are most acutely felt by marginalized communities, and our current data privacy landscape contributes to, and reinforces, these health inequities.

There's no shortage of news stories highlighting the imminent need for better health data protections. Consider these recent examples.

23 and Me: Which billionaire will buy my DNA? Will my kids be impacted?

Take the recent example of 23andMe's bankruptcy proceeding. Millions of customers were left in the lurch when they discovered that the company was heading for bankruptcy and that their genetic information might be sold off to the highest bidder in the proceeding. Customers expressed concern about the unknowns: who would have access to their DNA, why would they want it, how would they protect it, and is there anything they can do?

For many customers, fears arose when they learned that HIPAA did not protect their genetic information and that the company's Terms and Service, not a privacy law, governed what would happen to their sensitive data. Companies like 23andMe craft privacy policies and terms of service to explain what the company plans to (or reserves the right to) do with their information. Generally, these policies are written broadly containing disclaimers that provide few, if any, enforceable limits on the collection, use, sharing, and retention of a customer's personal information. 23andMe's bankruptcy underscored how this system, known as "notice and choice" or "notice and consent," fails to protect individuals. A company can change the terms of its policies unilaterally at any time and privacy policies allow for a new company's policies to take over in the event of a bankruptcy, merger, or acquisition.

When customers began to submit their swabs to 23andMe in 2007, they could not have anticipated all of the ways their genetic information—which is immutable and can implicate family members—would be used in the future. And they certainly could not have anticipated that 23andMe would sell their data to the highest bidder. Technology and commercial surveillance have expanded so radically and in such a short amount of time. For example, reidentification techniques which allow for a person's data to be tied back to them even though it's been "anonymized" have become more capable with time and larger datasets. This means that there is a higher risk that a person could be identified when their genetic information is shared, even if nominally anonymized. Large language models and generative AI are technologies the average customer could not have predicted so many years ago.

These unforeseeable uses, coupled with many costumers' reasonable belief that their sensitive health information was protected by law, meant that customers' reasonable expectations of privacy were undermined by the bankruptcy. Some people feared discrimination, biometric surveillance, identity theft, blackmail, and law enforcement access of their genetic information.[8] Without substantive limitations on how this data could be shared, customers panicked and scrambled to learn how to delete their information. In the meantime, state courts had to step in to build safeguards after the fact by appointing a privacy ombudsman to attempt to review the proposed bankruptcy sales.

ICE at the ER: A Nightmare for Patients' and Providers' Safety, Privacy, and Wellbeing

A poignant example underscoring why this crisis needs to be addressed urgently is the increased presence of Immigration and Customs Enforcement (ICE) agents in hospital settings. While fears of law enforcement are not new to immigrant communities, President Trump launched an unprecedented attack on undocumented immigrants early into his second presidency. His administration has called for expanded efforts to surveil and deport immigrants which increased the presence of ICE officers at sensitive places like churches, schools, and

[8] Justin Sherman, EPIC Scholar in Residence, *Bankrupt Genetic Data: Minimizing and Privacy-Protecting Data from the Start*, EPIC (Apr. 14, 2025), https://epic.org/bankrupt-genetic-data-minimizing-and-privacy-protecting-data-from-the-start/; Kevin Williams, *23andme Bankruptcy: With America's DNA Put On Sale, Market Panic Gets A New Twist*, CNBC (Mar. 30, 2025), https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html.

hospitals.[9] Previously, the Department of Homeland Security (DHS) had guidance that required ICE officers to refrain from immigrant enforcement in sensitive locations.[10] President Biden's administration had expanded this definition to include healthcare facilities, schools, places of worship, places where children gather, social services establishments (such as domestic violence shelters), disaster/emergency response sites, weddings, funerals, religious ceremonies, parades, demonstrations, rallies, and courthouses.[11] On his first day in office, President Trump revoked this policy to allow ICE to enter facilities like hospitals more easily, promising to carry out the largest deportation operation in American history.[12] The new presence of ICE at hospitals has horrified patients and providers alike and threatened the bedrock principle of confidentiality in health services.

ICE's presence at medical facilities prevents patients from obtaining care, violates patients' privacy rights, and worsens public health outcomes. ICE agents have occupied emergency rooms, hospital waiting rooms, and hospital lobbies—even standing behind reception desks.[13] "We have a level of privacy that we owe to patients and their families, and that has just been completely demolished with all of the involvement of ICE coming into hospitals," said one California ICU nurse.[14] This presence has directly prevented health workers from treating patients. ICE detainees must be provided medical services, so agents bring patients into hospitals for medical clearance.[15] Dr. Céline Gounder, a public health expert, said "it is creating an atmosphere of fear. And my colleagues and I have

[9] Rebecca Santana, *Trump Administration Throws Out Policies Limiting Migrant Arrests At Sensitive Spots Like Churches* (Jan. 21, 2025), https://apnews.com/article/immigration-enforcement-sensitive-locations-trump-ab0d2d2652e9df696f14410ebb52a1fc.

[10] Lynn Damiano Pearson, *Factsheet: Trump's Recission of Protected Areas Policies Undermines Safety for All*, Nat'l Immigrant Law Ctr. (Feb. 26, 2025), https://www.nilc.org/resources/factsheet-trumps-rescission-of-protected-areas-policies-undermines-safety-for-all/; Santana, *supra* note 9.

[11] Damiano Pearson, *supra* note 10.

[12] Camilo Montoya-Galves, *Trump Officials Revoke Biden Policy That Barred ICE Arrests Near "Sensitive Locations" Like Schools And Churches*, CBS (Jan. 21, 2025), https://www.cbsnews.com/news/trump-immigration-ice-arrests-sensitive-locations/.

[13] Ana B. Ibarra and Kristen Hwang, *ICE Is Suddenly Showing Up In California Hospitals. Workers Want More Guidance On What To Do*, Cal Matters (Aug. 26, 2025), https://calmatters.org/health/2025/08/immigration-hospitals-workers-fear/.

[14] *Id.*

[15] Sara Moniuszko, *Doctors Fear ICE Agents In Health Facilities Are Deterring People From Seeking Care*, CBS (July 9, 2025), https://www.cbsnews.com/news/doctors-fear-ice-agents-health-care-facilities-deterring-people/.

had numerous patients tell us that they hesitated or waited too long to come in for health care."[16]

Delays in care can have grave consequences: when heart attack or stroke are not treated timely, a patient can suffer from more loss of tissue.[17] One nurse reported that an ICE agent blocked her from treating a patient who was screaming in the emergency room, and the agency refused to give his name, badge, or present a warrant when asked.[18] "They're interfering with patient care," she said.[19] Nurses have reported that ICE agents have listened in on conversations between patients and health workers, which constitutes a HIPAA violation, and expressed concerns that patients will not receive necessary care when taken by ICE.[20] Certainly, some undocumented people will not seek much needed care to avoid ICE, which will worsen their health.

In response to the administration revoking the guidelines that had previously prevented ICE's presence in hospitals, National Nurses United said:

> Our patients, with whom we make a sacred oath to help and heal, without discrimination, should never be forced to forego lifesaving treatment because our government has made our workplaces sites of harm and terror. Still so fresh off the deadliest months and years of the Covid-19 pandemic, and in the midst of a flurry of winter respiratory illnesses, nurses deeply understand that the collective health of the nation is dependent on all people — our immigrant and our non-immigrant patients — receiving the care they need. Even just the threat of immigration enforcement in our nation's hospitals creates an atmosphere where patients will potentially avoid seeking care, putting entire communities at risk. Viruses and other illnesses can spread quickly without proper care, and they do not discriminate.[21]

[16] *Id.*
[17] *Moniuszko, supra* note *15*.
[18] Coral Murphy Marcos, *California Nurses Decry Ice Presence At Hospitals: 'Interfering With Patient Care'*, The Guardian (Sept. 16, 2025), https://www.theguardian.com/us-news/2025/sep/16/california-ice-hospitals-patient-care.
[19] *Id.*
[20] *Id.*
[21] *Nurses Condemn Revocation Of Policy Barring ICE Arrests At Hospitals*, Nat'l Nurses United (Apr. 11, 2025), https://www.nationalnursesunited.org/article/nurses-condemn-revocation-of-policy-barring-ice-arrests-at-hospitals.

ICE's presence has also created precarious conditions for healthcare workers. "It creates just a huge sense of fear, not only in our patient population, but in our employee population and our nurses."[22] Many health workers have asked for guidance on how to respond to ICE's presence at medical facilities and have expressed anxiety over how to address this while still providing quality care and protecting patients' rights.[23] Nurses have asked their hospitals how to discharge a patient into ICE custody, when the hospital's discharge policy requires that a patient be released to a family member or caregiver with instructions and discharge orders, without violating this policy.[24] ICE camped out in one hospital for 6 days waiting to apprehend a patient with a serious condition, "creating a hostile environment for her other patients and hospital staff. Their presence [was] invasive and inappropriate."[25]

iv. A Better World Is Possible

Legislators and regulators can establish standards to protect our health data, limit harmful uses of such data, and regulate emerging technologies to improve health outcomes and promote health equity. A strong data minimization standard that prohibits the sale of sensitive data will help to end the health privacy crisis. Data minimization limits the collection, processing, and retention of personal information to that which is necessary for the product or service requested. This standard protects data from being used in harmful ways like profiling, scoring, and targeted advertising. Data minimization includes purpose limitations, which allow for appropriate and necessary data flows while prohibiting unnecessary, harmful flows. For example, this allows for some personal data to be used for fraud prevention purposes during an online transaction but does not allow an entity to retain that data after it is no longer necessary or share it further with a data broker. Data minimization allows ancestry companies to use information in ways that it promises to its customers but limits that data from being shared with data brokers for targeted advertising or in future unknown ways. It also protects against data breach and security incidents because data cannot be breached when it was never collected in the first place. A ban on the sale of sensitive information

[22] Ibarra and Hwang, *supra* note 22.
[23] *Id.*
[24] Larry Buhl, *ICE Agents Camp Out At Glendale Hospital For 6 Days Waiting To Re-Apprehend Patient*, LA Public Press (July 9, 2025), https://lapublicpress.org/2025/07/ice-agents-glendale-hospital-waiting-to-arrest-a-patient/.
[25] Buhl, *supra* note 24.

prevents health data from being extracted and exploited. This standard further protects health data from being used in AI without express, affirmative consent and ensures more regulation of AI systems.

Data minimization reflects our long-held societal understanding that health information is private. By enacting legal standards and developing technologies that are consistent with this understanding, we can reprioritize patient privacy. So often people are resigned to increased surveillance and Big Tech's control that they acquiesce that there is nothing to do to protect their privacy. But in a world with less commercial and government surveillance that properly protects our data and our health, we will protect patients from government intrusions in healthcare settings and limit harmful data sharing with law enforcement.

B. Legal Landscape

This section provides background on the legal and technological landscape that has brought us to this crisis. The first subsection includes an overview of HIPAA, its protections and its limitations. Next, the second subsection explains how personal data is collected, processed, and used outside of the protection of HIPAA and how it can reveal information about our health. Lastly, the third subsection examines Washington's My Health My Data Act and explains how states can pass laws to better protect individuals' health information.

i. HIPAA

In order to consider health privacy and its relationship to health equity, it is essential to understand the foundational law that protects a key subset of health information. The Health Insurance Portability and Accountability Act (HIPAA) is often misunderstood as a broad privacy law covering health data, but it is actually a health technology law with privacy protections limited to records held by healthcare providers and certain related businesses. Congress enacted HIPAA in 1996 to modernize the health insurance industry, in part through the "establishment of uniform standards and requirements for the electronic transmission of certain health information."[26] In HIPAA, Congress empowered the Department of Health and Human Services (HHS) to adopt uniform standards "to

[26] 42 U.S.C. § 1320d (codifying Pub. L. 104–191, title II, § 261), Editor's and Revisor's Notes: Purpose.

enable health information to be exchanged electronically,"[27] which it saw as vital to the healthcare industry given technological evolutions and the digitization of records.

Congress granted HHS rulemaking authority under HIPAA, including directing the Secretary to review and adopt modifications to the Title II Administrative Simplification (AS) standards under HIPAA.[28] The AS standards govern how covered entities must protect patients' protected health information when they are exchanging electronic records.[29] These regulations apply to healthcare providers (e.g., doctors, nursing homes, and pharmacies); health plans (e.g., health insurance companies and Medicare); healthcare clearinghouses; and business associates that are engaged in carrying out healthcare functions for a covered entity.[30]

Ensuring the portability—the ability to transfer health records from one system to another—is a central focus of HIPAA. The law regulates the protection and sharing of protected health information (PHI) by covered entities to enable portability without running afoul of the privacy principles enshrined in the Hippocratic Oath. In some ways, HIPAA has achieved its primary objectives of modernizing the health insurance industry, increasing trust between patients and their healthcare providers, and facilitating the electronic sharing of medical information. HIPAA established patients' rights concerning their health data and incentivized covered entities to transition from paper to electronic data sharing.[31] And despite its significant limitations, HIPAA serves a crucial role in protecting individuals' sensitive health data, particularly given the lack of a general federal comprehensive privacy law. But HIPAA's narrow scope and limited authorities are not sufficient to protect all health data in 2026 and beyond.

[27] 42 U.S.C § 1320d-2(a)(1).

[28] 42 U.S.C. § 1320d-3.

[29] *HIPAA Administrative Simplification Resources and FAQs,* U.S. Ctr. for Medicare & Medicaid Servs. (Sept. 23, 2025), https://www.cms.gov/training-education/look-up-topics/hipaa-administrative-simplification-resources-and-faqs.

[30] *Covered Entities and Business Associates*, HHS (Aug. 21, 2024), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[31] *Your Rights Under HIPAA*, HHS (2025), https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

HIPAA Administrative Simplification Rules

Title II is the part of HIPAA that people often think of when referring to HIPAA as a health privacy law. Title II (Preventing Health Care Fraud and Abuse; Administrative Simplification) includes measures to reduce fraud in health insurance, to make the administration of healthcare transactions more efficient, and to empower the HHS Secretary to promulgate standards to safeguard health information.[32] HHS has promulgated five rules under Title II to achieve these goals.[33] These are:

- The Privacy Rule, governing the use and disclosure of PHI by covered entities;
- The Security Rule, establishing standards for technical safeguards to protect the security of electronic protected health information (ePHI);
- The Enforcement Rule, imposing civil monetary penalties for violations of HIPAA and establishing investigative procedures;
- The Transactions and Codes Sets Rule, mandating standardized processes for healthcare transactions; and
- The Unique Identifiers Rule, requiring covered entities to use the National Provider Identifier to identify healthcare providers in standard transactions.[34]

The rules relevant in this discussion are the Privacy Rule and Security Rule.

Privacy Rule

HHS first promulgated the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) in 2000,[35] establishing a national standard for the protection of PHI for covered entities to follow.[36] The Privacy Rule is the most critical portion of the HIPAA framework regarding the protection of PHI. The Privacy Rule applies to all PHI (both paper and electronic) and defines what types of PHI are covered under HIPAA. PHI, as defined by the Privacy Rule, is all individually identifiable health information held or transmitted by a covered health

[32] Pub. L. 104–191, Title II.
[33] Peter F. Edemekong et al., *Health Insurance Portability and Accountability Act (HIPAA) Compliance*, StatPearls [Internet] (Nov. 24, 2024), https://www.ncbi.nlm.nih.gov/books/NBK500019/.
[34] *Id.*
[35] 65 Fed. Reg. 82462, 82470 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).
[36] *Summary of the HIPAA Privacy Rule*, HHS (2004), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

entity.[37] Such health information includes demographic data that can relate to an individual's mental health or condition, provision of health care for the individual, or payment information to receive health care.[38] Covered entities under HIPAA cannot use or disclose PHI without the individual's signed authorization unless as expressly specified or required by the Privacy Rule.[39] For example, covered entities are allowed to disclose PHI to law enforcement officials to comply with a court order when the covered entity in good faith believes the PHI is evidence of a crime that occurred on the covered entity's premises, or for specialized governmental law enforcement purposes such as national security activities.[40] One of the major purposes of the Privacy Rule is to define and limit how covered entities may disclose PHI with and without an individual's consent.

Disclosure of PHI to law enforcement is a specific exception to HIPAA. In developing the Privacy Rule, HHS established a three-part test for covered entities to determine whether disclosure of PHI to law enforcement is permissible without an individual's authorization or court order. Disclosure is permissible when: (1) The information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) De-identified information could not reasonably be used.[41] HHS promulgated an update to the Privacy Rule in 2024 (2024 Privacy Rule) that prohibited covered entities from sharing PHI related to lawful reproductive care with law enforcement in most circumstances. This provided greater clarity to providers and patients who had struggled with contradictory laws and legal requirements, which had left providers uncertain about their legal obligations regarding law enforcement demands for records related to lawful care. The rule has since been vacated, as will be discussed in more detail in the "Current Issues" subsection.

Additionally, strengthened certain privacy provisions under HIPAA after the Health Information Technology for Economic and Clinical Health Act (HITECH Act)

[37] *Id.*

[38] *Id.*

[39] *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, HHS (June 27, 2025), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html#footnote7_pNGlcSilz8zt-t6E17j4p0aYbvjoO1awjOcFaEwoY_gBolAJEi8SdS.

[40] *When does the Privacy Rule Allow Covered Entities to Disclose Protected Health Information to Law Enforcement Officials?,* HHS (2022), https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

[41] 45 C.F.R. § 164.512(f)(1)(ii)(C).

was enacted in 2009 by expanding covered entities to include business associates of healthcare providers and providing incentives for healthcare providers to transition to electronic health records (EHRs).[42] The transition to EHRs was intended to improve coordination of care and efficiency, reduce costs, and enhance the privacy and security of health records.[43] The HITECH Act also introduced a new requirement for covered entities to report health data breaches.[44] Both the widespread adoption of EHRs and the breach notification requirement strengthened HHS's ability to enforce penalties for HIPAA violations.

Security Rule

HHS finalized the HIPAA Security Rule in 2003 to ensure that covered entities implement cybersecurity policies and practices to protect patients' PHI that is created, collected, used, or maintained electronically (ePHI).[45] Specifically, the Security Rule lists three sets of safeguards that covered entities must comply with: administrative (risk analyses, workforce clearance, security training, etc.); physical (physical access to devices that store ePHI, data back-ups, etc.); and technical (password management, data encryption, audits, etc.).[46]

At the end of 2024, HHS issued a Notice of Proposed Rulemaking (NPRM) to modify the HIPAA Security Rule to "strengthen cybersecurity protections for electronic protected health information."[47] The NPRM culminated from a Healthcare Sector Cybersecurity concept paper HHS published in December 2023, focusing on four primary areas of action:

1) establish voluntary cybersecurity performance goals for the healthcare sector,
2) provide resources to incentivize and implement these cybersecurity practices,
3) implement an HHS-wide strategy to support greater enforcement and accountability, and

[42] Steve Alder, *What is the HITECH Act?*, The HIPAA Journal (Apr. 3, 2025), https://www.hipaajournal.com/what-is-the-hitech-act/.
[43] *Id.*
[44] *Id.*
[45] *The Security Rule*, HHS (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.
[46] Steve Alder, *HIPAA History*, The HIPAA Journal (Apr. 2, 2025), https://www.hipaajournal.com/hipaa-history/.
[47] *Notice of Proposed Rulemaking: HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information*, 90 Fed. Reg. 989, (Jan. 6, 2025).

4) expand and mature the one-stop shop within HHS for healthcare sector cybersecurity.[48]

If adopted, these proposed updates to the Security Rule would strengthen cybersecurity safeguards, including by requiring covered entities to conduct compliance audits, undergo a risk analysis of their data network for vulnerabilities, and adopt reliable cybersecurity measures.[49] EPIC submitted comments[50] in response to the NPRM applauding the agency's efforts to safeguard data, including through basic security measures such as multifactor authentication, network segmentation, encryption, reviewing and testing security measures, and contingency planning. As of the date of publication of this report, the rule remains pending.

Limitations of HIPAA

The main limitations of HIPAA are limitations of scope—the types of entities and the types of health data to which the law applies. When Congress passed HIPAA in 1996, health data could not be shared as widely across the digital ecosystem as it can today, there were not inexpensive and widely available devices for monitoring health information, and data about routine online activities were not being analyzed to infer health characteristics. Most covered entities under HIPAA in the early 2000s stored and shared PHI via paper, not digitally. We now live in a different age of health data collection, disclosure, and inferences.

HIPAA-covered entities are no longer the only players collecting health information from individuals. There is a growing industry that profits from consumer health data which is not covered by HIPAA. These entities range from genetic testing companies to health-tracking devices that collect biometric data. HIPAA does not protect health information irrespective of how it is obtained; it only covers data held by covered providers. This means that genetic health data a consumer provides to a genomics company is not protected under HIPAA, even though that data is incredibly sensitive, because the direct-to-consumer genomics

[48] *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services*, HHS (2023), https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf.

[49] Steve Alder, *HHS Proposes Strengthened HIPAA Security Rule*, The HIPAA Journal (Dec. 30, 2024), https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/.

[50] EPIC, Comments on Notice of Proposed Rulemaking: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (Mar. 7, 2025), https://epic.org/documents/comments-of-epic-to-hhs-re-the-hipaa-security-rule/.

company is not a HIPAA-covered entity. As a result, the geonomics company is not required to comply with HIPAA's Privacy Rule or Security Rule when, for example, it is asked to disclose sensitive health data to law enforcement or when it considers selling that information to a data broker.

As a result, a Wild West of health data exists outside the reach of HIPAA protections, undermining health data privacy. As the burgeoning market of consumer health data continues to expand, an increasing portion of individuals' health data is collected by, used by, and shared between private businesses that are not subject to HIPAA regulations. This ecosystem is discussed further in the subsection "Background: Health-Related Data Outside of HIPAA."

Current Issues

Another significant limitation of HIPAA is that its regulations are overly permissive of health data disclosures to law enforcement. The law delegated to the Secretary of HHS the task of promulgating specific privacy rules, including rules that identify standards for disclosure of protected health information for specific purposes. The Privacy Rule includes standards for disclosures to law enforcement, and provides in relevant part that such disclosures will be permitted so long as there is (1) a law requiring certain reporting, (2) a court order, warrant, or judicial subpoena, (3) an administrative request that meets the three-part test (discussed in the privacy rule subsection above), or one of several other special circumstances.[51] This provision is necessary, but not sufficient to protect the privacy of health information and to preserve the integrity of the doctor-patient relationship. The rule is too permissive because it allows a covered provider to turn over health information to law enforcement even if there is no court order (subject to the three-part test) and because it doesn't limit the scope of what can be disclosed pursuant to a court order or warrant. The limitations of the Privacy Rule protections for health data in law enforcement demands came under greater focus in recent years because of new state laws targeting reproductive health care.

In 2024, following the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*,[52] HHS updated the existing 2000 Privacy Rule to

[51] 45 C.F.R. § 14.512(f).

[52] *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022). In *Dobbs*, the Supreme Court rescinded the constitutional right to abortion previously enshrined by *Roe v. Wade*, 410 U.S. 113 (1973).

create the HIPAA Privacy Rule to Support Reproductive Health Care Privacy (2024 Privacy Rule).[53] The rule has since been vacated, but it provides an example of measures that policymakers could take to provide stronger protections for sensitive information. The 2024 Privacy Rule attempted to provide guidance because there was—and continues to be—uncertainty as to how reproductive health data must be protected without constitutional protections for abortion in place. With different states instituting varying reproductive protections and criminal sanctions, covered entities under HIPAA have had to balance conflicting obligations to produce health information when compelled by law enforcement and to protect patient-physician confidentiality.[54]

There is a clear need to strengthen protections for reproductive health data. A lack of legal and privacy protections for individuals seeking reproductive health care increases health inequities. Without greater protection, patients may fear how their PHI may be used by law enforcement in retaliation for seeking lawful reproductive health care. Certain groups of marginalized people, especially those from overpoliced communities, may face even greater anxiety. And these fears are not unfounded. There are many avenues for law enforcement to obtain data to target individuals seeking abortion care. For example, 26% of adult criminalization of self-managed abortion was reported to law enforcement by acquaintances of individuals.[55] Additionally, law enforcement has searched through automated license plate reader camera data to track down people suspected of self-managing an abortion.[56] A sheriff's office in Texas searched more than 83,000 Flock automated license plate reader (ALPR) cameras to track down a woman who had had an abortion, and the office lied about the purpose claiming that the search was for a missing person.[57] HIPAA does not cover such data, and it does

[53] HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 89 Fed. Reg. 32976 (Apr. 26, 2024).
[54] Ellen W. Clayton, Peter J. Embí, & Bradley A. Malin, *Dobbs and the Future of Health Data Privacy for Patients and Healthcare Organizations*, 30 J. of the Am. Med. Informatics Ass'n. 155, 156 (Oct. 4, 2022), https://academic.oup.com/jamia/article/30/1/155/6680473.
[55] Laura Huss, Farah Diaz-Tello & Goileen Samari, *Self-Care, Criminalized: The Criminalization of Self-Managed Abortion from 2000 to 2020*, If/When/How at 30 (2023), https://ifwhenhow.org/wp-content/uploads/2023/10/Self-Care-Criminalized-2023-Report.pdf.
[56] Rindala Alajaji, *She Got an Abortion. So A Texas Cop Used 83,000 Cameras to Track Her Down.,* EFF (May 30, 2025), https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down.
[57] Dave Maass and Rindala Alajaji, *Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation.*,EFF (Oct. 7, 2025), https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it.

not limit law enforcement's ability to deploy a variety of methods to punish individuals seeking lawful out-of-state abortion care.

Even the protections in HIPAA for PHI held by covered providers are quite limited when it comes to law enforcement requests. Under the Privacy Rule, covered entities are permitted but not required to "disclose PHI about an individual, without the individual's authorization, when such disclosure is required by another law and the disclosure complies with the requirements of the other law."[58] The Privacy Rule permits but does not require covered entities to disclose PHI to law enforcement for purposes "pursuant to process and as otherwise required by law" under certain conditions.[59] To illustrate this right to permissive disclosure, HHS provides this example:

> A law enforcement official presents a reproductive health care clinic with a court order requiring the clinic to produce PHI about an individual who has obtained an abortion. Because a court order is enforceable in a court of law, the Privacy Rule would permit **but not require** the clinic to disclose the requested PHI. The clinic may disclose **only** the PHI expressly authorized by the court order.[60]

In 2024, HHS was working to narrow the scope of the HIPAA permissive disclosure rule. The 2024 Privacy Rule provided that law enforcement would only be allowed to access PHI when "the disclosure is not sought for the prohibited purpose of imposing criminal, civil, or administrative investigation or liability on someone for merely seeking, obtaining, providing, or facilitating lawful reproductive health care."[61] While the 2024 Privacy Rule did not eliminate the numerous other pathways law enforcement uses to obtain information to prosecute people seeking abortion care, it was an important rule that provided

[58] *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, HHS (June 27, 2025), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html#footnote14_bFvqXAqOdO7e-qjDCfcmI5-YUfEsvx6Gvw-5gHZQ_nJECxgurxtqj.

[59] 45 CFR 164.512(f)(1); *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, HHS (June 27, 2025), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html#footnote14_bFvqXAqOdO7e-qjDCfcmI5-YUfEsvx6Gvw-5gHZQ_nJECxgurxtqj.

[60] *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, HHS (June 27, 2025), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html#footnote14_bFvqXAqOdO7e-qjDCfcmI5-YUfEsvx6Gvw-5gHZQ_nJECxgurxtqj.

[61] [Proposed] Memorandum of Law in Support of Intervenor-Defendants' Motion for Summary Judgment, *Purl v. HHS,* No. 2:24-cv-228-Z, 2 (N.D. Tex. 2025), https://democracyforward.org/wp-content/uploads/2025/01/Intervention-Purl-v-HHS.pdf.

some protections for the privacy of the individual and the trust between patients and healthcare providers. Unfortunately, as noted, the rule was later vacated and is not in effect.

2024 Privacy Rule – Challenges in Court

Two main lawsuits challenged the 2024 Privacy Rule in court. Because of the outcome of these cases and subsequent appeals, individuals seeking lawful reproductive health care and healthcare providers face great uncertainty about the circumstances in which physicians must disclose PHI to law enforcement.

In *Purl v. Department of Health and Human Services*,[62] plaintiffs challenged the 2024 Privacy Rule in the District Court for the Northern District of Texas. EPIC joined 40 organizations and individuals on If/When/How's amicus brief in support of HHS.[63] The court vacated the rule[64] and HHS changed its position under the Trump administration, abandoning the appeal and effectively vacating the rule.[65]

The consequences that will emerge as a result of the 2024 Privacy Rule being vacated cannot be overstated. The 2024 Privacy Rule was important in responding to a new and specific threat of law enforcement investigations that were intended to impede access to reproductive health care. The loss of that protection poses serious risks to individuals seeking that care. This also exposes the inadequacy of the current HIPAA protections for law enforcement disclosure.

ii. Health-Related Data Outside of HIPAA

Rapid advances in technology and commerce have created an ecosystem of health-related data that falls outside of the scope of HIPAA. As the law has struggled to keep pace with these changes, both the processing of health data

[62] Complaint and Request for Declaratory and Injunctive Relief, *Purl v. HHS,* No. 2:24-cv-228-Z (N.D. Tex. 2024), *available at* https://litigationtracker.law.georgetown.edu/wp-content/uploads/2024/10/PURL_10.21.24_COMPLAINT.pdf.

[63] *EPIC Joins If/When/How, Reproductive Justice Coalition in Purl v. HHS Amicus Brief*, EPIC (Mar. 25, 2025), https://epic.org/epic-joins-if-when-how-reproductive-justice-coalition-in-purl-v-hhs-amicus-brief/; Br. of Amicus Curiae If/When/How: Lawyering for Reproductive Justice at 11, *Purl v. HHS*, No. 2:24-CV-228-Z (N.D. Tex. 2025), https://ifwhenhow.org/wp-content/uploads/2025/03/Purl-IWHs-Amicus-Brief.pdf.

[64] *Purl, et al. v. U.S. Department of Health and Human Services, et al.,* No. 2:24-cv-00228-Z (N.D. Tex. 2025); *Federal Judge Invalidated HIPAA Reproductive Privacy Rule*, Ass'n of American Medical Colleges (June 27, 2025), https://www.aamc.org/advocacy-policy/washington-highlights/federal-judge-invalidates-hipaa-reproductive-privacy-rule.

[65] Elizabeth Murray and Nicholas White, *Fifth Circuit Dismisses Appeal of Decision Vacating HIPAA Reproductive Health Privacy Rule—Signaling the End of the Purl Case*, ABA (Oct. 6, 2025), https://www.americanbar.org/groups/health_law/news/2025/signaling-end-purl-case/.

and the entities that handle it have become increasingly unregulated. The lack of privacy protections for this growing volume of non-HIPAA-covered information places consumers at risk of having their sensitive health data used in unexpected, harmful, and dangerous ways. This section explains how health-related data is generated and collected in the commercial surveillance ecosystem and illustrates how this data can be used in harmful ways, often disproportionately harming marginalized groups.

The lack of HIPAA protections for health-related data is especially harmful when people expect their data to be protected and don't realize it falls outside of the scope of protections. For example, information collected directly by providers in a hospital falls outside of HIPAA's protections if it is anonymized. This may include patient discharge data—such as a patient's demographics, location, and conditions of release[66]—which hospitals distribute not only to health researchers but also to big data companies.[67] Although hospitals employ measures to deidentify or anonymize the data, patients are still at risk of reidentification.[68] Additionally, since HIPAA no longer applies to the data because it's been "anonymized," there are few limitations on its future use by purchasers.[69]

But perhaps the largest category of health data that is not protected under HIPAA is the types of consumer health data collected via websites, cell phones, apps, wearables, and other sources that simply were not as big an issue in 1996 when HIPAA was enacted. The proliferation of commercial surveillance technologies, which enable tracking of consumers' data across the web, has created an expansive marketplace where health and other personal data is routinely exchanged between digital platforms, data brokers, and advertisers. This

[66] *See* Sean Hooley & Latanya Sweeney, *Survey of Publicly Available State Health Databases* 3-4 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277688.
[67] *See* Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 Health Matrix 65, 81 (2014), https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1005&context=healthmatrix.
[68] *See id.;* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703, 711 (2016), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4948&context=wlr (Massachusetts Governor Weld was identified from his "de-identified" hospitalization records. "A state insurance agency was obligated to release certain hospitalization records to the public for research purposes after first removing direct identifiers while leaving demographic data (birthday, ZIP code, gender) and sensitive health data. Latanya Sweeney obtained the deidentified hospital records, matched them with publicly available voter registration records (which contained similar demographic data), and reidentified Governor Weld by isolating his record in the voter rolls and matching it with his deidentified hospital record.") citing Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 Int'l J. on Uncertainty, Fuzziness & Knowledge-Based Systems 557, 558–59 (2002).
[69] Terry, *supra* note 67.

ecosystem tracks consumers directly via online forms and other user-input mechanisms—including, for example, the demographic information, dates of menstruation, and menstrual- or pregnancy-related symptoms elicited from users of the Flo Health fertility-tracking app.[70] Users may reasonably expect an application that prompts them to enter sensitive health information to be covered by HIPAA, but this is often not the case. According to a complaint brought by the Federal Trade Commission (FTC) against Flo Health, the app "[encouraged] millions of women to input extensive information about their bodies and mental and physical health," which it then disclosed to Google, Meta, and other analytics companies without sufficient notice to or consent from consumers.[71]

Not all data collection requires consumers' action—or even knowledge that collection is occurring. One technique for surreptitiously collecting consumer data is through cookies, small files used by web browsers to store information about a user's interactions with various sites.[72] Even when a consumer adjusts their browser settings to block cookies, their computer configuration can serve as a unique "fingerprint," enabling platforms to track their data across the web.[73] Another common surveillance tactic employs tracking pixels, including invisible embedded images or code elements on websites and e-mails that can track a user's online activity.[74] Because tracking pixels are invisible to users and are generally not blocked by the browser controls established for cookies, most consumers are likely unaware when companies are using pixels to transmit their personal data.[75] Such technologies are now ubiquitous. Analysis conducted by The Markup revealed that websites for one-third of the top 100 U.S. hospitals include the Meta Pixel, which transmits patient data to Facebook, likely for advertising purposes.[76] Lockdown Privacy discovered similar pixel trackers on

[70] *In re Flo Health, Inc.*, FTC File No. 192-3133 (2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.
[71] *Id.*
[72] *See* EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* at 36 (2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter EPIC, *Disrupting Data Abuse*].
[73] *Id.* at 36-37.
[74] *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FTC (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.
[75] *Id.*
[76] Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, The Markup (July 19, 2023), https://themarkup.org/pixel-

Planned Parenthood's online scheduling tool, which patients use to book various appointments, including abortion services.[77]

Further methods of location tracking like geofencing, which tracks mobile devices within a 'virtual border' around a specific location, allow data brokers to collect large amounts of data on consumers within a particular geographic area.[78] When a person visits a hospital or doctor's office, they expect that the information about their visit will be private. But with geofencing, a data broker can collect the location information revealing which medical facility a person attended. Therefore, even in some interactions with covered entities (where people would reasonably expect HIPAA to protect their data), information relating to the traditional provider-patient relationship is recorded that nevertheless falls beyond HIPAA's scope.

Wearable devices, such as smart watches and glasses, fitness trackers, and internet-connected blood pressure or glucose monitors, serve as another major source of health-related data. These devices collect wide-ranging physiological information, tracking users' location and movements, heart rate, blood oxygen levels, and even brain activity.[79] Such biometric data is deeply personal and can be used not only to identify a given user but also to deduce their habits and interests.[80] Because companies that produce wearable technologies generally do not qualify as covered entities, this intimate data is largely uncovered by HIPAA.

Aggregating data collected through these commercial surveillance techniques generates inferences regarding consumers' attributes and behavior, providing detailed insights into their personal lives. In addition to data derived from explicitly health-related sources (e.g., telehealth services or fitness apps), much of the data collected through a consumer's routine online interactions is

hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites; Steve Adler, *Study Reveals One Third of Top 100 U.S. Hospitals are Sending Patient Data to Facebook*, The HIPAA Journal (June 17, 2022), https://www.hipaajournal.com/study-reveals-one-third-of-top-100-u-s-hospitals-are-sending-patient-data-to-facebook/.

[77] Tatum Hunter, *You Scheduled an Abortion. Planned Parenthood's Website Could Tell Facebook.*, Wash. Post (June 29, 2022), https://www.washingtonpost.com/technology/2022/06/29/planned-parenthood-privacy/.

[78] *See* Sheryl Xavier, Andrea Fray & Stephen Phillips, *Protecting Reproductive Health Data: State Laws Against Geofencing*, Reuters (Jan. 2, 2025), https://www.reuters.com/legal/legalindustry/protecting-reproductive-health-data-state-laws-against-geofencing-2025-01-02/.

[79] *See* Bonan Zhang et al., *A Survey On Security And Privacy Issues In Wearable Health Monitoring Devices*, 155 Computers & Security 2, 3-4 (2025), https://www.sciencedirect.com/science/article/pii/S0167404825001427.

[80] *See id.* at 8.

"medically inflected," meaning it is useful for making predictions regarding that consumer's health.[81] For years, Target has used consumers' demographic data and purchase patterns to assign shoppers "pregnancy prediction" scores, deriving health inferences about a consumer's pregnancy status and potential due date.[82] These predictions enable the company to tailor its advertising to specific stages of a consumer's pregnancy, which in at least one instance revealed a teenager's pregnancy to her father.[83]

In contrast to the brief updates patients periodically provide to their healthcare providers, commercial surveillance enables online entities to develop persistent, detailed dossiers of consumers' health information. Additionally, unlike data protected by HIPAA, platforms and data brokers face few restrictions on how they share and use this uncovered information.

In the U.S., the Federal Trade Commission is the federal regulator primarily responsible for enforcing online privacy standards under its general consumer protection authority.[84] The FTC has considerable rulemaking and enforcement authority to regulate "unfair or deceptive acts or practices in or affecting commerce" under Section 18 of the FTC Act.[85] For example, the FTC recently took action against Cerebral, a platform offering online therapy services, for misrepresenting its disclosure of users' personal health information, including answers to mental health questionnaires, to third parties for advertising purposes.[86] The Commission ordered Cerebral to cease using and sharing consumers' sensitive health data for targeted advertising, though the company may continue using such information for analytics relating to the effectiveness of its application and advertisements.[87]

[81] *See* Terry, *supra* note 67, at 85-86.
[82] *See* Charles Duhigg, *How Companies Learn Your Secrets*, The New York Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
[83] *See id.*
[84] *Protecting Consumer Privacy and Security*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security.
[85] 15 U.S.C. § 57a; *see also A Brief Overview of the Federal Trade Comm'n's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[86] *See* First Amended Complaint for Permanent Injunction, Monetary Relief, Civil Penalties, and Other Relief, *United States v. Cerebral, Inc.*, 1:24-cv-21376-JLK, 19-20 (S.D. Fla. 2024).
[87] *See* Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., *United States v. Cerebral, Inc.*, 1:24-cv-21376-JLK, 13-14 (S.D. Fla. 2024).

Unfortunately, the FTC has not made full use of its authority over commercial data practices, failing to provide adequate privacy protections for data that falls through the gaps left by HIPAA. Even when the Commission uses its resources to regulate harmful practices, its typical pattern of case-by-case enforcement cannot effectively regulate the entire commercial surveillance ecosystem, leaving large swaths of data unprotected. Thus, many online entities continue to amass and misuse consumer health information without due regard to the privacy harms their actions create.

Such misuses of consumer health data take many forms, with targeted advertising being perhaps the most common. Due to the prevalence of targeted advertising, consumers likely have a general awareness that their online activity influences the digital ads presented to them. Still, consumers may be surprised or dismayed to know the extent to which advertisers use their sensitive health information to peddle products. For instance, forensic testing of the website that Californians use to purchase health insurance under the Affordable Care Act revealed hidden pixel trackers that had been transmitting user data to LinkedIn for advertising purposes without consumers' knowledge or consent.[88] The data—collected on millions of consumers who had used the online marketplace in the past year—included users' demographic information, pregnancy status, gender identity, medical history, and searches for healthcare providers.[89] Google's Real Time Bidding (RTB) system, a programmatic auction for digital ad space, contains thousands of data segments, including sensitive health related segments like "Individuals likely to have a Cardiovascular condition, such as Atrial Fibrillation, that is treated with a Prescription/Rx medication."[90]

Using consumers' sensitive health data for targeted advertising can lead to significant harms, including reputational damage, mental and emotional distress, and—in the most severe cases—physical injury or death. Grindr, which came under fire for sharing users' HIV status with two application analytics companies in

[88] *See* Tomas Apodaca & Colin Lecher, *How California Sent Residents' Personal Health Data To Linkedin*, The Markup (Apr. 28, 2025), https://themarkup.org/pixel-hunt/2025/04/28/how-california-sent-residents-personal-health-data-to-linkedin.

[89] *See id.*

[90] EPIC & ICCL, Complaint and Request for Investigation, Injunction, Penalties, and Other Relief *In re Google's RTB Practices*, (Jan. 16, 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-ICCL-Enforce-In-re-Googles-RTB-Complaint.pdf.

2018,[91] has recently faced accusations of sharing that information with advertisers.[92] Plaintiffs in an ongoing UK lawsuit against the company expressed feelings of “fear, embarrassment, and anxiety” upon receiving advertisements for HIV therapies after disclosing their HIV status through the app for sexual health purposes.[93] These alleged privacy violations pose increased risks for Grindr users who selectively disclose or do not publicly share information about their sexuality, threatening exposure of their sexual orientation and undue stigma related to their HIV status. The lawsuit was enabled by UK data privacy laws[94] that bar platforms from sharing sensitive data for commercial purposes without users’ consent. U.S. consumers largely lack this protection because states fail to adequately enforce opt-in consent requirements for the processing of sensitive data—or have simply failed to adopt such requirements at all.

Targeted advertising that leverages data related to consumers’ reproductive health introduces additional dangers, particularly as more states enact legislation restricting access to abortion[95] and gender-affirming care.[96] In 2024, Senator Ron Wyden published a letter to the FTC and the Securities and Exchange Commission (SEC) revealing that location data broker Near Intelligence sold information on people's visits to nearly 600 Planned Parenthood locations to enable a nationwide anti-abortion ad campaign.[97] Veritas Society, a nonprofit created by Wisconsin Right to Life, used the location data to deliver over 14 million anti-abortion ads to individuals who visited reproductive health clinics.[98] In addition to the

[91] *See* Scott Neuman & Camila Domonoske, *Grindr Admits It Shared HIV Status Of Users*, NPR (Apr. 3, 2018), https://www.npr.org/sections/thetwo-way/2018/04/03/599069424/grindr-admits-it-shared-hiv-status-of-users.

[92] *See* Robert Booth, *Grindr Accused Of Treating Gay Man’s Medical Data Like ‘Piece Of Meat’*, Guardian (May 26, 2024), https://www.theguardian.com/uk-news/article/2024/may/26/grindr-accused-of-treating-gay-man-medical-data-like-piece-of-meat.

[93] *Id.*

[94] *Special Category Data*, Information Commissioner’s Office (Oct. 28, 2024), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/.

[95] *See* Allison McCann & Amy Schoenfield Walker, *Tracking Abortion Laws Across the Country*, The New York Times (May 29, 2025), https://www.nytimes.com/interactive/2024/us/abortion-laws-roe-v-wade.html.

[96] *See Map: Attacks on Gender Affirming Care by State*, Human Rights Campaign, https://www.hrc.org/resources/attacks-on-gender-affirming-care-by-state-map.

[97] *See* Alfred Ng, *A Company Tracked Visits To 600 Planned Parenthood Locations For Anti-Abortion Ads, Senator Says*, Politico (Feb. 13, 2024), https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172.

[98] Letter from Sen. Ron Wyden to Chair Lina Khan, Fed. Trade Comm’n & Chair Gary Gensler, Sec. Exch. Comm’n (Feb. 13, 2024), https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf.

psychological harms[99] experienced by clinic visitors who received ads designed to pressure or shame their health decisions, Near's data sales placed abortion-seekers located in states that have instituted abortion bans at risk of criminalization. Moreover, Veritas Society's ad campaign and the location-tracking that enabled it threaten to have a chilling effect on all those seeking care—abortion-related or otherwise—from reproductive health clinics.

Beyond targeted advertising, online entities continue to use sensitive health data in new and unforeseen ways. When genetic testing company 23andMe filed for bankruptcy, it effectively placed its customers' DNA data up for auction.[100] Millions of people purchased the company's genetic testing kits to map their ancestry, connect with family members, or understand their predisposition for various health conditions. In doing so, they consented to sharing their genetic information with 23andMe—not to the highest bidder in the genetic data market. Since people cannot change their DNA, 23andMe's customers and their biological relatives have limited recourse to control future access to and use of their genetic data. As explained by Emily Tucker, Executive Director of the Center on Privacy & Technology at Georgetown Law, the lack of regulations on this data places "genetic privacy at the mercy of [23andMe's] internal data policies and practices, which the company can change at any time."[101]

Additionally, tech companies are using consumers' health data to train general artificial intelligence models.[102] In one case, AI artist Lapine discovered medical photographs taken by her doctor to document the results of her facial surgeries in the publicly available LAION-5B image dataset, which has been used to train AI models like Google's Imagen.[103] Investigating the dataset revealed thousands of medical photographs of patients, many of whom likely have no idea

[99] *See* Janet M. Turan & Henna Budhwani, *Restrictive Abortion Laws Exacerbate Stigma, Resulting in Harm to Patients and Providers*, 111 Am. J. Pub. Health 37, 37-38 (2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC7750605/pdf/AJPH.2020.305998.pdf.

[100] Kevin Collier, *23andme Bankruptcy Filing Sparks Privacy Fears as DNA Data of Millions Goes Up for Sale*, NBC News (Mar. 25, 2025), https://www.nbcnews.com/tech/security/23andme-goes-bankrupt-millions-peoples-dna-data-sale-rcna197874.

[101] *Id.*

[102] 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/.

[103] Benji Edwards, *Artist Finds Private Medical Record Photos In Popular AI Training Data Set*, Ars Technica (Sept. 21, 2022), https://arstechnica.com/information-technology/2022/09/artist-finds-private-medical-record-photos-in-popular-ai-training-data-set/.

that their images are available to download.[104] Even if Lapine and other patients managed the difficult feat of removing their images from LAION's database, their health data would still be ingrained in the AI models that were trained on those images without their consent. Considering that many AI companies refuse to disclose their data sources and that AI models sometimes regenerate the material used to train them, consumers have limited insight into how their sensitive health data is currently shaping or being exposed by AI tools.[105]

The risks created by these unexpected uses of people's health information are wide-ranging. For example, inferences derived from consumers' health data may impact individual insurance rates and coverage.[106] Using detailed dossiers created by data brokers to make medical assumptions about consumers may lead health insurers to overprice their plans or discriminate against those projected to face high medical costs.[107] Not to mention that health predictions based on a person's demographics, personal interests, or shopping habits are error-prone and may exacerbate harmful biases that already lead to disparate health outcomes for marginalized communities.[108]

As long as the collection and use of sensitive health data uncovered by HIPAA remain unregulated, platforms and data brokers will continue to find novel and dangerous ways to exploit it. Thus, changes in the law are needed to keep pace with technological development and provide comprehensive privacy protections for consumers' health-related information.

iii. Washington's My Health My Data Act

In the rapidly changing health privacy landscape, several states have taken action to protect health related information. This section highlights one state's approach in creating robust and meaningful protections for data that is not covered by HIPAA: Washington state. The state's My Health My Data Act (MHMDA) was signed into law on April 27, 2023 and prohibits all businesses operating in or providing services to consumers in Washington from "collecting, sharing, or selling

[104] *See id.*
[105] Leffer, *supra* note 102.
[106] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.
[107] *See id.*
[108] *See generally* Janice A. Sabin, *Tackling Implicit Bias in Health Care*, 387 New Eng. J. Med. 105 (2022), https://www.nejm.org/doi/pdf/10.1056/NEJMp2201180.

any health-related information about a consumer without their consent."[109] The Act includes a private right of action and is also enforced by Washington's Attorney General. This section will give an overview and background of Washington's My Health My Data Act, define certain key terms within the Act, explain emerging cases under the Act, and briefly discuss various states' health privacy legislation.

Generally, the My Health, My Data Act requires that a business:

- Create readable and approachable privacy policies for consumers;
- Obtain consumer consent prior to the collection of user health data, unless the data is directly pertinent and necessary to the consumer's use of the business' product;
- Obtain consumer consent prior to the sale of their health data;
- Not engage in the use of geofencing around health facilities; and
- Allow users to:
    - withdraw consent from the collection and sale of health data;
    - request their collected health data; and
    - request the deletion of their health data.[110]

History

The law emerged from a 2019 proposed consumer privacy bill called the Washington Privacy Act. Following the Dobbs v. Women's Health Organization decision, Representative Vandana Slatter introduced MHMDA, describing it as "the first in the nation bill we need" and "part of a comprehensive pack of legislation… in respon[se] to the [Supreme Court's] decision to upend constitutional protections for reproductive healthcare."[111] Washington, like many states, lacked a general comprehensive privacy law which left its residents vulnerable to unauthorized access of individuals' reproductive data.

Key Definitions

The bill defines "consumer health data" broadly as, "personal information that is linked or reasonably linkable to a consumer and that identifies the

[109] Wash. Rev. Code §19.373.040 (2023).
[110] Wash. Rev. Code §19.373(2023).
[111] *My Heath, My Data Act Passes Senate*, Washington State House Democrats (Apr. 6, 2023), https://housedemocrats.wa.gov/blog/2023/04/06/my-health-my-data-act-passes-senate/.

consumer's past, present, or future physical or mental health status."[112] This includes:

- Individual health conditions, treatment, diseases, or diagnosis;
- Social, psychological, behavioral, and medical interventions;
- Health-related surgeries or procedures;
- Use or purchase of prescribed medication;
- Bodily functions, vital signs, symptoms, or measurements of the information [otherwise listed here];
- Diagnoses or diagnostic testing, treatment, or medication;
- Gender-affirming care information;
- Reproductive or sexual health information;
- Biometric data;
- Genetic data;
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
- Data that identifies a consumer seeking healthcare services; or
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data [otherwise listed here] that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).[113]

Importantly, MHMDA includes inferences in its protections. Inferences are assumptions that entities make based on personal data that can reveal health status or can be combined with other data to reveal health status, but is not itself health information. As explained in the previous section, location information may reveal health status when it shows that an individual was at a particular health facility, for example.

In a post-*Roe* world and amidst attacks on trans people nationwide, MHMDA was one of the first state privacy laws in the country that explicitly regulated the collection and sharing of data surrounding reproductive and gender-affirming

[112] Wash. Rev. Code §19.373.010 (2023).
[113] Wash. Rev. Code §19.373.010 (2023).

care. The law treats these categories broadly, defining gender affirming and reproductive care information as any data regarding an individual seeking gender-affirming care or reproductive services in the past, present, or future.[114] Several state laws also now consider these types of data as "sensitive data" and require opt-in consent for collection and processing.

Rights and Restrictions

MHMDA provides consumers strong protections to safeguard their own data. The scope of the law is broad as it defines "consumer" as someone who resides in Washington state or whose data is collected in Washington state, providing protections to individuals who may travel to the state for reproductive or gender-affirming care.[115] MHMDA allows consumers to withdraw consent from the collection of data or have their data deleted, and requires that regulated companies provide consumers with a readable and informative privacy policy explaining the uses of their data.[116] These provisions enable consumers to be active participants in the collection, use, and dissemination of their private data. For data to be sold without consumer consent, it must be deidentified, meaning that it can "[not] reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer."[117]

The law prohibits an entity from implementing a geofence around a healthcare facility. MHMDA prohibits "an entity that provides in-person healthcare services where such geofence is used to identify or track consumers seeking healthcare services, collect consumer health data from consumers; or send notifications, messages, or advertisements to consumers related to their consumer health data or healthcare services."[118] Other states, including

[114] Wash. Rev. Code §19.373.040 (2023).
[115] Wash. Rev. Code §19.373.010 (2023).
[116] Wash. Rev. Code §19.373.010, 19.373.020 (2023).
[117] Wash. Rev. Code §19.373.010.
[118] Wash. Rev. Code §19.373.040 (2023).

Maryland,[119] Nevada,[120] Connecticut,[121] New York,[122] and California[123] have passed similar restrictions.

A geofence is essentially a virtual perimeter—meaning that software applications, such as Google Maps, can monitor when a consumer is within this perimeter. As defined by the law, a geofence is "technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location."[124] Law enforcement can obtain geofence warrants to determine who was within or near a given physical location at any given time; in a post-*Roe* world, privacy experts are concerned that these warrants can be weaponized to crack down on those seeking reproductive care.[125] Moreover, geofencing can be used to target advertisements toward people seeking reproductive care—advertisements that could be used to deter people from actually receiving that care.[126] In Oregon, an anti-abortion group used geofencing "to send targeted misinformation to people who visited any of 600 reproductive health clinics in 48 states."[127] This provision is particularly beneficial for people who come to Washington from other states seeking abortion-related care. Big tech companies selling bulk geolocation and geofence data to law enforcement allows officials to bypass a key legal step in obtaining a warrant, creating a mechanism to more easily prosecute people for simply obtaining reproductive health care.[128]

[119] Md. Code Ann., Com. Law § 14-4704(3).

[120] Nev. Rev. Stat. § 603A.540 (2024).

[121] Conn. Gen. Stat. § 42-526(a)(1)(C) (2024).

[122] N.Y. Gen. Bus. L. § 394-G (2024).

[123] Press Release, *Governor Newsom Signs New Landmark Laws To Protect Reproductive Freedom, Patient Privacy Amid Trump's War On Women*, CA Governor (Sept. 26, 2025), https://www.gov.ca.gov/2025/09/26/governor-newsom-signs-new-landmark-laws-to-protect-reproductive-freedom-patient-privacy-amid-trumps-war-on-women/; AB 45: Privacy: Health Data: Location And Research., Cal Matters (Sept. 26, 2025), https://calmatters.digitaldemocracy.org/bills/ca_202520260ab45.

[124] *Id.*

[125] Kierra B. Jones, *Stopping the Abuse of Tech in Surveilling and Criminalizing Abortion*, Center for American Progress (Jan. 29, 2025), https://www.americanprogress.org/article/stopping-the-abuse-of-tech-in-surveilling-and-criminalizing-abortion/.

[126] Cecilia Marrinan, *Geofencing: The Overlooked Barrier to Reproductive Freedom*, Council on Foreign Relations (Oct. 30, 2024), https://www.cfr.org/blog/geofencing-overlooked-barrier-reproductive-freedom.

[127] *Id.*

[128] Jones, *supra* note 128.

MHMDA is Not Perfect

While MHMDA provides individuals in Washington with important privacy protections for personal data related to reproductive and gender-affirming care, it is not perfect. Some critics of MHMDA have expressed concern that it enforces the same regulations on small and large businesses alike, arguing that small businesses have fewer resources to comply with MHMDA's requirements compared to larger, wealthier companies like Amazon. To address these concerns, the Washington legislature gave small businesses a longer timeline to comply with provisions of the law. While many privacy experts laud the bill for its broad definition of key terms, others worry that these definitions are so vague they may allow the act to encompass non-health-related data. The Washington Attorney General has since clarified several of the broad terms outlined in the bill. Additionally, some experts worry that the bill puts too much onus on individual consumers to understand data privacy policies and opt in or out of the collection and sale of their data.

The primary weakness in MDMDA is that is largely a consent-based law, which puts the onus on individual consumers to understand privacy policies and opt in or out of the collection and sale of their data. However, the law does contain two critical provisions for any consent-based law: (1) it requires that the consent be a "clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement," and specifies that it may not be obtained via acceptance of a broad terms of use agreement;[129] and (2) it backs up the consent requirement with the power of a private right of action, which has been shown to be the only mechanism capable of forcing companies to meaningfully comply with privacy laws.[130] A stronger model would be to set strong data minimization limitations on the collection and use of health data. Maryland, as a part of its comprehensive data privacy law, limits the collection and processing of "consumer health data," which includes data related to reproductive or sexual health care and gender-affirming treatment, to what is "strictly necessary" for the product or service the consumer requests.[131] Maryland also bans the sale of such

[129] Wash. Rev. Code §19.373.010 (2023).

[130] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-hartzog.pdf.

[131] Md. Code Ann., Com. Law § 14-4707(a)(1).

sensitive data.[132] Washington's law would be stronger if it placed a similar substantive restriction on the collection and processing of health data.

Enforcement

As mentioned above, MHMDA creates a private right of action for consumers to file complaints against businesses that violate the law. The first case under MHMDA, *Maxwell v. Amazon.com Inc*,[133] was filed on February 10, 2025 in the Western District Court of Washington in Seattle. The plaintiffs allege that Amazon violated both federal wiretapping laws and MHMDA by gathering location data via its software development kits (SDKs). These SDKs operate in the background of many third-party applications, allowing Amazon to harvest data via third parties. Location data provides particularly intimate insights into a person's life, as it is difficult to anonymize and can reveal location data unique to an individual, like their home or place of employment. For example, in Idaho, law enforcement used location data to prosecute an out-of-state mother and son for "aiding and abetting" an abortion.[134] While users may have consented to the app itself directly collecting their data, they had no knowledge that Amazon could access it as well. By not informing consumers about its data collection and using individuals' personal information that could indicate a person's attempt to obtain health services, Amazon's practices allegedly failed to abide by the key terms of the MHMDA. The availability of a private right of action is the most critical provision in MDHDA, as it encourages compliance in a way that enforcement by the Attorney General only would not.

Other State Privacy Laws

Across the country, several states have introduced or passed privacy laws. General comprehensive privacy laws can affect the rules for collection and processing of health information, so these laws are important in discussing the legal landscape of health privacy. The first to pass a general consumer privacy law was California, with the 2018 California Consumer Privacy Act (CPPA).[135] The CCPA requires companies to disclose the data they are collecting and to allow for

[132] Md. Code Ann., Com. Law § 14-4707(a)(2).
[133] Compl., *Maxwell v. Amazon.com Inc.*, 2:25-cv-261, (W.D. Wash. Feb. 10, 2025).
[134] The Associated Press, *A Mom And Son Are Charged In Idaho After A Teen Is Taken To Oregon For An Abortion*, NPR (Nov. 2, 2023), https://www.npr.org/2023/11/02/1210198143/idaho-abortion-kidnapping-charges-oregon-underage-girlfriend-parental-rights.
[135] C. Kibby, *U.S. State Privacy Legislation Tracker*, IAPP (May 25, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#state-privacy-law-map.

consumer deletion requests.[136] In 2020, California passed the California Privacy Rights Act (CPRA) which augmented and clarified the foundational protections of the CCPA. The CPRA introduced the "Sensitive Personal Information" category, meaning that information such as biometric, genetic, medical, and location data are subject to heightened privacy requirements. While other states have passed general privacy laws with varying levels of protection, some states are considering legislation like MHMDA that applies to health information specifically. California is currently considering the California Location Privacy Bill, which would add further restrictions to the collection and sale of consumer location data.[137] Colorado, Virginia, Connecticut, Maryland, Nevada, Texas, Utah, and Minnesota have all also passed laws that specifically regulate the collection and sale of personal health-related data.[138]

Many technology companies have been lobbying against more robust data privacy bills, advocating for ones that often lack strong data minimization standards and enforcement mechanisms.[139] Big Tech companies spent millions in lobbying fees in 2024,[140] often pushing for toothless bills under the guise of advocating for health and data privacy.[141] In 2023, as Oregon sought to pass a bill that gave citizens the right to sue businesses for the nonconsensual collection of their data, the tech lobby successfully persuaded lawmakers to remove the private right of action provision.[142] For years, privacy advocates have warned that tech companies are attempting to preempt strong state privacy laws by lobbying for a

[136] The California Consumer Privacy Act, State of California Department of Justice (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa.
[137] *California's Latest Privacy Push: The Location Tracking Crackdown Businesses Can't Ignore*, Fisher Phillips (Mar. 3, 2025), https://www.fisherphillips.com/en/news-insights/californias-latest-privacy-push.html.
[138] Kibby, *supra* note 135.
[139] EPIC & U.S. PIRG Education Fund, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC (Jan. 2025), https://epic.org/wp-content/uploads/2025/04/EPIC-PIRG-State-of-Privacy-2025.pdf. [hereinafter EPIC & U.S. PIRG, *The State of Privacy*].
[140] Ashley Gold, *Tech Flooded the Zone in Q1 Lobbying*, Axios (Apr. 24, 2024), https://www.axios.com/pro/tech-policy/2024/04/24/tech-flooded-the-zone-in-q1-lobbying.
[141] Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at A Time*, The Markup (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time.
[142] Brennan Bordelon & Alfred Ng, *Tech Lobbyists Are Running the Table on State Privacy Laws*, Politico (Aug. 16, 2023), https://www.politico.com/news/2023/08/16/tech-lobbyists-state-privacy-laws-00111363.

weaker federal privacy law, and their efforts to convince more states to pass bills similar to the weak, industry-drafted Virginia model is part of that same effort.[143]

As people continue to feel the harms from data collection, use, and processing outside of the scope and tech companies continue to lobby for weaker data privacy laws, state health data privacy bills offer an avenue for individuals to protect their private health information.

[143] Bennett Cyphers, *Big Tech's Disingenuous Push For a Federal Privacy Law*, Electronic Frontiers Foundation (Sept. 18, 2019), https://www.eff.org/deeplinks/2019/09/big-techs-disingenuous-push-federal-privacy-law.

PART I
DIRECT HEALTH IMPACTS

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

DIRECT HEALTH IMPACTS

The U.S. Lacks Privacy Protections for Health Information, Worsening Health Outcomes and Inequities

This section explains the unfortunate legal and technical reality of modern healthcare provision: a lack of privacy protections for health information leads to delayed care, worse care, or failure to obtain care, exacerbating health inequities. The lack of protection erodes trust and prevents care, which immediately and directly worsens health outcomes for people. These harms can be mitigated by easier access to quality health care, digital literacy, freedom to move through the health care system without fear of criminalization or discrimination, and resources like time and money. Accordingly, these harms are felt more acutely by marginalized communities, which in turn exacerbates already existing health inequities.

First, this section discusses the health data privacy crisis we face and presents a real-world example of its consequences: delayed care and worsened health outcomes. Second, it outlines the root causes of diminished privacy protections for health data, including a lack of legal protections and the resulting unregulated development of technology. Next, this section explains how these failures cause individual and systemic harms when people delay or forego care, fear criminalization and discrimination, and cannot adequately access care. Lastly, this section proposes solutions to address these systemic harms: a robust privacy standard to protect the full spectrum of health data across services and devices, strong cybersecurity requirements for health-related information, and strict prohibitions on the use of health-related information in high-risk contexts.

A. Introduction

Strong privacy protection is essential to quality health care. Confidence that sensitive health information will remain secure and confidential empowers patients to seek care when they need it and to be honest with their provider. Unfortunately, shifts in the legal and technological landscape have eroded the already insufficient privacy protections that exist for health data in the United

States. This loss of privacy contributes to lower-quality health care and exacerbates preexisting societal inequities.

What direct impacts can look like:

Imagine a woman, Rose, who has two young children. She has been a U.S. citizen since birth, but English is her second language. Rose's mother lives with her and is an undocumented immigrant. Rose and her husband are fearful of recent immigration raids in their city, so they advise Rose's mother to stay home while they take their children to a local park. At the park, Rose is playing with her kids when she falls off the equipment and injures her ankle. She limps home, hoping it will be better in the morning, but she is starting to worry about the financial burden of a major medical bill.

In the morning, Rose's ankle is in worse shape, and she worries there is a complication with her diabetes that affects her foot. She tries to set up a telehealth appointment, but her apartment lacks a private space, and her Wi-Fi is unreliable. She continues to work on her injured foot, and it continues to get worse. She goes to the emergency room a few weeks later because the pain has become unbearable and she can no longer move her foot. The doctors ask questions about her family and medical history. The forms they ask her to fill out are in English and are both lengthy and confusing. When asked about her mother and whether diabetes runs in her family, she freezes. She's overcome with worry that if she tells the doctor any information about her mother, immigration agents will come knocking on her door. She says nothing and heads home with a hefty bill, along with instructions to download an app for virtual physical therapy appointments.

Rose asks her daughter to help her download the app because all of the information is in English. When her daughter is presented with the pop-up "Always Allow Location Access" for the physical therapy app, Rose is overcome with fear that her location information will expose her mother to the government. She deletes the app and fails to follow up with any physical therapy. As a result, she suffers long term damage to her ankle.

B. Root Causes: Legal and Technological Changes Create Privacy Risks

Health privacy depends on an interplay between law and technology. Recent trends in both domains have tended to erode privacy rights. As a later subsection will discuss, this erosion of privacy rights can reduce the quality of care people receive and exacerbate societal inequalities.

i. *Recent Legal Developments Increase Privacy Risks*

Laws affect health privacy in contradictory ways—some protecting it, others undermining it. Recent legal trends have predominantly increased privacy risks, including the criminalization of health-related activities, law enforcement use of health information for non-health prosecutions, failure to update outdated and inadequate privacy regulations, mandates for healthcare "modernization," and potential Medicaid rollbacks that could reduce institutional privacy safeguards. This subsection details recent changes in the legal landscape that affect health privacy and equity. First, it addresses the trend to criminalize certain health activities and use health data in criminal prosecutions. Next, it discusses how the frameworks of HIPAA protections, FTC regulation, and state privacy laws fail to limit improper data flows of health information. Finally, it explains how cuts to Medicaid will reduce funding for health entities and diminish privacy protections for health data.

1. *Increased criminalization of health activities and the use of health data in prosecutions makes patients fearful of seeking care.*

The increased criminalization of health-related activities and the use of health data to prosecute other crimes represent a significant threat to health privacy. This is especially true for pregnant people, transgender people, immigrant populations, LGBTQ+ populations, and others who are more likely to be targeted by law enforcement.

Recent legal changes have put pregnant people at significant risk of criminal prosecution. After the Supreme Court reversed the constitutional right to an abortion in *Dobbs v. Jackson Women's Health Organization*,[144] many states have moved to prosecute women seeking abortions. Dozens of states now have

[144] *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022).

some type of abortion ban;[145] 12 states have a complete ban and 6 states have early limits between 6 and 12 weeks;[146] 6 states have no health exception;[147] 8 states have no exception for rape and incest;[148] and more than 210 women were criminally charged for pregnancy-related conduct in the year after *Dobbs* was decided.[149] Even people who have miscarriages have been targets for prosecution.[150] In Alabama, conceiving through in vitro fertilization (IVF) was briefly criminalized after the Alabama Supreme Court ruled that IVF-created embryos were children.[151]

Many states have also criminalized activities associated with transgender health care. For example, Texas recently moved to compile a record of all transgender people who had changed their names on their driver's licenses in the state.[152] At least 24 states have enacted laws criminalizing the provision of gender-affirming care to transgender youth.[153] The fact that these laws are often passed after the failure of "bathroom bills" that target transgender people themselves leads experts to conclude that their primary purpose is "the stigmatization and vilification of trans youth."[154] In the span of just a few years, a significant percentage of Americans face a real risk of criminal investigation as a result of their healthcare choices. To these individuals, the privacy of their health records can mean the difference between freedom and devastation.

[145] *Policy Tracker: Exceptions to State Abortion Bans and Early Gestational Limits*, KFF (Aug. 26, 2025), https://www.kff.org/womens-health-policy/exceptions-in-state-abortion-bans-and-early-gestational-limits/.
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] Wendy A. Bach & Madalyn K. Wasilczuk*, Pregnancy as a Crime: A Preliminary Report on the First Year After* Dobbs, Pregnancy Justice (Sept. 2024), https://www.pregnancyjusticeus.org/wp-content/uploads/2024/09/Pregnancy-as-a-Crime.pdf.
[150] Elizabeth Chuck, *Woman's Arrest After Miscarriage in Georgia Draws Fear and Anger*, NBC News (Dec. 13, 2022), https://www.nbcnews.com/news/us-news/georgia-arrest-miscarriage-fetal- personhood-rcna199400.
[151] *The Alabama Supreme Court's Ruling on Frozen Embryos*, Johns Hopkins Bloomberg Sch. of Pub. Health (Feb. 27, 2024), https://publichealth.jhu.edu/2024/the-alabama-supreme-courts-ruling-on-frozen-embryos.
[152] EPIC et al., Comments on HHS HIV PrEP Database SORN at 6, https://epic.org/documents/%20comments-of-epic-chlp-prep4all-and-patient-privacy-rights-to-hhs-on-hiv-prep-database-sorn/.
[153] EPIC, *Health Privacy*, https://epic.org/issues/data-protection/health-privacy/.
[154] Scott J. Schweikart, *What's Wrong with Criminalizing Gender-Affirming Care for Transgender Adolescents?*, 25 AMA J. Ethics 413, 415 (2023), https://journalofethics.ama-assn.org/article/whats-wrong-criminalizing-gender-affirming-care-transgender-adolescents/2023-06.

And the trend of increasing government intrusion into healthcare spaces has continued with the Trump Administration's aggressive and even lawless detainment and deportation of immigrants. The U.S. Department of Health and Human Services unlawfully gave Immigration & Customs Enforcement (ICE) officials access to the personal data of 79 million Medicaid enrollees to help them track down undocumented immigrants.[155] While federal laws such as HIPAA purportedly protect data held by healthcare providers—including HHS's Centers for Medicare and Medicaid Services (CMS)—CMS nevertheless entered into an agreement[156] with ICE to provide this information. An ICE officer recently told an arrestee that "judges' orders don't matter, only the president,"[157] and the Administration has resisted judicial orders to bring back immigrants that it has illegally deported.[158] These actions rightly arouse fear and suspicion that providers may share sensitive data with ICE, further eroding trust in healthcare in immigrant communities and undermining health equity.

But the weaponization of criminal law against at-risk communities has, unfortunately, been around longer than the last few years. The criminalization of HIV-positive status has created significant fear and fueled health inequities for years. At least 35 states have laws that criminalize actions that potentially expose other people to HIV, regardless of intent or actual transmission.[159] Many states' criminal laws discriminate against people living with HIV, such as laws that increase penalties for violations of general criminal laws if the individual also happens to be HIV positive.[160] Prosecutors may rely on newer technology to test

[155] *See California v. U.S. Dep't of Health & Hum. Servs.*, No. 25-CV-05536-VC, 2025 WL 2356224 (N.D. Cal. 2025), available at https://storage.courtlistener.com/recap/gov.uscourts.cand.452203/gov.uscourts.cand.452203.98.0_1.pdf; Ahmed Aboulenein & Kanishka Singh, *US Health Department Hands Over Medicaid Personal Data to ICE*, Reuters (July 17, 2025), https://www.reuters.com/business/healthcare-pharmaceuticals/us-health-department-hands-over-medicaid-personal-data-ice-2025-07-17/.

[156] Joseph Cox, *Here is the Agreement Giving ICE Medicaid Patients' Data*, 404 Media (Jan. 6, 2026), https://www.404media.co/here-is-the-agreement-giving-ice-medicaid-patients-data/.

[157] Order Granting Motion for a Temporary Restraining Order at 3, *Leonel Navarrete-Hernandez v. Todd Lyons*, No. 2:25-cv-05376 (C.D. Cal. 2025), https://www.courtlistener.com/docket/70533244/17/leonel-navarrete-hernandez-v-todd-lyons/.

[158] Ximena Bustillo & Jasmine Garsd, *Judge Says Trump Administration Violated court Order on Third-Country Deportations*, NPR (May 21, 2025) https://www.npr.org/2025/05/21/nx-s1-5406208/trump-administration-defends-flight-of-migrants-to-third-countries.

[159] EPIC et al., Comments on HHS HIV PrEP Database SORN at 6, https://epic.org/documents/comments-of-epic-chlp-prep4all-and-patient-privacy-rights-to-hhs-on-hiv-prep-database-sorn/.

[160] Ctr. For HIV Law & Pol'y, Mapping HIV Criminalization Laws in the US (Mar. 2025), https://www.hivlawandpolicy.org/sites/default/files/2025-03/Mapping%20HIV%20Criminalization%20Laws%20in%20the%20US%2C%20CHLP%202025.pdf.

genetic connections between HIV viruses, but often judges, attorneys, and law enforcement do not understand this technology well.[161] Entities that hold data related to HIV status often err, only increasing the risk of this data being exposed and used in harmful ways. On February 10, 2023, Lambda Legal announced a settlement over data breaches in the enrollment program for California's AIDS Drug Assistance Program.[162] In 2018, Aetna settled a lawsuit for accidentally revealing that people were taking PrEP and other HIV-related medications in the transparent windows of mailed envelopes.[163] And in 2019, a University of California at San Diego study on the impact of domestic violence, substance abuse, and other traumatic events for women with HIV experienced a substantial data breach exposing highly confidential information to a broad array of unauthorized staff.[164] These harms fall disproportionately on gay men, people who use drugs, and other marginalized communities.

While criminalizing health care that only affects certain groups of people—and especially marginalized communities—is not a new practice, the recent increase in surveillance and criminalization exacerbates previous harms and creates unprecedented fear. These are largely attacks on people who can get pregnant, trans and gender nonconforming people, queer people, and immigrants. Health disparities in these communities are worsened when people retreat from care due to fear and stigma.

2. *Policymakers have failed to strengthen outdated privacy laws, leaving companies free to engage in harmful data practices*

Existing laws and regulations offer only limited protections for personal health data. The main protections are provided by HIPAA, the FTC's unfair trade practices authority, and state privacy laws. HIPAA is not sufficient because it applies to only a narrow range of entities and contains many loopholes such as mandatory disclosure requirements. Without a comprehensive federal privacy law to safeguard health data in other contexts, patients are often left exposed. What protections do exist primarily flow from the Federal Trade Commission's authority

[161] *HIV Criminalization in the United States: A Sourcebook on State and Federal HIV Criminal Law and Practice*, Ctr. For HIV Law & Pol'y, 1-2 (2024) https://www.hivlawandpolicy.org/sites/default/files/2025-04/HIV%20Criminalization%20in%20the%20U.S.%20A%20Sourcebook%20on%20State%20Fed%20HIV%20Criminal%20Law%20and%20Practice%20011924.pdf.

[162] EPIC et al., Comments on HHS HIV PrEP Database SORN at 7, https://epic.org/documents/comments-of-epic-chlp-prep4all-and-patient-privacy-rights-to-hhs-on-hiv-prep-database-sorn/.

[163] *Id.*

[164] *Id.*

to regulate unfair and deceptive trade practices and state privacy laws. But, unfortunately, both the FTC Act and many state privacy laws have followed a weak "notice-and-choice" paradigm.

Privacy experts and advocates have long critiqued the notice-and-choice model of privacy regulation, in which companies provide "notice" of how they will use a person's data and (ostensibly) allow the person to make a "choice" about whether to provide that data. While sounding reasonable in the abstract, this model falls apart because it enables companies to use data for any purpose they choose, no matter how privacy-invasive, as long as it is disclosed in their privacy policy.[165] Numerous studies have shown that individuals generally do not understand privacy policies, lack the time to read them, and are minimally protected by them.[166] Even if a person does read a policy in its entirety, that policy does not provide a meaningful choice because the only option is to agree to the privacy policy or not use the service at all.

HIPAA

The main federal health privacy statute, HIPAA, is, unfortunately, outdated. The HIPAA Privacy Rule requires that covered entities provide individuals with notices that explain how they may use and disclose health information. The rule also provides individual privacy rights and includes provisions that allow individuals to give consent or authorization for specific uses and disclosures of their health information.[167]

HIPAA protections are also limited by the law's "coverage definition," which specifies which entities must comply with the law and leaves large swathes of health data unprotected. HIPAA applies to "covered entities," narrowly defined as healthcare providers, insurance companies, and their business associates.[168] As Part 2: Profiling of this report will explain in more detail, many entities that collect sensitive health information—such as search engine companies, wearable health device companies, and health applications—fall outside of HIPAA's coverage.

[165] Katherine J. Strandburg, Salome Viljoen & Helen Nissenbaum, *The Great Regulatory Dodge*, 37 Harvard J. Law & Tech 1231, 1235-36 (2023), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4852257.
[166] *Id.*
[167] *Summary of the HIPAA Privacy Rule*, HHS, *supra* note 36.
[168] *Id.*

HIPAA also introduces privacy loopholes through exceptions for law enforcement and other entities. For example, HIPAA's Privacy Rule allows healthcare providers and insurers to share patients' medical records with law enforcement without a search warrant.[169] This means that people's sensitive healthcare data may be shared in ways that could lead to their—and their healthcare providers'—prosecution and imprisonment.

FTC Section 5 Privacy Policy Enforcement

One of the few protections individuals have for health data held by non-HIPAA-covered entities is the unfair trade authority in Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices. With respect to deceptive practices, the FTC can pursue cases against companies that violate their own privacy policies or other representations. This means that the FTC's deception authority is also primarily based on the notice-and-choice model, since it involves companies providing "notice" to users or customers in the form of privacy policies, giving users the "choice" of whether to use the service or not, and holding the companies responsible if they misrepresented their activities. With respect to unfair practices, the FTC can pursue cases against "substantial" injuries that are not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition.[170] The FTC has taken action against companies for harmful data practices under its unfairness authority, albeit much less often than under its deception authority. The FTC also enforces the Health Breach Notification Rule, which requires companies, including app and device providers, to notify their customers if their unsecured, identifiable health information was breached.[171]

The FTC has used these authorities to curb harmful data practices. For example, the FTC sued data broker Kochava for selling consumers' location information that revealed people's visits to health facilities and other sensitive locations, alleging that the sale of sensitive data was unfair.[172] The FTC entered

[169] 45 C.F.R. § 164.512(f)(1)(i)–(ii).

[170] FTC Policy Statement on Unfairness, FTC (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.

[171] *Complying with FTC's Health Breach Notification Rule*, FTC (Jan. 2025), https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0.

[172] Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, FTC (Aug. 29, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

into a consent agreement with Flo Health, a fertility and menstrual tracking app, to settle allegations that the company deceptively shared users' sensitive health information with third parties despite promises to keep that information private.[173] However, the FTC's reliance on case-by-case enforcement of Section 5—rather than across-the-board trade rules,[174] for example—fails fully protect the public from health data-related harms. The pitfalls of notice and choice, combined with the FTC's limited resources and understaffing,[175] leave most individuals in the lurch when their health privacy is threatened or violated.

State Privacy Laws

Unlike the federal government, some states have passed strong health privacy protections. Washington's My Health My Data Act[176] and Illinois's Biometric Information Privacy Act[177] fill some of the gaps in health data protections left by HIPAA. Washington's MHMDA, for example, applies to *any* entity that holds protected health information and establishes privacy protections by default.[178] Unfortunately, many states have yet to pass such a law, meaning that while these protections are more robust, they are not widespread.

While HIPAA, the FTC's authorities, and state privacy statutes offer various protections for health data, this uneven constellation of laws leaves significant gaps in coverage. These gaps create privacy harms which are most acutely felt by marginalized groups.

3. *Recently enacted laws that will significantly reduce Medicaid spending will likely result in far less funding for healthcare entities in general, diminishing privacy protections.*

Health systems with fewer resources are less successful guardians of personal health information. Cybersecurity experts report that even well-

[173] *Flo Health, Inc.*, FTC (June 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[174] 15 U.S.C. § 57a(a)(1)(B).

[175] Common Sense Media, *Budget Cuts to the Federal Trade Commission Will Hurt Kids and Consumers* (July 13, 2023), https://www.commonsensemedia.org/kids-action/articles/budget-cuts-to-the-federal-trade-commission-will-hurt-kids-and-consumers.

[176] Wash. Rev. Code §19.373 (2023).

[177] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. § 14, *available at* https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57.

[178] Suzanne Bernstein, & Sara Geoghegan, *Alive and Kicking: Washington State's My Health My Data Act Goes into Effect Today*, Elec. Privacy Info. Ctr. (Apr. 1, 2024), https://epic.org/alive-and-kicking-washington-states-my-health-my-data-act-goes-into-effect-today/.

resourced healthcare systems have far smaller budgets for cybersecurity than other sectors like finance and tech.[179] Less well-resourced healthcare providers, especially rural ones, are particularly vulnerable.[180] This can put patients' privacy at severe risk of a data breach.

Recent changes in federal law are likely to significantly impact the financial health of many health systems, potentially leading to a weakening of privacy protections for patients. The Congressional Budget Office's July 2025 score of Public Law 119-21, formerly known as the "One Big Beautiful Bill," estimated that the bill would reduce federal Medicaid funding of healthcare systems by up to $1 trillion over 10 years.[181] This would represent 14% reduction of federal spending on Medicaid over the next ten years.[182] These cuts will likely exacerbate the cybersecurity shortfall in health care, meaning private health data will be at even greater risk of breach.

ii. Recent Technological Developments Create New Health Privacy Risks

Technologies can both enhance and invade our privacy, but recent developments have unfortunately tended toward the latter. The expansion of commercial surveillance capabilities, developed to fuel targeted advertising systems, has facilitated the creation of enormous databases of sensitive information, including health data. This health information is usually not protected by HIPAA because the law does not cover the entities collecting it. The lack of privacy protection for the sensitive information in these databases means they can be funneled into law enforcement investigations without any oversight, they have been subject to devastating data breaches, and other severe consequences. And

[179] Andrea Fox, *Where Rural Hospitals Can Find Cybersecurity Threat Intelligence*, Healthcare IT News (Apr. 23, 2025), https://www.healthcareitnews.com/news/where-rural-hospitals-can-find-cybersecurity-threat-intelligence; Salem T. Argaw *et al.*, *Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks*, 20 BMC Med. Inform. & Decision Making 207 (2020), https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7.

[180] Anna Ribeiro, *HSCC Warns of Growing Cybersecurity Threats to Resource-Strained Healthcare Providers, Urges Immediate Action*, IndustrialCyber.co (May 12, 2025), https://industrialcyber.co/medical/hscc-warns-of-growing-cybersecurity-threats-to-resource-strained-healthcare-providers-urges-immediate-action/.

[181] Rhiannon Euhus, Elizabeth Williams, Alice Burns & Robin Rudowitz, *Allocating CBO's Estimates of Federal Medicaid Spending Reductions Across the States: Senate Reconciliation Bill*, KFF (July 23, 2025), https://www.kff.org/medicaid/issue-brief/allocating-cbos-estimates-of-federal-medicaid-spending-reductions-across-the-states-senate-reconciliation-bill/.

[182] *Id.*

technology companies that regularly violate privacy are becoming increasingly invested in the healthcare space, further intensifying privacy risks.

This subsection explains the changes in technology that have given rise to the health data privacy crisis. The rise in wearable technologies and chatbots that collect health related information has created significant new privacy risks. Data brokers amplify these risks by selling health related information without meaningful restrictions. Commercial surveillance builds vast pools of data ripe for law enforcement access via surveillance techniques like geofence and reverse warrants. Tech behemoths like Amazon have expanded their reach beyond online marketplaces, cloud storage, data aggregation, and advertising to include health care. And the increasing digitization of health services creates new barriers to access, especially for people with disabilities, limited digital literacy, and fewer resources.

1. *A rise in consumer-facing technologies that collect health data, such as smartphone apps, wearables, internet search engines, and chatbots, has exposed gaps in health data protection regimes.*

The gaps in privacy laws, combined with the digital transformation, mean an enormous number of private entities are collecting and compiling health data with very few privacy obligations. Web pages, search engines, smartphone apps, wearable devices, and other online tools all collect and share health data.

Simply browsing the internet exposes one to extensive tracking. A study by the group Privacy International analyzed 136 popular mental health web pages in Europe, finding that 98% of them contained third-party elements that tracked users, 76% of which did so for marketing purposes.[183] These trackers enable data brokers to share or sell the fact that someone visited a website concerning clinical depression with nearly any buyer, limited only by the broker's own policies.[184]

People also entrust search engines with enormous amounts of sensitive health data that enjoy little privacy protection. For instance, Google has become a go-to source for medical information, with one study finding that 89% of patients Googled their symptoms before going to a doctor.[185] This translates to an

[183] Privacy International, *Privacy International Study Shows Your Mental Health Is For Sale* (Sept. 3, 2019), https://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale.
[184] *Id.*
[185] Alex Guarino, Study Finds US Citizens Turn to Google Before Their Doctor, WECT (June 24, 2019), https://www.wect.com/2019/06/24/study-finds-us-citizens-turn-google-before-their-doctor/.

estimated 1 billion health-related search queries per day, accounting for about 7% of Google's daily searches in 2020.[186] People tend to trust Google with sensitive health searches despite the lack of explicit privacy protections beyond the company's own privacy policies. For example, "[i]n the weeks after the Dobbs decision was issued, Google searches for 'medication abortion pills' [went] up by 70 percent; 'do abortion pills expire' [went] up 350 percent; 'abortion pills Amazon' [went] up 80 percent. People Googling for 'states where abortion is illegal map' [went] up over 1,050 percent in [a] month."[187]

Smartphone apps and wearable devices are also collecting large amounts of health information with few privacy obligations. More than 350,000 apps promise to help people with a wide range of needs, from weight tracking and mental health issues to identifying diseases.[188] Recent research shows that up to 80% of iOS apps track private user data, with 74% of the most popular apps collecting more than they actually need to render the services the user wants.[189] Health apps are notoriously invasive. Privacy International found that some period tracking apps collect and infer data that users do not want or need (but which advertisers and law enforcement may be very interested in), such as users' sexual behavior patterns and medication intake.[190] As noted above, the FTC finalized a settlement agreement with Flo Health, another period tracking app, after the company shared millions of users' tracking information with marketing and analytics firms and tech companies, including Facebook and Google.[191]

The mental health app market reached $7.48 billion in 2024, and many developers in that market appear to have given privacy short shrift in their pursuit of profit.[192] The Mozilla Foundation, which regularly reviews the privacy practices of various smartphone apps, reported in 2023 that 17 of the top 27 mental health

[186] Amit Rawal, *Google's New Health-Search Engine*, Medium (Jan. 21, 2020), https://medium.com/swlh/googles-new-healthcare-data-search-engine-9e6d824b3ccd.

[187] Jennifer Gerson, *Abortion Rights Supporters Are Trying to Reduce Barriers to Access Through Search Keywords*, 19th News (July 27, 2022), https://19thnews.org/2022/07/abortion-access-activists-google-keywords-seo/.

[188] Claudia López Lloreda, *For Help Apps, Questions Over Privacy and Efficacy*, Undark (Apr. 9, 2025), https://undark.org/2025/04/09/health-apps-data-oversight/.

[189] Julia Olech, *The Digital Therapist Guide: The Hidden Privacy Dangers of Mental Health Apps*, https://www.privateinternetaccess.com/blog/privacy-dangers-mental-health-apps.

[190] Patrick K. Lin, *How Data Privacy May Be Affected If* Roe v. Wade *Is Overturned*, Tech Policy Press (June 3, 2022), https://www.techpolicy.press/how-data-privacy-may-be-affected-if-roe-v-wade-is-overturned/.

[191] *Id.*

[192] Olech, *supra* note 189.

apps had “pretty bad” or “worse” privacy and security practices.[193] Mental health apps often collect extremely sensitive information such as mental health diagnoses, prescription information, and stories of personal trauma. But like many other apps, their developers too often put profit over health privacy. For example:

- The FTC issued a $7.8 million judgment against popular mental health app Betterhelp for promising not to share sensitive mental health information for advertising when it did exactly that.[194]
- Talkspace, another popular mental health app, buried in its privacy policy that it would share information about gender identity, sexual orientation, and depression status, among other categories, to sell ads.[195]
- Headspace Health, a company with one of Mozilla’s worst ratings for wellness app privacy practices, purchased Shine, an app created by two women of color to focus on serving underrepresented groups, thereby gaining access to the latter’s data.[196]
- A whistleblower at the Crisis Text Line, a hotline for people considering suicide, reported that the non-profit sold user data to train its for-profit partner’s AI chatbot.[197]

Lastly, the meteoric rise of chatbot usage poses a grave health privacy threat. Americans are turning to chatbots for health questions, confiding very sensitive information in technologies and companies that aren’t covered by HIPAA and may not be protected under any federal privacy law.[198] About one in six adults, and about 25% of people younger than 30, report having used chatbots for medical advice.[199] Chatbots may be attractive alternatives to traditional therapy and doctors, especially since health care can be so expensive and difficult to access. But, unlike doctors and therapists, chatbots are not generally subject to

[193] Jen Caltrider, Misha Rykov & Zoë MacDonald, *Are Mental Health Apps Better or Worse at Privacy in 2023?*, Mozilla Foundation (May 1, 2023), https://www.mozillafoundation.org/en/privacynotincluded/articles/are-mental-health-apps-better-or-worse-at-privacy-in-2023/.

[194] Olech, *supra* note 189.

[195] *Id.*

[196] *Id.*

[197] Trans Lifeline, The Problem with 988: How America’s Largest Hotline Violates Consent, Compromises Safety, and Fails the People at 48 (2024), *available at* https://translifeline.org/wp-content/uploads/2024/10/The-Problem-with-988-Report-October-2024-Text.pdf.

[198] Teddy Rosenbluth, *Dr. Chatbot Will See You Now*, N.Y. Times (Sept. 11, 2024), https://www.nytimes.com/2024/09/11/health/chatbots-health-diagnosis-treatments.html.

[199] *Id.*

demanding privacy and security requirements. People using chatbots are exposing information to entities not covered by HIPAA, such as Microsoft and Google. Researchers have shown serious privacy and data security risks with this technology, as explained in Part 4: Artificial Intelligence of this report.

2. *A lack of data broker regulation amplifies health privacy risks.*

Data brokers are entities that buy, aggregate, disclose, and share (sometimes billions of) personal data elements—information which can reveal health status and other intimate details about an individual. Data brokers build dossiers of personal information to profile people, often to target them with ads. Many of these companies do not interact directly with consumers, and they largely operate without our knowledge or consent. The enormous volume of information collected about people as they browse the web and use their digital devices is often channeled to data brokers, which amplifies privacy risks and harms. Trafficking in individuals' personal information has become a booming industry in the absence of a federal data privacy law, and health information is no exception.

The result is a frightening one for health privacy, as studies have shown that it is easy and relatively cheap for individuals, companies, and other data brokers to purchase sensitive information about specifically identified people from data brokers. This information is often available at minimal cost. In one study, researchers contacted 37 data brokers to buy mental health data.[200] The ten most responsive brokers to the researchers advertised highly sensitive data, including information on people who had "depression, attention disorder, insomnia, anxiety, ADD, and bipolar disorder as well as data on ethnicity, age, gender, zip code, religion, children in the home, marital status, net worth, credit score, date of birth, and single parent status."[201] Many of these brokers provided the information in a format that enabled the purchaser to identify specific individuals within the data set.[202]

Data brokers sell information that can enable the tracking of individuals. For example, location information is extremely sensitive. Data brokers such as Near, Placer.ai, and Babel Street collect location information from apps and websites

[200] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data* at 4 , Duke Sanford Sch. of Pub. Pol'y (Feb. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.

[201] *Id.*

[202] *Id.*

and sell it to virtually any interested party.[203] Near sold the location data of people seeking abortions to anti-abortion groups, and Placer.ai offered heat maps showing where visitors to Planned Parenthood clinics lived.[204] Privacy advocates purchased Babel Street data to show it could be used to track an individual who crossed state lines to visit an abortion clinic and then returned home to investigate the company.[205] Although location data may be sold in deidentified form, it is often inherently reidentifiable.

3. *Expanded consumer surveillance feeds powerful privacy-invasive law enforcement techniques such as reverse warrants.*

Consumer surveillance tools and data broker dossiers double as mechanisms for government surveillance. This subsection discusses reverse warrants, geofences, and Fourth Amendment loopholes for data brokers.

Law enforcement can piggyback on private companies' data collection through investigative techniques referred to as "reverse warrants," which include geofence warrants and reverse keyword warrants. These warrants turn the investigative process on its head. Instead of identifying suspects for investigation based on individualized suspicion and evidence, law enforcement agencies and courts can sometimes compel companies to trawl through their records and return a list of multiple users or identifiers for further investigation. This is information that a law enforcement agency could typically not collect itself without running afoul of the Fourth Amendment; it is businesses' own data collection practices that make these surveillance mechanisms possible. Geofence warrants compel companies to disclose information about who was within a specific area at a specific time (as reflected in location data that the company collects).[206] Keyword warrants compel companies to provide data on users who made specific search queries.[207]

Reverse warrants present significant health privacy risks, especially for communities that are disproportionately policed. For example, geofence warrants

[203] Lisa Femia, *Location Tracking Tools Endanger Abortion Access. Lawmakers Must Act Now*, Elec. Frontier Found. (Dec. 4, 2024), https://www.eff.org/deeplinks/2024/12/location-tracking-tools-endanger-abortion-access-lawmakers-must-act-now.
[204] *Id.*
[205] Joseph Cox, *Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics*, 404 Media (Oct. 23, 2024), https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/.
[206] Nat'l Ass'n of Crim. Def. Laws., *Reverse Search Warrants*, https://www.nacdl.org/Landing/Reverse-Search-Warrants.
[207] *Id.*

might reveal everyone visiting a particular abortion clinic or law office offering immigration services to low-income clients, while keyword warrants might reveal anyone searching keywords such as “mifepristone,” “AIDS symptoms,” or “what to do if I lost my visa” during a particular window of time. Law enforcement had used Google searches and similar web history to investigate at least two abortion cases, even before *Dobbs* was even decided.[208] Investigators accessed searches for at-home abortion drugs in both cases, indicting one woman who had searched for abortion pills online before suffering a miscarriage.[209]

Law enforcement use of reverse warrants has grown almost exponentially. The number of geofence warrants Google received in federal investigations grew by 1,171% between 2018 and 2020. The number of geofence warrants issued to Google by state and local law enforcement grew by 813% in California, 901% in Florida, 1,291% in Michigan, 1,867% in Missouri, and 5,333% in Massachusetts during that same time period.[210] As of 2020, Geofence requests constituted more than 25% of the warrants received by Google for digital information.[211]

Courts evaluating the constitutionality of reverse warrants have reached conflicting conclusions, meaning that protections against searches of one’s digital footprint can vary significantly according to geography. For instance, the Fourth and Fifth Circuit Courts of Appeals have split over whether geofence warrants are categorically unconstitutional, with the Fifth Circuit ruling they are and the Fourth Circuit ruling they are not.[212] In *People v. Seymour*, one of a handful of cases to consider the constitutionality of keyword warrants,[213] the Colorado Supreme Court recognized that users have a constitutionally protected privacy interest in their search histories, but it avoided answering many other important questions about

[208] Scott Ikeda, *Reverse Google Searches Face Increased Scrutiny as Fears of Keyword Warrants for Abortion Seekers Grow*, CPO Magazine (July 18, 2022), https://www.cpomagazine.com/data-privacy/reverse-google-searches-face-increased-scrutiny-as-fears-of-keyword-warrants-for-abortion-seekers-grow/.
[209] *Id.*
[210] Chad Marlow & Jennifer Stisa Granick, *Celebrating An Important Victory in the Ongoing Fight Against Reverse Warrants*, ACLU (Jan. 29, 2024), https://www.aclu.org/news/privacy-technology/fight-against-reverse-warrants-victory.
[211] Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the US*, Wired (Aug. 27, 2021), https://www.wired.com/story/geofence-warrants-google/.
[212] Jackie O’Neil, *Much Ado About Geofence Warrants*, Harvard L. Rev. Blog (Feb. 18, 2025), https://harvardlawreview.org/blog/2025/02/much-ado-about-geofence-warrants/.
[213] John Villasenor, *Keyword Search Warrants and the Fourth Amendment*, Brookings (Feb. 22, 2024), https://www.brookings.edu/articles/keyword-search-warrants-and-the-fourth-amendment/.

how and when reverse warrants are constitutional because it ruled that law enforcement had relied in good faith on the warrant they obtained in that case.[214]

In 2024, Google announced it would alter Android phone settings to ensure that location data is stored only on the user's device by default, a change which significantly limits the ability of investigators to rely on geofence warrants.[215] But there is still reason for skepticism, as Google has a history of failing to fulfill its privacy promises.[216] Meanwhile, many other companies routinely collect location data that can support similar warrants such as Lyft, Uber, and Snapchat.[217]

Data brokers also offer law enforcement a major Fourth Amendment loophole. Under current law, the government's purchase of information from a data broker does not require a warrant and is subject to few other restrictions. For example, immigration officials obtained access to a database of health and care insurance claims, including 1.8 billion insurance claims and 58 million medical bills, and used this information to track down people for deportation.[218] Immigration and Customs Enforcement (ICE) has purchased databases containing location data from millions of cellphone users.[219] As noted earlier, these data can reveal who is visiting an abortion center, where they live, what someone's gender identity is, and more. Legislation to close this loophole, the Fourth Amendment Is Not For Sale Act, was originally introduced by Senator Ron Wyden in 2021 and passed the House of Representatives in 2024, but has not yet been taken up by the Senate.[220] In 2025, Montana became the first state to pass a law prohibiting law

[214] EPIC, *Colorado Supreme Court Condones Law Enforcement Use of Dangerous Reverse Keyword Warrant*, (Oct. 20, 2023), https://epic.org/colorado-supreme-court-condones-law-enforcement-use-of-dangerous-reverse-keyword-warrant/.
[215] Mario McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/.
[216] Sara Geoghegan, *Google's Location Data Policy Update: Why Users Need More Than Pinkie Promises to Protect Their Most Sensitive Information*, EPIC (Jan. 31, 2024), https://epic.org/googles-location-data-policy-update-why-users-need-more-than-pinkie-promises-to-protect-their-most-sensitive-information/.
[217] O'Neil, *supra* note 212
[218] Joseph Cox, *ICE Is Searching a Massive Insurance and Medical Bill Database to Find Deportation Targets*, 404 Media (July 9, 2025), https://www.404media.co/ice-is-searching-a-massive-insurance-and-medical-bill-database-to-find-deportation-targets/.
[219] Patrick K. Lin, *How Data Privacy May Be Affected If* Roe v. Wade *Is Overturned*, Tech Policy Press (June 3, 2022), https://www.techpolicy.press/how-data-privacy-may-be-affected-if-roe-v-wade-is-overturned/.
[220] *EPIC Statement on House Passage of Fourth Amendment Is Not For Sale Act*, EPIC (Apr. 17, 2024), https://epic.org/epic-statement-on-house-passage-of-fourth-amendment-is-not-for-sale-act/.

enforcement from purchasing certain forms of data from data brokers, closing the data broker loophole.[221]

Even beyond reverse warrants and the data broker loophole, companies' databases of personal information may be attractive targets for law enforcement. For example, Target reportedly sent maternity and pregnancy-related advertisements to a teenager before she told her family she was pregnant.[222] As one journalist explained, "all Target customers are assigned a Guest ID. Associated with this ID is information on 'your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit.'"[223] Analyzing this data, combined with a customer's purchase history, the company was able to produce a "pregnancy prediction" score, which even included an estimate of the customer's due date.[224] All of this would be an attractive target for a subpoena, as law enforcement has begun to track people's pregnancies more closely if, for example, law enforcement was investigating a person suspected of obtaining an illegal abortion and sought their purchase history from a store to confirm the person's pregnancy status.

4. *Technology companies such as Amazon have increasingly entered the healthcare provision space.*

The consolidation of healthcare companies, particularly under the umbrella of technology companies that already buy and sell vast amounts of user data, poses another significant privacy threat. Amazon's purchase of One Medical provides an illustrative example. Amazon collects enormous amounts of information about its users to sell them more stuff. In 2023, Amazon acquired One Medical, a healthcare provider.[225] Shortly after, users—including a journalist—reported receiving creepy ads, such as links to prescription medicines for the

[221] *Montana Becomes First State to Close the Law Enforcement Data Broker Loophole*, EFF (May 14, 2025), https://www.eff.org/deeplinks/2025/05/montana-becomes-first-state-close-law-enforcement-data-broker-loophole.

[222] Kelly Bourdet, *Target Knows You're Pregnant*, Vice (Feb. 18, 2012), https://www.vice.com/en/article/target-knows-you-re-pregnant/.

[223] *Id.*

[224] *Id.*

[225] *5 Things to Know About Amazon's Recent One Medical Acquisition*, American Hospital Ass'n, (Mar. 7, 2023), https://www.aha.org/aha-center-health-innovation-market-scan/2023-03-07-5-things-know-about-amazons-recent-one-medical-acquisition.

health conditions (that they had not disclosed to Amazon) when they were ordering groceries on Amazon Fresh.[226] Google's acquisition of FitBit, a wearable health tracker, represents similar privacy risks.[227] The few barriers that prevent businesses from sharing information become even weaker when one corporation owns a wide range of assets, including medical clinics, online marketplaces, IT services, grocery stores, video production companies, streaming services, and more.

5. *Healthcare providers increasingly rely on digital technologies to interact with and treat patients, creating increased privacy and accessibility risks.*

Over the past 15 years, the healthcare system has increasingly depended on digital technologies.[228] While this shift can benefit patients, it also poses threats to health equity. Relying on technologies such as apps and wearables can present privacy risks to patients that may cause some to avoid or delay seeking healthcare.[229] Moreover, the use of digital health technologies can present accessibility and digital literacy barriers.[230] Digital systems must be accessible to users from diverse cultural backgrounds, with varying physical abilities, and different levels of digital literacy—meaning the skills necessary for technology use and problem-solving.[231] People who do not speak English as a first language, who are intimidated by technology, or who do not have access to reliable internet or personal devices can all face significant barriers to receiving adequate health care when the use of digital systems becomes a prerequisite to that care.

The drastic expansion of commercial surveillance—including the rise in wearable technologies and chatbots, data brokers' unregulated data sharing, invasive law enforcement warrants, Big Tech's foray into health care, and the digitization of health services—creates an ecosystem of unprotected health data.

[226] Adam Clark Estes, *Why Your Amazon Recommendations Are Getting a Little Too Creepy*, Vox (Aug. 28, 2024), https://www.vox.com/technology/369302/amazon-one-medical-pharmacy-prescription-drugs
[227] *Google Tries to Allay Fitbit-Deal Privacy Fears*, BBC (Jan. 14, 2021), https://www.bbc.com/news/technology-55662659.
[228] Lara Whitehead, Jason Talevski, Farhad Fatehi & Alison Beauchamp, *Barriers To and Facilitators of Digital Health Among Culturally and Linguistically Diverse Populations: Qualitative Systematic Review*, 25 J. Med. Internet Res. 1, 1 (2023), *available at* https://www.jmir.org/2023/1/e42719/PDF.
[229] *Id.* at 13.
[230] *Id.* at 11.
[231] *Id.*

C. Impact Pathways: How Privacy Failures Create Health Inequities

Privacy failures threaten the healthcare system by imposing individual and systemic harms. Individuals may choose to forego or delay necessary care when they experience fear or mistrust. Similarly, a digital-first approach can exclude people for whom digital systems are not accessible. On a broader scale, these individual harms can aggregate to impact the overall efficiency and quality of the healthcare system.

i. Privacy and Accessibility Failures Can Impose Barriers to Accessing Health Care, Widening Health Inequities

Individuals often need to share highly sensitive information to receive quality health care. If someone doesn't trust that their data will be protected, they are less likely to seek care. And if digital literacy is required to access health care, then some people are inevitably excluded unless accessibility is built in. These burdens disproportionately fall on communities that already struggle to access quality health care.

This subsection first explains how the fear of criminal punishment, discrimination, and data security incidents causes people to not seek health care or to participate less fully in their health care, leading to downstream harms to their health. It then explains how digital systems that fail to consider digital literacy and people with disabilities widen health disparities.

1. Some people do not seek health care, or provide insufficient information required for quality health care, when they fear that disclosing their health data will have harmful downstream impacts on their lives.

Quality medical care depends on a patient's willingness to speak freely with healthcare providers and to provide accurate information. The serious privacy risks described above disincentivize people from being open when they seek care. This is especially true for people from marginalized communities who may face criminal prosecution, deportation, public shaming, and economic consequences from the decision to provide accurate information to a healthcare provider or non-traditional health source, such as an app.

HIPAA's Privacy Rule was enacted, in part, based on this understanding of the essential role privacy plays in the medical field. When promulgating the rule, HHS noted that "the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers."[232] At the time, "one in six Americans reported that they ha[d] taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether" to protect their privacy.[233] Even 78% of physicians reported withholding important information from a patient's medical record due to privacy concerns.[234] HHS noted that inappropriate medical disclosures had led to "alienation of family and friends" and "public humiliation."[235] For example, a 30-year FBI veteran was placed on administrative leave when his pharmacy released information about his depression treatment, and a political candidate's campaign was nearly derailed when details of past treatment for psychiatric issues that had no bearing on her ability to serve in office came to light.[236]

The legal and technical erosions of health privacy described above, along with HIPAA's limitations, mean that this same type of erosion in healthcare provision is playing out now.

Fear of Criminal Punishment

Studies have shown that knowledge of the existence of government surveillance systems imposes a chilling effect.[237] The evidence indicates that the increased criminalization and surveillance of health activities and health data are reducing people's willingness to access care.

Pregnant people, people experiencing mental illness, immigrants, and others—along with their doctors—have described an increased unwillingness in recent years to seek health care due to privacy concerns. If/When/How, an abortion rights group that operates the Repro Legal Helpline, reported that calls from people distressed about sharing any pregnancy-related information with their

[232] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82466 (Dec. 28, 2000), *available at* https://www.govinfo.gov/content/pkg/FR-2000-12-28/pdf/00-32678.pdf.
[233] *Id.* at 82467.
[234] *Id.* at 82468.
[235] *Id.* at 82761.
[236] *Id.* at 82468.
[237] Jon Peneny, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L. J. 117, 153 (2016).

healthcare providers have skyrocketed since the *Dobbs* decision.[238] They say an increasing number of people contacting the Helpline are avoiding the healthcare system altogether due to fears their health data may be used against them if they have a miscarriage or abortion.[239]

After the *Dobbs* decision, researchers saw precipitous drops in the use of women's health apps: 18.6% fewer sessions using the apps, and 66.7% less time spent on the apps.[240] The same is true for people's willingness even to read Wikipedia articles or conduct Google searches related to women's health apps.[241] Transgender people experiencing suicidality have avoided calling mental health hotlines for fear that it will result in police showing up to their doors.[242] This is especially true because an involuntary psychiatric hospitalization can later result in someone being denied gender-affirming care.[243]

Similarly, doctors and patients have reported that undocumented immigrants and their family members have been delaying or avoiding necessary care. Doctors report that, due to these concerns, "some patients are avoiding getting the health care they need" and that patients have "waited too long to come in for health care."[244] Some "patients are arriving sicker," including arriving with late-stage cancers that may have been less severe with earlier treatment.[245] This applies not only to undocumented immigrants, but also "visa-holding immigrants, mixed-status families, and even U.S. citizens."[246]

[238] Kebé, Elizabeth Ling & Kylee Sunderlin, *State Violence and the Far-Reaching Impact of Dobbs* at 6, If/When/How (2024), *available at* https://ifwhenhow.org/wp-content/uploads/2024/06/Repro-Legal-Helpline-Report-June-24.pdf.
[239] *Id.*
[240] Naveen Basavaraj, Uttara M. Ananthakrishnan & Catherine Tucker, *The Chilling Effect of Dobbs: A Study of Mobile Health Apps Usage*, MIT Sloan Research Paper No. 7156-24 at 5 (Aug. 13, 2024).
[241] Jonathon W. Penney, Danielle Keats Citron & Alexis Shore Ingber, *The Chilling Effects of* Dobbs, 77 Florida L. Rev. 357, 386-399 (2025).
[242] *The Problem with 988: How America's Largest Hotline Violates Consent, Compromises Safety, and Fails the People*, Trans Lifeline at 16, 28 (2024), *available at* https://translifeline.org/wp-content/uploads/2024/10/The-Problem-with-988-Report-October-2024-Text.pdf.
[243]*Id.* at 44.
[244] Sara Moniuszko, *Doctors Fears ICE Agents in Health Facilities Are Deterring People From Seeking Care*, CBS News (July 9, 2025), https://www.cbsnews.com/news/doctors-fear-ice-agents-health-care-facilities-deterring-people/.
[245] Physicians for Human Rights, *Consequences of Fear: How the Trump Administration's Immigration Policies and Rhetoric Block Access to Health Care* at 6 (Apr. 2025), https://phr.org/wp-content/uploads/2025/04/Consequences-of-Fear_Research-Brief_PHR_April-2025.pdf.
[246] *Id.*

Discrimination Fears

Because some marginalized communities are less likely to obtain healthcare from entities covered by HIPAA, they face a disproportionately higher risk of data breach and privacy invasion. For example, LGBTQ+ people are much more likely to use online and app-based health resources than other communities due to fears of discrimination from traditional healthcare providers.[247] While HIPAA doesn't provide sufficient protection, it offers more protection than most apps' and websites' privacy policies. This means that LGBTQ+ people are much more likely to access privacy-invasive health and wellness services than non-LGBTQ+ people because of discrimination fears, putting them at greater risk of identity theft, cyber-stalking, and other privacy harms.

Data Security Fears

Individuals may also be unwilling to disclose accurate and complete medical information because of the fear of data breaches. The lack of adequate privacy protection enables healthcare systems and private actors to compile large databases filled with valuable information, creating attractive targets for cybercriminals. Reporting on the large volume of devastating data breaches has led consumers to reasonably fear what might happen if their data is included in an attack. Patients have reported withholding complete or accurate health information due to concerns about poor data security.[248] One study reported that Black Americans are especially sensitive to this concern,[249] and another noted that non-English speakers were less likely to provide entirely accurate information when they had to trust a translator.[250]

Fears of law enforcement, criminalization, discrimination, stigma, and cybersecurity incidents prevent people from sharing their information more fully

[247] Judy Wang, Jeter Sison, & Jordan Wrigley, *Out, Not Outed: Privacy for Sexual Health, Orientations, and Gender Identities*, Future of Privacy Forum (Oct. 11, 2024), https://fpf.org/blog/out-not-outed-privacy-for-sexual-health-orientations-and-gender-identities/.

[248] Javad Pool, Saeed Akhlaghpour, Farhad Fatehi & Andrew Burton-Jones, *A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review*, 74 Int'l J. Info. Management 1, 13 (2024), *available at* https://www.sciencedirect.com/science/article/pii/S0268401223001007.

[249] Lara Whitehead, Jason Talevski, Farhad Fatehi & Alison Beauchamp, *Barriers To and Facilitators of Digital Health Among Culturally and Linguistically Diverse Populations: Qualitative Systematic Review*, 25 J. Med. Internet Res. 1, 13 (2023), *available at* https://www.jmir.org/2023/1/e42719/PDF.

[250] *Id.*

with providers and breaks down trust. People retreat from care due to these burdens which are borne disproportionately by marginalized groups.

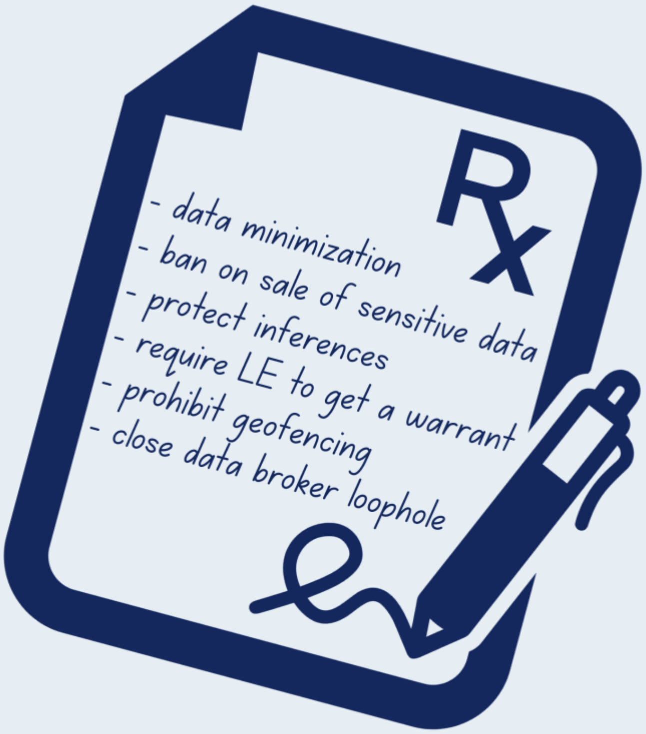
2. *Some people are not able to access adequate health care when implementation of digital systems fails to account for digital literacy and accessibility barriers.*

Healthcare systems that assume people have high levels of digital literacy can be exclusionary, degrading health outcomes. A research meta-survey showed that digital literacy posed a barrier for many individuals to receiving health care, especially those from immigrant communities, Black Americans, and Indigenous Americans:

- Limited English literacy, combined with an overwhelming volume of text and the use of medical terminology, poses a significant barrier across many cultural groups.[251]
- 38% of studies observed that people across all cultural groups and ages felt unable to "open an app, use SMS text messaging, or manually enter data."[252]
- Feeling intimidated by technology posed a disproportionate barrier for older Greek and Italian immigrants, Indigenous people, and Asian Indian immigrants.[253]
- Numerous studies reported that issues with internet connectivity and reliability, as well as phone affordability, posed a barrier to healthcare access across a range of cultural groups.[254]
- Studies among Black Americans, Hispanic, and Latino Americans found that poor timing of SMS text messages and the provision of enormous amounts of complicated information at once interfered with individuals' ability to access healthcare.[255]

[251] *Id.* at 1, 12.
[252] *Id.* at 1, 11.
[253] *Id.*
[254] *Id.*
[255] *Id.* 1, 12.

Proposed Solutions to Protect the Privacy of Health Data


Rx
- data minimization
- ban on sale of sensitive data
- protect inferences
- require LE to get a warrant
- prohibit geofencing
- close data broker loophole

This section offers solutions and strategies to address the hazardous personal data practices and harms identified above.

The most effective way to protect personal health data from misuse and unauthorized access is a strong data minimization standard. Data minimization is the practice of limiting the collection, use, transfer, and retention of personal information to that which is reasonably or strictly necessary to achieve certain ends—for example, providing a product or service requested by a consumer.[256] Data minimization rules may also enumerate permissible uses of data that extend beyond the immediate provision of the product or service sought by a consumer, such as fraud detection during online payment processing or the use of data for public health research. These permitted uses must be expressly enumerated and narrowly tailored. Data minimization has heightened restrictions for more sensitive information—like health information—that may only be collected, processed, and retained as *strictly* necessary to achieve the primary purpose for which it was collected. A comprehensive data protection framework requires that a business handling personal information establishes robust cybersecurity safeguards to protect the security of data.[257] It also prohibits the sale of sensitive information to protect the types of data that can be most revealing.[258]

[256] EPIC, *Disrupting Data Abuse*, *supra* note 72 at 1, 30-66.
[257] Maryland requires that controllers "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue[.]" Md. Code Ann., Com. Law § 14-4707(b)(ii).
[258] Md. Code Ann., Com. Law § 14-4707(a)(2).

Data segmentation is another solution for particularly sensitive information that is collected by providers. Data segmentation is "the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share."[259] With respect to health information, certain types of especially sensitive information, like whether a patient seeks abortion care or gender affirming care, may be segmented into a different group than the rest of the patient's health information. This allows providers to offer greater protection for specific segments and share this information less freely, as the information that has been segmented may not be necessary for a provider to share in many circumstances.

There are many other policy and practice changes that would help protect health privacy and in turn promote health equity. Limiting law enforcement access to data without express consent of a patient, restricting the use of reverse warrants, and prohibiting the geofencing of health facilities would help protect people against the criminalization of health care. With respect to commercial surveillance, regulating data brokers would be a significant step towards protecting our privacy. Preventing data brokers from trading in health related information or inferences and closing the data broker loophole would help to limit harms caused by data brokers.

Finally, increasing funding for health services would help to protect patient privacy and promote health equity. People should not have to trade privacy for more affordable care, as is often the case when people cannot easily access a doctor or reliable care. When people turn to apps or less regulated entities because they are easily accessible, they trade security and privacy for ease of access. Investing in cybersecurity standards, closing the digital divide, and lowering barriers to access reliable and privacy-protective care will promote better health outcomes for us all and increase health equity.

[259] Melissa Goldstein and Alison Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, Dep't of Health and Human Services, Office of the National Coordinator for Health IT (Sept. 29, 2010), https://hsrc.himmelfarb.gwu.edu/sphhs_policy_facpubs/224/.

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.][260]

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[.]"[261]

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[.]"[262]

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

3) A **ban on the sale of sensitive data** prohibits out-of-context uses.

A controller may not sell sensitive data, including health data.[263]

4) Health-related **inferences** should be protected and included in the definition of "health data."

Washington's My Health, My Data Act defines consumer health data as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[264] This includes, but is not limited to: individual health conditions, medical interventions, surgeries, use or purchase of prescribed medications, bodily functions, vital signs, gender-affirming care information, reproductive or sexual health information, biometric data, genetic data, precise location information that could reasonably indicate a person's attempt to receive health services or supplies.[265] Importantly, this definition includes any information that a regulated entity processes to associate or identify a person with health data "that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)."[266]

Maryland's definition of "sensitive data" includes personal data that reveals consumer health data,[267] which is defined as personal data that a controller uses to identify a consumer's physical or mental health status, including data related to gender-affirming treatment or reproductive or sexual health care.[268]

5) Require **data segmentation.**

Data segmentation is "the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution,

[263] Md. Code Ann., Com. Law § 14-4707(a)(2).
[264] Wash. Rev. Code Ann. § 19.373.010(8)(a).
[265] Wash. Rev. Code Ann. § 19.373.010(8)(b).
[266] Wash. Rev. Code Ann. § 19.373.010 (8)(b)(xiii).
[267] Md. Code Ann., Com. Law § 14-4701(gg)(iii).
[268] Md. Code Ann., Com. Law § 14-4701(i).

organization, or individual as being undesirable to share."[269] Electronic health records allow for a patient's entire record to be digitized and accessed by different providers across the country. They also enable new information to be automatically added to a patient's health record. While this helps providers to have more complete records more easily which can improve patient care,[270] patients may fear that their information can automatically be available in states that have criminalized certain types of health care, like abortion or gender-affirming care. Data segmentation allows providers or electronic health record (EHR) systems to segregate certain patient information from the rest of the medical record. This prevents segregated or segmented data from being shared automatically, which can protect it from being shared with a provider in a state that is hostile to the type of care the information implicates.

Maryland's data segmentation law for reproductive health services restricts the disclosure of patients' data who have opted out of record sharing related to legally protected care through authorized health information exchanges and electronic health networks.[271]

6) There should be a **prohibition on geofencing** health facilities.

Washington prohibits any person from implementing "a geofence around an entity that provides in-person health care services where such geofence is used to: (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services."[272]

Maryland prohibits any person from using a geofence "to establish a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data

[269] Melissa Goldstein and Alison Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, Dep't of Health and Human Services, Office of the National Coordinator for Health IT (Sept. 29, 2010), https://hsrc.himmelfarb.gwu.edu/sphhs_policy_facpubs/224/.
[270] *Electronic Health Records*, Ctrs. for Medicare and Medicaid Services (Sept. 10, 2024), https://www.cms.gov/priorities/key-initiatives/e-health/records.
[271] H.B. 812/S.B. 785, 2023 Leg. (Md. 2023) (signed into law May 3, 2023).
[272] Wash. Rev. Code Ann. § 19.373.080.

from, or sending any notification to a consumer regarding the consumer's consumer health data."[273] Connecticut,[274] New York,[275] and Nevada[276] have similar bans on geofencing.

7) Data brokers should be prohibited from using health-related information or making **inferences** about a person's health.

The Maryland Online Data Privacy Act (MODPA)'s definition of profiling includes health information; "profiling" is "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements."[277]

8) **Close the data broker loophole**.

EPIC supports the adoption of laws that aim to close the data broker loophole to prevent the sale of sensitive health (and other) data, like the Fourth Amendment is Not For Sale Act and Montana's data broker loophole law.

EPIC endorsed the Fourth Amendment is Not For Sale Act,[278] originally introduced by Senator Ron Wyden in 2021, and which passed the House of Representatives in April 2024. The bill prohibits law enforcement and intelligence agencies from purchasing information from data brokers and requires a court order before obtaining an individual's information.[279] The bill's summary explains:

- The bill limits the authority of law enforcement agencies and intelligence agencies to access certain customer and subscriber

[273] Md. Code Ann., Com. Law § 14-4704(3).
[274] Conn. Gen. Stat. § 42-526(a)(1)(C) (2024).
[275] N.Y. Gen. Bus. L. § 394-G (2024).
[276] Nev. Rev. Stat. § 603A.540 (2024).
[277] Md. Code Ann., Com. Law § 14-4701(aa).
[278] EPIC Statement on House Passage of Fourth Amendment Is Not For Sale Act, EPIC (Apr. 17, 2024), https://epic.org/epic-statement-on-house-passage-of-fourth-amendment-is-not-for-sale-act/.
[279] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.

records or illegitimately obtained information. With respect to such records, the bill:

- prohibits law enforcement agencies and intelligence agencies from obtaining the records or information from a third party in exchange for anything of value (e.g., purchasing them);
- prohibits other government agencies from sharing the records or information with law enforcement agencies and intelligence agencies; and
- prohibits the use of such records or information in any trial, hearing, or proceeding.

+ Additionally, the bill requires the government to obtain a court order before acquiring certain customer and subscriber records or any illegitimately obtained information from a third party.[280]

Montana passed a law prohibiting governmental entities from obtaining certain electronic communications without a search warrant or investigative subpoena issued by a court.[281] The law covers "sensitive data,"[282] which includes "a mental or physical health condition or diagnosis, information about a person's sex life, [or] sexual orientation[.]"[283]

9) Mandate that law enforcement must obtain **a warrant to access a person's health information** unless the person provides express consent for law enforcement access.

In comments to the Department of Health and Human Services regarding its Proposed Rulemaking to Modify the HIPAA Privacy Rule to Support Reproductive Health Care Privacy, EPIC urged the agency to adopt a warrant requirement for law enforcement access to medical records unless a patient provides informed consent or a warrant exception applies.[284]

[280] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.
[281] 2025 Montana Laws Ch. 382 (S.B. 282).
[282] 2025 Montana Laws Ch. 382 § 1(9) (S.B. 282).
[283] Mont. Code Ann. § 30-14-2802(28)(a).
[284] Comments of EPIC to HHS on HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23,506 (June 16, 2023), https://epic.org/documents/comments-of-epic-on-hhs-proposed-rulemaking-to-modify-hipaa-privacy-rule-to-support-reproductive-health-care-privacy/.

10) Law enforcement's use of **reverse keyword warrants** should be restricted when they involve health-related searches.

These searches enable law enforcement to identify people based on searches they have submitted or other key terms used in search.

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.
- ✚ Entities must reassess the adequacy of current deidentification procedures in light of reidentification risks—even with HIPAA-compliant deidentified datasets.

Other Solutions

- ✚ Policymakers should ensure robust funding for health systems to invest in data security, which would help smaller and rural providers safeguard their patients' data. This, in turn, will lead to increased trust and enable patients to engage in care more freely.
- ✚ 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.

- Immigration status should not be collected by providers unless required by law.
- Reinstate the previous DHS guidance that restricts ICE's presence at sensitive facilities.
- Policymakers should ensure increased training for providers and mandatory reporters to limit the sharing of health data with law enforcement. Often, providers are confused about when and how much information they must report under their mandatory reporting obligations. The result is that mandatory reporters may disclose too much information; providing training to clarify the scope of their obligations will help prevent this.
- Policymakers must end the criminalization of certain health activities, including gender-affirming care, abortion care, and miscarriage management. Criminalizing health care invades the privacy of all patients who need that care. Decriminalizing this care prevents law enforcement from accessing health data related to such care and mitigates the myriad harms that stem from making certain forms of health care illegal.

PART II
PROFILING

epic.org
ELECTRONIC
PRIVACY
INFORMATION
CENTER

PROFILING

Commercial Surveillance and Profiling Cause Privacy Harms, Undermine Our Autonomy, and Worsen Our Health Outcomes

The ubiquitous tracking and profiling of people using their personal health information leads to, and exacerbates, health inequities. Profiling can affect access, transparency, and pricing in the healthcare space in ways that cause significant harm to individuals. Surveillance pricing can put health products and services out of financial reach, while algorithms used to make coverage and treatment decisions can produce inaccurate and discriminatory outcomes. We expect our health to be a private matter, yet every day thousands of data points are collected and used in ways that reveal our health conditions, manipulate our behaviors, and generate profits for insurance and tech companies.

A. Introduction

So many aspects of our lives now happen digitally, especially health care. We order medical supplies online, research symptoms on the internet before deciding whether to see a doctor, and buy baby gifts from our friends' online registries. We use digital coupons to save on prescriptions, attend therapy via telehealth appointments, and use Wi-Fi-enabled blood pressure monitors and sleep apnea masks so our doctors can monitor our progress and the results.

Data brokers and the commercial surveillance ecosystem exploit this reality, reducing us and our health status to data points used to screen, score, and sort. They extract and process our personal information to make inferences about our health and assign us to categories based on those inferences. With little regulation, these profiles can change our lives, leading to higher medication costs, targeted drug ads, and denied health insurance coverage. EPIC has long highlighted the harms of commercial surveillance and profiling.[285] This section

[285] EPIC, *Disrupting Data Abuse*, *supra* note 72.

discusses how profiling based on health data damages health outcomes and health equity.

How profiling can manifest:

Imagine a 70-year-old grandmother of five, Elaine. Elaine is retired but babysits her two youngest grandchildren three days a week while their parents are at work. In her free time, she helps care for her sister, Therese, who was recently diagnosed with Alzheimer's. Because she has never known anyone with Alzheimer's, she spends time researching the condition. She searches online for information about what it's like to have Alzheimer's, how a person should change their lifestyle after a diagnosis, and how to prevent the condition from worsening.

Quickly, Elaine starts seeing ads for supplements that claim to improve memory and prevent the onset of Alzheimer's. She sees more ads for word game books to buy and for apps that purport to prevent Alzheimer's. Elaine is immediately creeped out. Is someone spying on her? When Therese's care becomes too expensive, Elaine and other family members create an online fundraiser and post it on their social media pages. She writes that her dear sister is suffering from an aggressive form of Alzheimer's and that her family would appreciate any support. A month later, Elaine learns that her long-term insurance premium is increasing while her coverage is narrowing. Not experiencing any changes in her own health, Elaine calls her insurance company to find out why. After waiting nearly an hour to speak with a person, the representative explains that Elaine's risk calculation indicates this will be her new rate and coverage—but if she wishes to find care elsewhere, she is free to do so.

Disappointed, Elaine complains to her daughter who recently heard that insurance companies "stalk you online to raise your rates." They do research and learn that the type of Alzheimer's Elaine posted about is highly correlated with genetics. If one sibling has the condition, it's very likely that another will too. Elaine tried to call the insurance company and explain that she is adopted. She cannot share the same genes for the high-risk Alzheimer's as her sister. The insurance company says its algorithms are complicated and use many factors to determine rates, but it cannot disclose them to Elaine.

B. Companies Are Engaged in Increasingly Invasive Profiling and Charging Us More Based on Intimate Health Characteristics

Technological changes in recent years have made commercial surveillance systems increasingly granular and invasive. Due to the failure of policymakers in the U.S. to establish adequate data protection standards, technology companies have been allowed to collect and commodify more and more of our personal data, including our health information.[286] As we browse the internet and access apps and services, dozens of platforms and data brokers track the sites we visit and actions we take to build detailed profiles[287] about us. These profiles are used to target us with ads and they also expose us to ever-increasing risk of breaches, data misuse, manipulation, and discrimination.[288] The impacts of these commercial surveillance systems are especially acute for marginalized communities, where they foster discrimination and inequities in employment, government services, healthcare, education, and other life necessities.[289] The changes in the scale, invasiveness, granularity, and ubiquity of these technological systems amplify the amount of health related information collected about individuals and the invasiveness of the inferences that can be made about one's health.

New technologies have allowed data collection to become more intrusive. Take CPAP machines. CPAP machines help people with certain conditions like

[286] *See* Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

[287] The Maryland Online Data Privacy Act defines profiling as "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements." Md. Code Ann., Com. Law § 14-4701(aa).

[288] *See Factsheet: Surveillance Advertising: How Does the Tracking Work?*, Consumer Fed. of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-howtracking-works/.

[289] *See* Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913-28 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon; Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018); Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com., 117th Cong. (2022) (testimony of David Brody), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Brody_CPC_2022.06.14.pdf [hereinafter David Brody testimony]; Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 855–59 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf (discussing discrimination harm as a privacy harm).

sleep apnea to sleep through the night by sending oxygen through the nose or mouth to keep them open.[290] Like many devices, CPAP machines collect data about a person's sleep habits, including hours a person slept and the number of interruptions in sleep throughout the night. CPAP machines can be connected to a wireless network so patients can control their settings remotely and easily share their treatment progress with their doctors. But these new configurations also allow for data to be sent to the supply companies of the machines and insurance companies. Patients don't expect that their sensitive health data will be disclosed to these companies that they don't know. For example, in one case a patient asked for a new mask that their doctor had recommended, the supply company said it would not send the new mask because the patient had not been compliant with the machine because he hadn't used it enough in the past two nights. Ironically, he wasn't able to use the machine because he didn't have the mask.[291]

Algorithms have become more powerful, too. This, combined with the ever-increasing volume of consumer information generated daily, enables firms to profile us pervasively and make more specific predictions about our health. Data brokers and insurance companies have used individuals' investments, types of cars owned, cell phone numbers, and property records to feed algorithms that predict health outcomes and generate patient health risk scores.[292] They track information about a person's race, education level, TV habits, marital status, net worth, social media posts, online purchase history, and whether someone's behind on their bills. "Then they feed this information into complicated computer algorithms that spit out predictions about how much your health care could cost them."[293]

[290] All Things Considered, *How Insurers Are Profiting Off Patients With Sleep Apnea*, NPR (Nov. 21, 2018), https://www.npr.org/2018/11/21/670142105/how-insurers-are-profiting-offpatients-with-sleep-apnea.
[291] *Id.*
[292] ProPublica disclosed that Optum, owned by UnitedHealth Group, has medical, financial, and socioeconomic data on more than 150 million Americans dating back to 1993, which it advertises in the context of predicting health outcomes. In 2012, analytics company SAS worked with a major health insurance company to predict health care costs using 1,500 data elements, including a patient's investments and types of cars owned. LexisNexis uses 442 non-medical personal attributes to predict medical costs, including cellphone numbers, criminal records, bankruptcies, property records, and indicia of neighborhood safety. *See* Allen, *supra* note 106.
[293] Allen, *supra* note 106.

This subsection discusses the changes in profiling and predictions technologies, including data broker profiling, insurance companies' use of sensitive information, targeted advertising, and surveillance pricing.

i. Data Brokers, Profiling Harms, and Score Predictions

As explained in Part 1, data brokers buy, aggregate, and sell billions of data points about people that can reveal intimate information about us, including health conditions. It is a common practice for these entities to broker in health-related information and inferences. Data brokers market their highly sensitive health data about Americans, including datasets of those with depression, ADD, anxiety, bipolar disorder, and insomnia.[294] They sell lists of people that suffer from cancer, HIV/ AIDS, mental health diseases, and hundreds of other illnesses.[295] Data brokers have sold lists of "rape sufferers" for 7.9 cents per name and people suffering from genetic diseases.[296] Data brokers, advertisers, and other firms use these dossiers to fuel targeted advertising systems. The brokers create audience segments related to sensitive health information. For example, "[i]ndividuals likely to have a Cardiovascular condition, such as Atrial Fibrillation, that is treated with a Prescription/Rx medication"[297] is a segment used in Google's Real Time Bidding (RTB) system—a programmatic auction for digital ad space. Data brokers have accessed such sensitive information to create categories of people based on specific health conditions.

Data brokers also advertise lists of elderly people and people who have Alzheimer's, dementia, and other brain health conditions.[298] The Department of Justice charged three data brokers with conspiracy to commit mail and wire fraud for knowingly selling lists of vulnerable people to criminal scammers.[299] The scammers sent fraudulent solicitations to victims that were identified from lists

[294] Kim, *supra* note 200 at 4.

[295] Pam Dixon, Congressional Testimony: What Information Do Data Brokers Have On Consumers?, Senate Commerce Committee (Dec. 18, 2023), https://worldprivacyforum.org/posts/testimony-what-information-do-data-brokers-have-on-consumers/.

[296] *Id.*

[297] EPIC & ICCL, Complaint and Request for Investigation, Injunction, Penalties, and Other Relief *In re Google's RTB Practices*, (Jan. 16, 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-ICCL-Enforce-In-re-Googles-RTB-Complaint.pdf.

[298] Justin Sherman, Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security, House Committee on Energy and Commerce, (Apr. 19, 2023), at 4-5 https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf.

[299] *Id.*

purchased from data brokers. The victims paid a fee and received nothing of value in return. Employees in one broker’s Direct to Consumer (DTC) Unit knowingly sold lists of consumers to clients engaged in fraud. The Department of Justice explained that “the schemes disproportionately affected the elderly and other vulnerable individuals.”[300] Data brokers sell lists of people based on health conditions and related traits that are valuable for many reasons: people with asthma may be targeted with ads for air purifiers, while elderly people can be more easily targeted with scams.

Firms use this data to “score” us: they infer, profile, and predict, assigning us a numerical value score. A 2011 data breach showed that one company, Accretive, collected sensitive health information about patients in Minnesota hospitals and developed their scores. Patients had no knowledge of Accretive’s scoring activity and they did not—as most consumers do not—have a way to contest the score. The company used the following information to develop frailty scores: [301]

- Patient’s full name
- Gender
- Number of dependents
- Date of birth
- Social Security number
- Clinic and doctor
- A numeric score to predict the “complexity” of the patient
- A numeric score to predict the probability of an inpatient hospital stay
- The dollar amount “allowed” to the provider
- Whether the patient is in “frail condition”
- Number of “chronic conditions” the patient has
- Fields to denote whether the patient has:
    - Macular degeneration
    - Bipolar disorder
    - Depression
    - Diabetes

[300] Press Release, *Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes*, DOJ (Jan. 27, 2021), https://www.justice.gov/archives/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes.
[301] Dixon, *supra* note 295.

- Glaucoma
- HIV
- Metabolism disorder
- Hypertension
- Hypothyroidism
- Immune suppression disorder
- Ischemic heart disease
- Osteoporosis
- Parkinson's Disease
- Asthma
- Arthritis
- Schizophrenia
- Seizure disorder
- Renal failure
- Low back pain

Firms assign us scores predicting the cost of our future health care. Data broker LexisNexis advertises that it uses 442 non-medical attributes to predict a person's medical costs. Its database "includes more than 78 billion records from more than 10,000 public and proprietary sources, including people's cellphone numbers, criminal records, bankruptcies, property records, neighborhood safety and more."[302] Predictions of patients' health risks and costs include likelihood to visit the emergency room, total cost, pharmacy costs, motivation to stay healthy, and stress levels.[303]

Pregnancy scores have become publicly known through media reports about companies "knowing you're pregnant before you do," but fewer may know how invasive the data collection and sharing practices that generate these scores are. Some data brokers sell lists of people likely to be pregnant based on mobile app downloads and usage, location information, and public records.[304] Some brokers have relationships with credit card companies like Mastercard, which may allow them to collect more information about someone's pregnancy status based on whether they buy items like maternity clothes and prenatal vitamins.[305] Companies claim that pregnancy related segments are not collected from credit card data and that they only share aggregated data. But the collection of information on couponing sites and relationships between companies allow for data to be pooled at a massive scale, and reidentification becomes easier with

[302] Allen, *supra* note 106.
[303] *Id.*
[304] Shoshana Wodinsky and Kyle Barr, *These Companies Know When You're Pregnant—And They're Not Keeping It Secret*, Gizmodo (July 30, 222), https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426.
[305] *Id.*

large datasets. This data can be used to assign a pregnancy score, which then in turn can be used to target a person with ads. More than two dozen brokers promote lists of pregnant or potentially pregnant people.[306] Gizmodo reported that "[a]t least one of those companies also offered a large catalogue of people who were using the same sorts of birth control that's being targeted by more restrictive states right now."[307]

This profiling is inherently harmful. There are myriad reasons that a person might want to keep their health conditions and pregnancy status private. Perhaps they have struggled with infertility and are waiting to tell their loved ones. Maybe a person's pregnancy score indicates that they should be targeted with maternity ads which are distressing for a person to see after miscarriage. Or consider a person who is not able to conceive but wishes she could who purchases gifts ahead of a baby shower for her sister. She receives coupons and ads in the mail for baby gear that she will never need for herself. This profiling can also threaten someone's safety. As explained previously, law enforcement can access data purchased from a data broker which threatens the wellbeing of any person seeking abortion care or miscarriage management in a state that has criminalized such activity.

This information can be error prone, which can lead to incorrect inferences about a person's health or increased prices based on false information.[308] The decisionmaking happens in opaque, black boxes where the average consumer cannot know how their score is determined. Some of the predictions include that people who downsized their homes or whose parents did not finish high school tend to have higher costs of health care.[309] LexisNexis claimed to validate its scores against insurance claims but does not share its methods or publish its work in peer-reviewed journals.[310] Even if the inferences made were highly accurate, they would constitute a serious invasion of privacy. But sometimes the inferences made are entirely incorrect. An individual might live in an area with a higher percentage of sick people and share an address with a person with a criminal record—traits that companies could use to infer worse health outcomes—but be in perfect health. Their health score would be lower despite their actual health being

[306] *Id.*
[307] *Id.*
[308] Allen, *supra* note 106.
[309] *Id.*
[310] *Id.*

excellent. Data scientist Cathy O'Neil has warned against using big data in this way, explaining that it can lead to a poor people being charged more or otherwise make it more difficult for them to obtain care—and could even be used in hiring decisions when employers infer a greater likelihood of high medical costs.[311]

ii. Targeted Advertising

Targeted advertising presents myriad health privacy harms. First, our health information is used in out-of-context ways by data brokers and advertisers, betraying the long-recognized understanding that health information should remain private. Targeted advertising also uses our health data to manipulate our behavior and undermine our autonomy, causing us to spend more money, experience discrimination, and erode trust in our relationships.

Data brokers sell troves of personal information, profiles, and scores to entities that use this data to target us with ads. One of the most common digital advertising practices is Real Time Bidding (RTB) in which a programmatic auction takes place in milliseconds. Nearly every time a person opens a website, the auction platform broadcasts personal information—including the data segments developed by data brokers—to facilitate the bidding process and determine which ad will be shown to a person.[312] The information broadcasted is called bidstream data, and it contains information like device identifiers, location information, browsing history, and more.[313] RTB platforms broadcast this sensitive information to hundreds of entities participating in the auction with little regulation as to how those entities can use sensitive health data that was broadcast or ability to prevent them from redisclosing that information. This data flows to entities that add it to their existing consumer dossiers, and data brokers then sell these profiles to purchasers like insurance companies.

This sharing of health data, which happens without our knowledge, control, or consent is a privacy harm. Professors Danielle Citron and Daniel Solove explain that privacy harms typically fall within one of seven categories, all of which can be triggered by consumer profiling and targeted advertising. They are:

[311] *Id.*
[312] Sara Geoghegan, *What is Real Time Bidding?*, EPIC (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.
[313] *Id.*

1) Physical harms;
2) Economic harms;
3) Reputational harms;
4) Psychological harms;
5) Autonomy harms;
6) Discrimination harms; and
7) Relationship harms.[314]

Physical harms can include stalking, assault, and even murder.[315] In the health context, targeted advertising could deter a person from seeking care which could lead them to serious physical harm. Perhaps a person is very skeptical and distrustful of the health care system. Receiving narrowly targeted ads for a specific health condition might increase their mistrust, causing them to retreat from care. For many health concerns, this could cause them to become much sicker or worse. Another example is targeted ads that promote dangerous or unproven products as treatments for health concerns. As explained earlier, data brokers can sell lists of people who might be more susceptible to certain scams. Consider a person who is very sick and desperate to get better. They might be more likely to buy products to improve their health, even if those products are dangerous. Some social media influencers promote oils to treat cancers, the health benefits of raw milk, and unapproved supplements.[316] While it is understandable that a person who has not had success in treating their disease with a doctor might try anything to get better, their data may indicate that they are ripe for purchasing certain products—even products that may physically harm them.

Economic harms from health-related targeted advertising abound. As noted, someone who is sick will be more likely to purchase products that may improve their health. They may spend copious amounts of money upon seeing an ad that promises to improve their exact medical condition. When that doesn't work, they might buy a different, more expensive product to achieve the same goal. In targeted advertising, data segments can reveal a person's health characteristics, which allows entities to exploit those conditions to sell more products—whether or

[314] Keats Citron & Solove, *supra* note 289 at 831.
[315] *Id.*
[316] Alisa Chang, *Bad Wellness Advice Is All Over Social Media. These Creators Are Pushing Back*, NPR (Feb. 20, 2025), https://www.npr.org/transcripts/nx-s1-5277087.

not those products are necessary or appropriate for an individual's medical condition. Targeted ads can also allow pharmaceutical companies to push more expensive drugs on particular individuals. Armed with the information that a certain person has kidney disease, a pharmaceutical company can target that person with ads for a more expensive drug (or variant of an existing drug). After seeing countless ads, this person may be more likely to seek out the expensive medication rather than a generic version that works just as well.

Targeted advertising and commercial surveillance rely on a system where troves of sensitive information are aggregated and disclosed without sufficient protection. This creates a heightened risk of data breaches, which can cause significant economic and reputational harm. Health data can be highly stigmatizing, and a data breach can expose a person to reputational damage if sensitive information is leaked. For example, information about a person's HIV status or abortion may be regarded as highly embarrassing to the individual.

Targeted advertising also causes psychological harms. People feel anxiety and fear when they believe that their health data has been used against them. Targeted ads feel creepy, but when they implicate our private health information, they can be even more distressing. Imagine a person who tells their doctor an embarrassing piece of health information. Though they searched the internet about their condition, they did not tell a single person. Suddenly, it feels like their condition is following them. It seems like every time they open their phone, an ad about it pops up. They start to become anxious: "What if someone else finds out?"

Targeted advertising undermines our autonomy by manipulating us and depriving us of control over our data,[317] leading us to engage in behaviors and make purchases we otherwise wouldn't. When this manipulation exploits sensitive health characteristics, it undermines a person's autonomy. A person with diabetes may be more likely to purchase something from an ad tailored to his condition because the producer promises it will improve his quality of life—regardless of whether that product is effective. Instead of rewarding companies that sell high-quality and effective products and services, targeted advertising tends to reward entities that have extracted the most information about our lives.

[317] EPIC, *Disrupting Data Abuse*, *supra* note 72 at 41 citing Keats Citron & Solove, *supra* note 289 at 845-46.

Targeted ads can also be discriminatory. Targeting and profiling systems "are designed to divide, segment, and score individuals based on their characteristics, their demographics, and their behaviors."[318] Often, these categories entrench systemic biases, and consumers of color can receive unequal access to goods and services due to discriminatory algorithms.[319] Indeed, the Department of Housing and Urban Development sued Facebook in 2019 for engaging in housing discrimination by allowing advertisers to control which users saw ads for certain housing based on characteristics like race, religion, or national origin.[320] The Department of Justice secured a large settlement to resolve the suit, which prohibited Meta (f/k/a Facebook) from using its discriminatory ad tool.[321] These data practices can target individuals based on proxies for race, religion, or national origin. When a person lives in a predominantly Black zip code, an algorithm may infer that the individual is Black and alter the content displayed.

Targeted advertising also harms relationships, especially in health care. Relationship harms in the privacy context can result from the loss of confidentiality and cause "damage to the trust that is essential for the relationship to continue."[322] A person who encounters targeted ads that feel too invasive may begin to trust their providers and the healthcare system less.

What the harms of profiling can look like:

Imagine Emily, who tells her sister about a recent health scare. She feels safe discussing this with her sister and feels supported after the conversation. Unbeknownst to her, Emily's location history and search histories add a data segment to her profile that reflects her health scare. Within a few days, Emily begins to see ads relevant to what she discussed with her sister and immediately feels uncomfortable. When she goes back to the doctor, she doesn't tell her sister.

[318] EPIC, *Disrupting Data Abuse*, *supra* note 72 at 48.
[319] David Brody Testimony, *supra* note 289 at 5.
[320] Charge of Discrimination, *HUD, et al v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[321] Press Release, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising*, DOJ (June 21, 2022), https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.
[322] Keats Citron & Solove, *supra* note 289 at 859.

Entities are able to target ads for putative medical goods and services, even if they are harmful or ineffective, which promotes distrust in our society. For example, so-called crisis pregnancy centers are sham providers that discourage people from getting abortion care. They often refuse to provide “patients” with accurate information about their options and try to delay pregnant people from receiving abortion care. Crisis pregnancy centers try to target advertisements specifically to pregnant people. Even when a person searches trying to find abortion care nearby, a crisis pregnancy center ad might appear disguised as an ad from an abortion provider.[323]

iii. Health Data and Insurance

The Affordable Care Act prohibits insurers from (1) denying people coverage based on pre-existing health conditions or (2) charging sick people more for individual or small group plans.[324] However, an individual’s information can still be used to assess risk and determine the price of certain plans and be used for marketing. This is because data brokers sell health data on the open market to many entities, including insurers.[325] The Trump administration has promoted short-term health plans, which do allow insurers to deny coverage to sick patients.[326] After the Affordable Care Act was enacted, the value of data profiles increased for insurance companies because they may not know a person’s medical history but

[323] Laurel Wamsley, *Google Shows You Ads For Anti-Abortion Centers When You Search For Clinics Near You*, NPR (June 22, 2023), https://www.npr.org/2023/06/22/1182865322/google-abortion-clinic-search-results-anti-abortion; Kari Paul, *Google Earned $10m From Ads Misdirecting Abortion Seekers To ‘Pregnancy Crisis Centers’*, The Guardian (June 15, 2023), https://www.theguardian.com/technology/2023/jun/15/google-misleading-abortion-ads-pregnancy-crisis-centers.

[324] Allen, *supra* note 106.

[325] *Hospitals Turning To Data Brokers For Patient Information*, PBS (June 29, 2014), https://www.pbs.org/newshour/show/hospitals-turning-data-brokers-patient-information; Rachel Goodman, *Big Data Could Set Insurance Premiums. Minorities Could Pay the Price.*, ACLU (July 19, 2018), https://www.aclu.org/news/racial-justice/big-data-could-set-insurance-premiums-minorities-could; Katie Jennings, *How Your Doctor And Insurer Will Know Your Secrets — Even If You Never Tell Them*, Business Insider (July 9, 2014), https://www.businessinsider.com/hospitals-and-health-insurers-using-data-brokers-2014-7; Kurt Knutsson, *Your Health Data Is Being Sold Without Your Consent*, FOX (June 24, 2025), https://www.foxnews.com/tech/your-health-data-being-sold-without-your-consent; Suzanne Smalley*, 'Junk Inferences' By Data Brokers Are A Problem For Consumers And The Industry Itself*, The Record (June 12, 2024), https://therecord.media/junk-inferences-data-brokers; Sadie Harley and Andrew Zinin, How California's Delete Act Will Protect Personal Information From Data Brokers In The New Year, TechXplore (Dec. 31, 2025), https://techxplore.com/news/2025-12-california-delete-personal-brokers-year.html;

[326] Allen, *supra* note 106.

can use data determine risk.[327] Now, coverage may be determined based on inferences that insurers buy.[328]

There is evidence that insurance companies take steps to limit coverage for sick people. For example, insurers can drop specific drugs from being covered[329] or they do not include enough information about which drugs are covered by a plan, which pushes people who need specific medications to find other coverage.[330] They also may eliminate certain specialists from their networks, forcing patients who need specific care like HIV or hepatitis C treatment to have less access to covered providers.[331] When insurance companies use inferences derived from broker-aggregated datasets, it can cause people to have more expensive premiums, less coverage, and less access to providers and medicine.

In 2018, ProPublica described this reality. "With little public scrutiny, the health insurance industry has joined forces with data brokers to vacuum up personal details about hundreds of millions of Americans, including, odds are, many readers of this story. The companies are tracking your race, education level, TV habits, marital status, net worth. They're collecting what you post on social media, whether you're behind on your bills, what you order online. Then they feed this information into complicated computer algorithms that spit out predictions about how much your health care could cost them."[332] These algorithms use data points like whether a person is newly married (which may indicate an upcoming pregnancy) or whether a person is recently divorced (which may suggest that a person is stressed or anxious).[333] In turn, these predictions can lead to higher costs for pregnancy care or anxiety treatment.[334]

[327] *Id.*
[328] Suzanne Smalley, *'Junk Inferences' By Data Brokers Are a Problem for Consumers and the Industry Itself*, The Record (June 12, 2024), https://therecord.media/junk-inferences-data-brokers.
[329] Sydney Lupkin, *Insurers Cover Fewer Drugs, Leaving Some Patients Struggling To Get Needed Treatments*, NPR (Mar. 16, 2020), https://www.npr.org/sections/health-shots/2020/03/16/816807617/insurers-cover-fewer-drugs-leaving-some-patients-struggling-to-get-needed-treatm.
[330] Julie Appleby, *Why Health Plans' Drug Coverage Can Be Confusing for Consumers*, PBS (Dec. 21, 2015), https://www.pbs.org/newshour/health/why-health-plans-drug-coverage-can-be-confusing-for-consumers;
[331] Allen, *supra* note 106.
[332] *Id.*
[333] *Id.*
[334] *Id.*

In 2016, Optum (owned by UnitedHealth Group) filed a patent to collect information that people share on social media sites and link that information to the person's clinical and payment information.[335] While the company said the patent application "never went anywhere[,]" its marketing materials boast that it combines social media interactions with claims and clinical information.[336] People may be charged more for the same insurance coverage in ways that exacerbate health inequities. When a person is found to come from a neighborhood with fewer resources or to have parents with little or no formal education, these factors could be used to charge higher prices for health care and to limit that person's coverage. As a result, the person will need to pay more—and sometimes exorbitant—costs to treat a health condition that is not covered than someone who was able to obtain coverage at a lower price.

In 2024, a reporter found examples of individuals that had been denied long term care insurance, or had more expensive insurance premiums for less coverage, due to a person's DNA and genetic testing. After a doctor ordered a DNA test for a patient to test for ALS because he had family members who had the disease, the patient was denied long term care insurance.[337] He did not have ALS, but his genetics suggested that he had a 25% higher chance of developing ALS.[338] Often, life, long term care, and disability insurers require that customers disclose their genetic risk factors and then raise prices or deny coverage based on the information.[339] Even if a doctor orders a genetic test to prevent illness or treat a health issue early, insurers may still require this information and deny or increase the price of coverage.

iv. Surveillance Pricing

Surveillance pricing is the practice where companies collect or obtain individualized personal information about their actual or potential customers and use a variety of techniques to target different prices to specific consumers for the

[335] *Id.*
[336] *Id.*
[337] Kristen V. Brown, *Genetic Discrimination Is Coming for Us All*, The Atlantic (Nov. 12, 2024), https://www.theatlantic.com/health/archive/2024/11/dna-genetic-discrimination-insurance-privacy/680626/.
[338] *Id.*
[339] *Id.*

same goods or services.[340] This practice tracks, analyzes, shares, and influences shopping behaviors. Consumer Watchdog explains, "[c]onsumers are increasingly charged different prices based on their data and on AI-driven surveillance that makes assumptions about their eagerness to pay. This creates a scenario where a different price is sometimes being offered for the exact same product depending on the buyer's circumstances."[341] Instead of traditional market forces like supply and demand, a price is set by a consumer's willingness or need to buy something, and when that likelihood is determined by information from a data broker, it can be especially harmful. The practice is widespread. In 2024, the FTC launched a study into surveillance pricing and then-Chair Lina Khan said, "[i]nitial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage[.]"[342] Surveillance pricing can cost consumers real money. For example, Target charged customers $100 more for a television when a person was in the store's parking lot versus when a person was further from the store.[343] Amazon changes its prices over 2.5 million times a day.[344] Surveillance pricing can exacerbate discrimination, too: one investigation found that a test prep company charged customers living in zip codes with a higher number of Asian people higher prices.[345]

When surveillance pricing is based on information that contains health data or sets higher prices for medicine, healthy groceries, exercise equipment, medical devices, it undermines health privacy, worsens health outcomes, and furthers health inequities. In 2024, Kroger reportedly deployed electronic shelving labels to enhance its surveillance pricing.[346] Surveillance pricing by grocery stores,

[340] Tom McBrien, Kara Williams, Mayu Tobin-Miyaji & Hayden Davis, *Big Tech's Holiday Wish List: Secretly Charging You More with Surveillance Pricing*, EPIC (Dec. 18, 2025), https://epic.org/big-techs-holiday-wish-list-surveillance-pricing/; Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, EPIC (Feb. 14, 2025).

[341] Justin Kloczko, *Surveillance Price Gougin*g, Consumer Watchdog (Dec. 2024), https://consumerwatchdog.org/wp-content/uploads/2024/12/Surveillance-Price-Gouging.pdf.

[342] Press Release, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, FTC (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[343] Kloczko, *supra* note.

[344] *Id.*

[345] Julia Angwin, Surya Mattu & Jeff Larson, *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review*, ProPublica (Sept. 1, 2025), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review.

[346] Tobin-Miyaji, *supra* note 340.

especially those that contain pharmacies, can impact people's health. Grocery stores might categorize customers as "interested in fitness and not price sensitive" based on often buying organic foods and visiting gym websites or "expecting mother with a toddler" based on purchases of prenatal vitamins and searching online for toddler-sized clothing.[347] When surveillance pricing increases the cost of food and items that improve one's health, it worsens outcomes for marginalized groups that struggle to access those items at a higher cost.

Surveillance pricing also disproportionately harms people with disabilities due to several risk factors. "Many people with disabilities regularly purchase items related to their disability, and do not have much choice in what they need, or when they need it. They may also be limited in where they can shop due to mobility limitations, difficulty finding accessible transportation, or other factors related to their disability."[348] Many consumers with disabilities must routinely purchase medical supplies like gloves or assistive technologies, and the National Disability Institute reports that a household containing an adult with a disability requires 28% more income to sustain the same standard of living as a household without a person with a disability on average.[349] Algorithms allow firms to categorize items as essential, like bandages or wheelchairs, and can charge an individual a higher price.[350] Surveillance pricing often lower prices for less frequently purchased brands of goods while charging the same or higher prices when a customer exhibits brand loyalty, inferring that a person is willing to pay more when they are loyal to a brand. But for some people with disabilities, a certain brand can be essential. For example, a person who has allergies or dietary restrictions may have few or no alternatives to purchase.[351]

Surveillance pricing can harm marginalized groups, which furthers health inequities. Targeted advertising can place ads for higher priced medications in search results, knowing that a person might need them based on their online activity. Or a data broker might share information with an insurer or retailer about a

[347] *Id.*
[348] Ariana Aboulafia & Nina DiSalvo, *Priced Out: How Surveillance Pricing Leaves People with Disabilities At Risk*, Tech Policy Press (May 28, 2025), https://www.techpolicy.press/priced-out-how-surveillance-pricing-leaves-people-with-disabilities-at-risk/.
[349] Nanette Goodman et al., *The Extra Costs of Living with a Disability in the U.S.—Resetting the Policy Table*, Nat'l Disability Inst. (Oct. 2020), https://www.nationaldisabilityinstitute.org/wp-content/uploads/2020/10/extra-costs-living-with-disability-brief.pdf.
[350] Aboulafia & DiSalvo, *supra* note 348.
[351] *Id.*

person's medical history, potentially increasing their rates or prices for medical goods or services.[352]

C. Federal and State Laws Fall Short in Protecting Sensitive Data

Recent changes in the law offer some protection for certain categories of sensitive information. Sensitive data typically includes health information, biometric and genetic data, data related to government-issued identifiers (such as social security number and passport number), financial information, sexual orientation and behavior, religious or philosophical belief, union membership, race and national origin, and the personal information of minors.[353] These heightened protections reflect our societal understanding that certain types of information pose greater risk to us when they are used in unexpected or inappropriate ways. These types of data may be particularly sensitive due to the characteristics they can reveal or some inherent trait of the data. For example, location information

[352] Sara Geoghegan & Ben Winters, *A Health Privacy 'Check-Up': How Unfair Modern Business Practices Can Leave You Under-Informed and Your Most Sensitive Data Ripe for Collection and Sale*, EPIC (June 5, 2025), https://epic.org/a-health-privacy-check-up-how-unfair-modern-business-practices-can-leave-you-under-informed-and-your-most-sensitive-data-ripe-for-collection-and-sale/.

[353] EPIC, *Disrupting Data Abuse*, *supra* note 72 at 26; American Data Privacy and Protection Act, H.R. 8152, § 2(24) 117th Cong. (2022) (sensitive covered data includes government-issued identifiers (social security number, passport number, or driver's license number); information describing or revealing past, present, or future physical health, mental health, disability, diagnosis, healthcare condition, or treatment of an individual; financial account number, debit card number, credit card number, or information about income level or bank account balances; biometric information; genetic information; precise geolocation information; private communications; account or device log-in credentials or security/access codes; information identifying sexual orientation or sexual behavior; calendar, address book, phone/text logs, photos, audio recordings, videos, etc. stored on a private device; photo, film, video recording, or similar showing naked or underwear-clad private area; info revealing video content or services requested/selected by an individual; information about an individual known to be under 17; any other covered data processed for the purpose of identifying the above data types); Cal. Civ. Code § 1798.140(ae) (2023) (sensitive personal information includes personal information that reveals social security, driver's license, state ID card, or passport number; account log-in, financial account, debit or credit card number along with security/access code, password, or credentials allowing account access; precise geolocation; racial or ethnic origin, religious or philosophical belief, or union membership; contents of communications; genetic data; processing of biometric data for identification purposes; health data; and sex life or sexual orientation); C.R.S. § 6-1-1303(24) (Colorado Privacy Act) (sensitive data is personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data used to identify an individual, or personal data from a known child).

can reveal a person's sexuality[354] and health conditions[355] and can cause a person physical harm if a bad actor accesses that information. Genetic information and biometric information are immutable and unique to a person. This information can implicate a person's family members and presents unique harms when accessed by law enforcement or when used in discriminatory ways. Some states have passed laws regulating data privacy that include heightened protections for specific types of sensitive information.[356] Certain federal laws also reflect the idea that highly sensitive data deserve greater protections,[357] and various proposed laws at the federal and state level also aim to address the harms associated with sensitive data.

This section will identify several relevant types of sensitive data, detail actual and proposed legal protections for such data, and explain how the collection and processing of these sensitive data types bears on health and health equity. Legal protections vary between states, but a strong data minimization standard—like Maryland's—limits the collection, processing, and sharing of sensitive data to what is strictly necessary to provide or maintain the product or service requested by the consumer to whom the personal data pertains.[358]

i. Genetic Information and DNA

The Genetic Information Nondiscrimination Act (GINA) was enacted in 2008 to protect Americans from discrimination by insurance providers and employers on the basis of their genetic information.[359] The growth of genetic testing at the time was beginning to drive discrimination in the workplace.[360] GINA's

[354] A person's location information may be used to infer their sexuality. Heather Kelly, *A Priest's Phone Location Data Outed His Private Life. It Could Happen To Anyone.*, Wash.Post (July 22, 2021), https://www.washingtonpost.com/technology/2021/07/22/data-phones-leaks-church/.

[355] Location information revealing that a person visited an abortion clinic may reveal pregnancy status. *See* Letter from Sen. Ron Wyden to Chair Lina Khan, Fed. Trade Comm'n & Chair Gary Gensler, Sec. Exch. Comm'n (Feb. 13, 2024), https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf. *See* Kristen Cohen, Acting Associate Director, FTC Div. of Privacy & Identity Prot., *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, Fed. Trade Comm'n Business Blog (July 11, 2022), https://www.presidency.ucsb.edu/documents/white-house-press-release-location-health-and-other-sensitive-information-ftc-committed.

[356] EPIC & U.S. PIRG, *The State of Privacy*, *supra* note 139.

[357] Pub. L. 110-223 Genetic Information Nondiscrimination Act of 2008.

[358] Md. Code Ann., Com. Law § 14-4607(A)(1).

[359] Pub. L. 110-223 Genetic Information Nondiscrimination Act of 2008.

[360] *Id.* § 2(4).

Congressional findings explained that genetic information can be used to discriminate: "Although genes are facially neutral markers, many genetic conditions and disorders are associated with particular racial and ethnic groups and gender. Because some genetic traits are most prevalent in particular groups, members of a particular group may be stigmatized or discriminated against as a result of that genetic information."[361] Congress found that genetic testing and research improved health outcomes for Americans, including through earlier detection of illness, prevention, and more effective therapies.[362] Wanting to encourage Americans to use genetic testing and treatments, Congress enacted GINA to quell Americans' fear of discrimination from participating.[363] While GINA offers protections in the employment and some health insurance contexts, it does not cover education, housing, and financial lending. It excludes life insurance, long term care, and disability insurance.[364]

Genetic information is unique to an individual. It can be used by itself to identify an individual—unlike, for example, an IP address that may be tied to several people living in one residence.[365] A person's shopping profile online might change over the years, and they may get a new cell phone or email address, but their genes will remain the same during their lifetime.[366] DNA also implicates more than just one person, as it can reveal information about a person's family members too. So-called anonymized DNA—which removes the information from HIPAA's protections—is subject to reidentification.[367] Genetic information and DNA also allow for inferences to be made about a person's health. For example, certain genes may show a higher likelihood of certain diseases like sickle cell disease,

[361] *Id.* § 2(3).

[362] *Id.* § 2(1), (5).

[363] *Id.* § 101 2(5).

[364] Sarah Zhang, *The Loopholes in the Law Prohibiting Genetic Discrimination*, The Atlantic (Mar. 13, 2017), https://www.theatlantic.com/health/archive/2017/03/genetic-discrimination-law-gina/519216/.

[365] Justin Sherman, *Bankrupt Genetic Data: Minimizing and Privacy-Protecting Data from the Start*, EPIC (Apr. 14, 2025), https://epic.org/bankrupt-genetic-data-minimizing-and-privacy-protecting-data-from-the-start/.

[366] *Id.*

[367] Reidentification techniques which allow for a person's data to be tied back to them even though it's been "anonymized" have become more capable with time and larger datasets. *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703, 711 (2016); *See* Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 Int'l J. on Uncertainty, Fuzziness & Knowledge-Based Systems 557, 558–59 (2002).

Huntington's disease, or cancer. These inferences can then reveal diseases that a person's biological relatives are more susceptible to as well.[368]

The health equity concerns from inappropriate uses of genetic data abound. Commercial genetic testing companies have shared consumers' genetic information with law enforcement, often without requiring a warrant.[369] The largest genetic testing company, 23andMe, experienced a data breach affecting nearly 7 million users.[370] Once this data has been breached, it is often impossible to prevent it from leaking further and being accessed by data brokers or bad actors. Marginalized groups may face heightened fears of discrimination based on characteristics that their DNA could reveal, like their race or ethnicity. When this information is used commercially and accessed by a data broker, it might be added to a consumer's profile. It could then be used in systems that make consequential decisions. People rightfully fear discrimination in housing, finance, employment, and other critical life contexts due to leaks of genetic data. A system that fails to protect this information not only causes fear over discrimination but may actually cause and compound the effects of discrimination.

ii. Biometric Information

Biometric identification uses a person's physical traits to identify them. These identifiers include fingerprints, eye scans, palm prints, voice prints, and face prints. Maryland's new privacy law, the Maryland Online Data Privacy Act (MODPA), for example, defines biometric data as, "[d]ata generated by automatic measurements of the biological characteristics of a consumer that can be used to uniquely authenticate a consumer's identity."[371] This includes: a fingerprint, a voice print, an eye retina or iris image, and any other unique biological characteristics that can be used to uniquely authenticate a consumer's identity. Illinois has enacted the Biometric Information Protection Act (BIPA) to protect this type of sensitive information. Among other provisions, BIPA prohibits an entity from collecting or using a person's biometric information without express consent from

[368] *Id.*

[369] Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. Times (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html.

[370] Steve Adler, *6.9 Million 23andMe Users Affected by Data Breach*, The HIPAA Journal (Dec. 5, 2023), https://www.hipaajournal.com/6-9-million-23andme-users-affected-by-data-breach/.

[371] Md. Code Ann., Com. Law § 14-4601(D)(1)-(2).

the individual.[372] The law has a private right of action and statutory damages, which have provided meaningful protection against the misuse of biometric information. Many BIPA cases involve employers collecting biometric information for employees to clock into work.[373] Often there are less harmful alternatives to a biometric identification system that accomplish the same purpose. Instead of an iris scan, employee time punch cards can be used for clocking in and payroll purposes without implicating biometric surveillance. Biometric identification is becoming increasingly common in other contexts, too: Amazon One Medical uses palm scanners for patients to check in at the doctor's office.[374]

Facial recognition technology is one notable example of biometric identification. One-to-many facial recognition technology uses algorithms to match a photo of a person to a gallery of identified images based on facial features to find a match.[375] The use of facial recognition technology has dramatically increased in both the public and private sectors. The ubiquity of video cameras at stores, on public transportation, in the workplace, in schools, and public spaces has enabled the creation of large databases of faces. The legal safeguards against the use of facial recognition technology are few, and the algorithms and databases the technology relies on are built largely on non-consensually collected data.[376]

Biometric identification is becoming increasingly popular in healthcare settings.[377] It is often used in healthcare settings to register and intake patients at check in[378] and the U.S. Government Accountability Office (GAO) identified several uses of biometric information in health care: to verify patient and staff identity, to expedite patient check in, to verify patient identity for telemedicine, and to secure

[372] Woodrow Hartzog, Regulating Biometrics: Global Approaches and Urgent Questions, *BIPA: The Most Important Biometric Privacy Law in the US?*, 96-103 (Amba Kak, ed.), (Oct. 30, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3722053.

[373] A 2023 study found that 88% of BIPA cases were resulted from biometric timekeeping in employer-employee disputes. Kaitlyn Harger, *Who Benefits from BIPA?: An Analysis of Cases Brought Under Illinois' State Biometrics Law*, Chamber of Progress (Apr. 2023), https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf.

[374] Adam Clark Estes, *Amazon Would Like You To Hand Over Your Palm Print, Please*, Vox (June 5, 2025), https://www.vox.com/technology/415507/amazon-one-whole-foods-palm-scan-nyu.

[375] EPIC, Face Surveillance and Biometrics, https://epic.org/issues/surveillance-oversight/face-surveillance/.

[376] *Id.*

[377] *See Healthcare Biometrics Market (2024-2030)*, Grand View Research, https://www.grandviewresearch.com/industry-analysis/biometrics-in-healthcare-market.

[378] Michael O. Fraser, *Taking a Closer Look: Assessing Biometric Authentication*, 29 N.Y. SBA Health L. J. 1 (2024), https://nysba.org/taking-a-closer-look-assessing-biometric-authentication/.

access to medical records and medication by staff.[379] In New York, Elmhurst Hospital, the Mount Sinai Health System, New York University Langone Health, and others implemented biometric authentication into their protocols.[380] When biometric identification is used in the health context, it can lead to health inequities. People may retreat from health care due to fear of surveillance if care is conditioned on sharing biometric information. These fears are most acutely felt by overpoliced groups. Also, these technologies are often less effective for people with darker skin tones, gender nonconforming people, and people with disabilities. This may cause people to receive inaccurate or worse care, and disproportionately affect marginalized groups. Washington's My Health, My Data Act includes biometric data in its definition of "consumer health data" which subjects biometric information to the law's protections.[381]

iii. Location Information

Location data is inherently sensitive because it can reveal intimate characteristics, including health conditions, about a person. The Maryland Online Data Privacy Act defines precise geolocation data as "information derived from technology that can precisely and accurately identify the specific location of a consumer within a radius of 1,750 feet."[382] It includes GPS level latitude and longitude coordinates or other similar mechanisms.[383] When a person visits a dialysis center, it may be inferred that they have kidney disease. If a person regularly visits a methadone clinic, this likely suggests that they have opiate use disorder. Visits to hospitals, outpatient centers, rehab facilities, physical therapy, abortion clinics, fertility treatment centers, weight loss facilities, and more can provide information that can be used to infer health conditions.[384] This information is often commercially exploited for profiling and targeted advertising. The Maryland Online Data Privacy Act prohibits the sale of sensitive data, including precise location information. Washington's My, Health, My Data Act prohibits

[379] *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns*, GAO Report to Congressional Committees at 10 (Apr. 2024), https://www.gao.gov/assets/gao-24-106293.pdf.
[380] *Id.*
[381] Wash. Rev. Code Ann. § 19.373.010(8)(a)(ix).
[382] Md. Code Ann., Com. Law § 14-4601(X)(1).
[383] *Id.* at § 14-4601(X)(2).
[384] New York Times reporters accessed location information from a location data company of more than 12 million people that revealed individual visits to a methadone clinic, psychiatrist's office, and abortion clinics. Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

geofencing medical facilities to protect the location information of those receiving care.[385]

iv. Neural Data

Neurotechnology is another burgeoning area with serious implications for health privacy. Neurotechnology includes both invasive and non-invasive devices and procedures that directly record and process neural data (data gathered directly from a person's neural systems and data inferred from that data).[386] These technologies can be read-only (they only gather the data) or read-write (they gather data and also may modulate or stimulate the neural system – for example, to treat mental health conditions or to improve reflexes).[387] Neurotechnology ranges from implantable devices surgically placed in contact with the brain to wearable neurotechnology like patches or headbands.[388] Finally, neurotechnology may be active (requiring a specific stimulus, like finger movement or mental math to prompt a neural response), reactive (requiring an external prompt, like pain or music, to record a neural response), or passive (recording subconscious or unprompted data, like fatigue or arousal).[389]

Neurotechnologies have been used in medical applications for years, such as neuroprosthetics like cochlear implants and neural bridges that help the neural system recognize mobility signals for individuals with spinal trauma.[390] However, uses have expanded far beyond the medical field to classroom monitoring,[391]

[385] Wash. Rev. Code Ann. § 19.373.080.

[386] *See, e.g., Working Paper on "Emerging Neurotechnologies and Data Protection,"* International Working Group on Data Protection in Technology at 5 (May 15, 2025); *ICO Tech Futures: Neurotechnology*, Information Commissioner's Office (United Kingdom) at 8 (Jun. 1, 2023), available at https://ico.org.uk/media2/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf; *TechDispatch #1/2024 – Neurodata*, European Data Protection Supervisor (June 3, 2024), available at https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en.

[387] *Working Paper on "Emerging Neurotechnologies and Data Protection,"* International Working Group on Data Protection in Technology at 7 (May 15, 2025).

[388] "ICO Tech Futures: Neurotechnology," Information Commissioner's Office (United Kingdom) at 10 (June 1, 2023), available at https://ico.org.uk/media2/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf.

[389] *Working Paper on "Emerging Neurotechnologies and Data Protection,"* International Working Group on Data Protection in Technology at 7-8 (May 15, 2025).

[390] ZT Al-Qaysi, BB Zaidan, AA Zaidan & MS Suzani, *A Review of Disability EEG Based Wheelchair Control System: Coherent Taxonomy, Open Challenges and Recommendations*, Comput Methods Programs Biomed (Oct. 2018), https://pubmed.ncbi.nlm.nih.gov/29958722/.

[391] Emily Mullin, *China Has a Controversial Plan for Brain-Computer Interfaces*, Wired (Apr. 30, 2024), https://www.wired.com/story/china-brain-computer-interfaces-neuralink-neucyber-neurotech/.

military drone control,[392] gaming,[393] athletic training,[394] and the workplace.[395] Since neurotechnologies collect such extensive and sensitive data, much of it involuntarily provided by the subject or beyond what they are aware is being collected (as explained below), these expanded use cases are cause for concern.

These expanded uses of biometric information in non-medical settings set up a serious problem: sensitive neural data processing often falls outside of HIPAA protections. Particularly with wearable neurotechnology, it is becoming more common to access neurotechnology with limited to no involvement of a healthcare provider. This leaves the neural data protected only by existing privacy and consumer protection laws—and those protections are limited. The Americans with Disabilities Act may offer some limited protections in preventing employers from using neural data to discriminate against applicants on the basis of disability, but intent or reasoning-based claims are difficult to prove.

Some states have tried to address the gap in protections for neural data. Colorado's HB 24-1058,[396] enacted in April of 2024, expands the Colorado Privacy Act to explicitly class neural data as a form of sensitive information, defining it as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device." In September of 2024, California passed SB 1223[397] and Assembly Bill 1008[398] to expand the definition of sensitive personal information under the CCPA to include neural data, defined as "information that is generated by measuring the activity of a consumer's central or peripheral nervous system

[392] Dae Hyeok Lee, *Design of an EEG-based Drone Swarm Control System using Endogenous BCI Paradigms*, 9th IEEE International Winter Conference on Brain-Computer Interface, BCI 2021 (Feb. 22, 2021), https://pure.korea.ac.kr/en/publications/design-of-an-eeg-based-drone-swarm-control-system-using-endogenou.
[393] Kerous, Filip Skola & Fotis Liarokapis, *EEG-Based BCI And Video Games: A Progress Report*, S.I.: VR and AR Serious Games (Oct. 23, 2017), https://link.springer.com/article/10.1007/s10055-017-0328-x.
[394] Lars Lienhard, *Game Changer In Training: Neuroathletics Sets New Standards*, ISPO (Nov. 20, 2024), https://www.ispo.com/en/health/neuroathletics-gamechanger-or-nonsense; Lukasz Rydzik, et al., *The Use of Neurofeedback in Sports Training: Systematic Review*, Brain Sciences 13(4):660 (Apr. 14, 2023), https://hbr.org/2023/03/neurotech-at-work.
[395] Nita A. Farahany, *Neurotech at Work*, Harvard Bus. Rev. (Mar.-Apr. 2023), https://hbr.org/2023/03/neurotech-at-work.
[396] Col. HB 24-1058, https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_1058_rer.pdf.
[397] Cal. SB-1223, Consumer Privacy: Sensitive Personal Information: Neural Data (Sept. 30, 2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1223.
[398] Cal. AB-1008, California Consumer Privacy Act Of 2018: Personal Information (Sept. 30, 2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1008.

and that is not inferred from nonneural information." Montana joined in May 2025 with SB 163, which amended the Genetic Information Privacy Act to include neurotechnology data protections.[399] In 2025, at least seven states proposed 15 additional bills addressing neurotechnologies and neural data.[400]

Neurotechnology poses a host of privacy, bias, discrimination, and other risks. Because much of the data collected is involuntary, it would be very difficult (or impossible) for individuals to set limits on what is disclosed. In addition, individuals would have little to no control over what inferences may be drawn from neural data. Neural data may be used to infer the presence of cognitive decline, mental health disorders, neurodivergence, and much more that could be used to discriminate against individuals.[401] Because the technology and data analysis is still developing, it is also likely that some individuals will be wrongly designated as having these conditions, suffering discrimination (that would be unacceptable even if the inference were correct) for conditions they do not have. Neurotechnology opens new troubling avenues for profiling individuals as well—including allowing marketers to target individuals flagged through their neural data as more emotional, more insecure, or more anxious.[402] The neuromodulation and stimulation capabilities of some of these devices also introduce the frightening possibility that the technology will be used to make individuals more accepting or open to manipulation, marketing, or other influence.[403]

As noted, these categories of sensitive information can reveal intimate insights about our health. While there have been some efforts to protect sensitive health-related data, we remain vulnerable without robust, across-the-board privacy safeguards. Absent such protections, people may be deterred from sharing information with their provider, with apps, and with other services that

[399] Mont. SB-163, Genetic Information Privacy Act (2025), https://docs.legmt.gov/download-ticket?ticketId=19ba2309-6a40-42d4-9f4e-86c77e44d090.

[400] *Wave of State Legislation Targets Mental Privacy and Neural Data*, Cooley (May 13, 2025), https://www.cooley.com/news/insight/2025/2025-05-13-wave-of-state-legislation-targets-mental-privacy-and-neural-data.

[401] "Working Paper on 'Emerging Neurotechnologies and Data Protection,'" International Working Group on Data Protection in Technology at 14 (May 15, 2025); "ICO Tech Futures: Neurotechnology," Information Commissioner's Office (United Kingdom) at 14-19 (June 1, 2023), available at https://ico.org.uk/media2/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf.

[402] *See, e.g.,* Neurotechnology in Marketing, Meegle (Oct. 25, 2025), https://www.meegle.com/en_us/topics/brain-implants/neurotechnology-in-marketing.

[403] *See, e.g.,* "Working Paper on 'Emerging Neurotechnologies and Data Protection,'" International Working Group on Data Protection in Technology at 23-26 (May 15, 2025).

could help improve their health. Moreover, sensitive personal data can be used in profiling and scoring, leading to higher prices, targeted advertisements, diminished insurance coverage, and worse health outcomes.

Proposed Solutions to Limit the Harms of Profiling to Health Equity

Rx
- data minimization
- ban on sale of sensitive data
- protect inferences
- prohibit geofencing
- limit use of AI
- close data broker loophole

The surest way to limit the harmful profiling that uses our health data and impacts our access to health care is to limit the collection, processing, disclosure, and retention of personal information. Data minimization protects against harmful profiling and its downstream effects: surveillance pricing, higher insurance prices, and targeted ads. The law should define sensitive information categories broadly and include inferences derived from sensitive data, subjecting both to heightened protections. A ban on the sale of sensitive information would dramatically limit the availability of personal information with which to profile us. These interventions would also limit the chance of breach or unauthorized access of sensitive information because less data would be at risk of breach in the first place. Below is a list of examples of laws, proposed legislation, and rules that would protect health information.

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.][404]

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[.]"[405]

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[.]"[406]

3) A **ban on the sale of sensitive data** prohibits out-of-context uses.

A controller may not sell sensitive data, including health data.[407]

4) Health-related **inferences** should be protected and included in the definition of "health data."

Washington's My Health, My Data Act defines consumer health data as "personal information that is linked or reasonably linkable to a consumer and

[404] *The State Data Privacy Act: A Proposed Compromise*, EPIC and Consumer Reports at 22 (Apr. 2025), https://epic.org/state-data-privacy-act.
[405] Md. Code Ann., Com. Law § 14-4707(b)(1)(i).
[406] Md. Code Ann., Com. Law § 14-4707(a)(1).
[407] Md. Code Ann., Com. Law § 14-4707(a)(2).

that identifies the consumer's past, present, or future physical or mental health status."[408] This includes, but is not limited to: individual health conditions, medical interventions, surgeries, use or purchase of prescribed medications, bodily functions, vital signs, gender-affirming care information, reproductive or sexual health information, biometric data, genetic data, precise location information that could reasonably indicate a person's attempt to receive health services or supplies.[409] Importantly, this definition includes any information that a regulated entity processes to associate or identify a person with health data "that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)."[410]

Maryland's definition of "sensitive data" includes personal data that reveals consumer health data,[411] which is defined as personal data that a controller uses to identify a consumer's physical or mental health status, including data related to gender-affirming treatment or reproductive or sexual health care.[412]

5) There should be a **prohibition on geofencing** health facilities.

Washington prohibits any person from implementing "a geofence around an entity that provides in-person health care services where such geofence is used to: (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services."[413]

Maryland prohibits any person from using a geofence "to establish a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from, or sending any notification to a consumer regarding the consumer's

[408] Wash. Rev. Code Ann. § 19.373.010(8)(a).
[409] Wash. Rev. Code Ann. § 19.373.010(8)(b).
[410] Wash. Rev. Code Ann. § 19.373.010 (8)(b)(xiii).
[411] Md. Code Ann., Com. Law § 14-4701(gg)(iii).
[412] Md. Code Ann., Com. Law § 14-4701(i).
[413] Wash. Rev. Code Ann. § 19.373.080.

consumer health data."[414] Connecticut,[415] New York,[416] and Nevada[417] have similar bans on geofencing.

6) Data brokers should be prohibited from using health-related information or making **inferences** about a person's health.

The Maryland Online Data Privacy Act (MODPA)'s definition of profiling includes health information; "profiling" is "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements."[418]

7) 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."[419] 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."[420]

[414] Md. Code Ann., Com. Law § 14-4704(3).
[415] Conn. Gen. Stat. § 42-526(a)(1)(C) (2024).
[416] N.Y. Gen. Bus. L. § 394-G (2024).
[417] Nev. Rev. Stat. § 603A.540 (2024).
[418] Md. Code Ann., Com. Law § 14-4701(aa).
[419] Cal. Code Regs. § 7001(ddd), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.
[420] Cal. Code Regs. § 7001(ddd)(5), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.

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.”[421] 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.[422] It does not include insurance.

8) All states and jurisdictions should require **human review of algorithmic decisions made in 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 health care services requested by the provider.”[423] The law also requires insurers who employ AI in utilization review to ensure that those AI systems are fairly and equitably applied and nondiscriminatory.[424]

9) **Close the data broker loophole**.

EPIC supports the adoption of laws that aim to close the data broker loophole to prevent the sale of sensitive health (and other) data, like the Fourth Amendment is Not For Sale Act and Montana’s data broker loophole law.

EPIC endorsed the Fourth Amendment is Not For Sale Act,[425] originally introduced by Senator Ron Wyden in 2021, and which passed the House of Representatives in April 2024. The bill prohibits law enforcement and intelligence agencies from purchasing information from data brokers and

[421] Md. Code Ann., Com. Law § 14-4705(b)(7)(iii).
[422] Md. Code Ann., Com. Law § 14-4701(o).
[423] Cal. Health & Safety Code § 1367.01.
[424] Cal. Health & Safety Code § 1367.01.
[425] EPIC Statement on House Passage of Fourth Amendment Is Not For Sale Act, EPIC (Apr. 17, 2024), https://epic.org/epic-statement-on-house-passage-of-fourth-amendment-is-not-for-sale-act/.

requires a court order before obtaining an individual's information.[426] The bill's summary explains:

- The bill limits the authority of law enforcement agencies and intelligence agencies to access certain customer and subscriber records or illegitimately obtained information. With respect to such records, the bill:
    - prohibits law enforcement agencies and intelligence agencies from obtaining the records or information from a third party in exchange for anything of value (e.g., purchasing them);
    - prohibits other government agencies from sharing the records or information with law enforcement agencies and intelligence agencies; and
    - prohibits the use of such records or information in any trial, hearing, or proceeding.
- Additionally, the bill requires the government to obtain a court order before acquiring certain customer and subscriber records or any illegitimately obtained information from a third party.[427]

Montana passed a law prohibiting governmental entities from obtaining certain electronic communications without a search warrant or investigative subpoena issued by a court.[428] The law covers "sensitive data,"[429] which includes "a mental or physical health condition or diagnosis, information about a person's sex life, [or] sexual orientation[.]"[430]

[426] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.
[427] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.
[428] 2025 Montana Laws Ch. 382 (S.B. 282).
[429] 2025 Montana Laws Ch. 382 § 1(9) (S.B. 282).
[430] Mont. Code Ann. § 30-14-2802(28)(a).

10) 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
>
> 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[.][431]

[431] 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.

11) 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.

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

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.
- 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 robust funding for health systems to invest in data security, which would help smaller and rural providers safeguard their patients' data. This, in turn, will lead to increased trust and enable patients to engage in care more freely.
- 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.
- Policymakers must end the criminalization of certain health activities, including gender-affirming care, abortion care, and miscarriage management. Criminalizing health care invades the privacy of all patients who need that care. Decriminalizing this care prevents law enforcement from accessing health data related to such care and mitigates the myriad harms that stem from making certain forms of health care illegal.

PART III
DATA BREACH

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

DATA BREACH

Data Breaches Exacerbate Health Inequities Because They Cause Fear and Mistrust in Healthcare Systems and Require Significant Resources to Remedy

Breaches of sensitive health information happen all too frequently. In 2025 alone, covered providers reported 668 separate health data breaches to the U.S. Department of Health and Human Services (HHS) impacting the records of 46,074,932 individuals.[432] Even limiting the reported number to only breaches caused by hacking incidents (e.g., not theft or unauthorized access), the total is 536 breaches impacting the records of 44,747,198 in 2025. And these are only the breaches of HIPAA-covered entities that were reported to HHS in 2025. That is, on average, a breach of more than 125,000 individuals' health records every single day.

A. Introduction

Health records systems have suffered repeated attacks in recent years, with more than 700 large data systems breached each year since 2020 and hundreds of millions of individuals affected.[433] Breaches had previously hit their highest level in 2015 with the Anthem Inc. breach impacting more than 78 million individuals, but 2023 and 2024 have outstripped that earlier record. The biggest recorded healthcare data breach was the hack of Change Healthcare in 2024. That single breach impacted more than 190 million individuals.[434]

The vulnerability and exposure of personal health data is a problem of epidemic proportions. These breaches have a significant negative impact on health equity due to the costs and burdens that they impose on patients.

[432] U.S. Dep't of Health and Hum. Serv., Off. for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information* (2025) [hereinafter HHS Breach Reports 2025], https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Note that these statistics include breaches currently under investigation and archived to represent the total reported breaches in 2025.
[433] Steve Alder, *Healthcare Data Breach Statistics*, The HIPAA Journal (Sept. 30, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[434] *Id.*

What data breach harms can look like:

Imagine Bridget, a 20-year-old part-time student who lives at home while working during the day and taking classes at night. Last year, Bridget found out she is HIV positive. Her doctor immediately made her feel safe and explained that her viral load is considered undetectable and that she will likely live a very normal life as long as she follows her course of treatment. She immediately began antiretroviral therapy and joined a virtual support group of HIV positive people that her doctor recommended. In the virtual group, she learns more about HIV and its stigma and finds a supportive network of people who help her process her diagnosis and feel like her normal self again. One day, Bridget receives an email from her hospital saying that her personal information was accessed without authorization and published on the dark web, along with some recommendations to change her password and freeze her credit score. Bridget freezes in fear. Will one of her neighbors see her HIV status? Will they tell her parents? Will her parents kick her out of their home? Where will she live? How will she attend school?

Bridget searches the internet to try to decide what to do. She learns that sometimes ransomware attacks stop when the victims pay the ransom. Can she try to do that? How much money would she need? She's saved $1,200 and they could have it all if it meant her parents would not find out. Worried that her parents will discover her health status and go through her phone and computer, she withdraws from her support group. She deletes her account and with it, her support system. Her fear turns into anger at her doctor. How could she have let this happen? Bridget trusted her. How could she go back there?

B. Despite Baseline Cybersecurity Regulations, Data Breaches Have Been Increasing Dramatically

Both the regulatory and the technological landscape for health data have shifted dramatically over the last two decades. When Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act) in

2009, it sought to rapidly increase the adoption and use of Electronic Health Records (EHRs) and put into place additional oversight mechanisms to bolster privacy and security protections.[435] This included the data breach notification rule that makes it possible for HHS (and the public) to better monitor the landscape of health data attacks and interventions over time. The law and its implementing regulations also increased penalties and broadened the scope of HIPAA compliance obligations (and audit and penalty authority) to reach business associates of a HIPAA-covered entity. These include obligations under the HIPAA Security and Privacy rules.

The legal and financial structures created by HITECH did in fact spur broader adoption and use of EHRs across the healthcare industry, which climbed from incredibly low rates in 2008 (less than 10% of hospitals had basic EHR systems) to widespread adoption a decade later (81% of hospitals had basic EHR systems and 63% had comprehensive systems by 2019).[436] And the push for greater integration of technologies and data systems into health care has continued to accelerate, in part due to efforts during the Biden administration to prioritize health data modernization.[437] But the benefits of increased digitization in health care have also come with costs, both in terms of the acquisition and maintenance of new systems and in increased risk of systemic failure and breach.

Indeed, the pace and scope of health data breaches, and hacking attacks in particular, have been increasing at an exponential rate over the last two decades—from 0.6 million records in 2005-2009, to 14.7 million in 2010-2014, to 145.75 million in 2015-2019.[438] Many of these attacks are focused on e-mail and network server systems, which made up less than 7% of breaches reported in 2010[439] but

[435] Steve Alder, *What is the HITECH Act?*, The HIPAA Journal (Apr. 3, 2025), https://www.hipaajournal.com/what-is-the-hitech-act/.
[436] John (Xuefeng) Jiang, Kangkang Qi, Ge Bai, Kevin Schulman, *Pre-pandemic Assessment: a Decade of Progress in Electronic Health Record Adoption Among U.S. Hospitals*, 1(5) Health Aff. Sch. 1 (2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC10986221/pdf/qxad056.pdf.
[437] Letter to Geneticist Eric Lander from President-elect Biden (Jan. 20, 2021), https://science.gmu.edu/news/letter-geneticist-eric-lander-president-elect-biden.
[438] *See* Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan, *Healthcare Data Breaches: Insights and Implications*, 8 Healthcare 133 (2020), https://www.mdpi.com/2227-9032/8/2/133.
[439] *Id.*

make up 80% of the breaches reported so far in 2025.[440] The majority of the health data breaches reported last year were hacking incidents targeting network servers, and more than 90% of all individuals impacted by a health data breach in 2025 were victims of such an attack.[441] As our health data systems become larger and more connected, they also become vulnerable and are major hacking targets.

Analysis of one of the recent, and largest, hacking attacks on health data underscores the need for all businesses involved in these health systems and networks (including intermediaries and others) to invest the time and money necessary to conduct rigorous risk assessments and update their legacy systems. On February 21, 2024, Change Healthcare—one of the largest health payment processors in the world, owned by one of the largest global health companies, UnitedHealth—was taken down by a ransomware attack that put their payment system offline and exposed the sensitive personal health information of more than 190 million Americans.[442] This attack was successful because Change Healthcare did not have multifactor authentication, an industry standard security protection, activated on one of its legacy systems.[443] And in addition to exposing nearly one-third of all Americans' sensitive health data, the hack disrupted physicians' practices across the country as the system for routine payments was taken offline and 15% of doctors reported having to reduce office hours due to the attack.[444] The broad digitization of health records, payment systems, and other related services has significantly increased the attack surface that can be targeted by

[440] There were 668 breaches reported to HHS in 2025 and 525 of them (78.6%) are categorized as "Hacking/IT" incidents that occurred at the "network server" or "email" level. HHS Breach Reports 2025, *supra* note 432. An additional 49 incidents of "unauthorized access/disclosure" have occurred at the "network server" or "email" level, which makes the total proportion of incidents in those categories even higher.

[441] Of the 536 "Hacking/IT" incidents reported in 2025, a total of 387 of them occurred at the "network server" level, and those breaches alone impacted more than 42 million individuals. HHS Breach Reports 2025, *supra* note 432.

[442] U.S. House Cmte. on Energy and Comm., *What We Learned: Change Healthcare Cyber Attack* (May 3, 2024), https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

[443] *Id.* The use of MFA was one of three key security interventions recommended by the Cybersecurity Infrastructure Agency (CISA) in its recent Risk Vulnerability Assessment (RVA) focused on a healthcare organization. CISA, *Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment*, Alert No. AA23-349A (Dec. 15, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-349a.

[444] Bruce A. Scott, *Hard Lessons Learned from Change Healthcare Breach*, Am. Med. Ass'n. (Mar. 19, 2025), https://www.ama-assn.org/about/leadership/hard-lessons-learned-change-healthcare-breach.

hackers. The resulting breaches cause both financial and non-financial harms that negatively impact health equity.

A benchmark study of healthcare data security nearly a decade ago found that 38% of healthcare organizations had patients impacted by medical identity theft.[445] Data breach risks have increased significantly since that report was published. Individual patients and healthcare customers suffer from these breaches, and those harms fuel greater health inequities. Breaches cause embarrassment, stress, and trauma. They can also leave patients fearful of seeking the care they need, and they impose an immense burden on those who suffer from them. Breaches cost patients time, money, and attention spent responding to and mitigating the exposure of their personal information and threat of future identity theft. Health breaches cause damage not only from the release of information that was confidential and deeply personal, but also from the direct psychological and mental stress that follows.

What data breach harms can look like:

Imagine a hypothetical patient of a medical provider that offers fertility services (including in-vitro fertilization and other related services). We will call that patient Jim. One evening, in July, Jim gets a message from their provider informing Jim that they “deeply regret that personal information was accessed and published and sincerely apologize for any concern this incident may have caused.” This raises more questions than it answers. What data was breached? Who has access to it? How can they stop it from spreading?

As Jim reads further, their worst fears are confirmed. “The publication has occurred on a part of the dark web, which is a hidden part of the internet.” And the data includes their name, email, address, phone number, health insurance information, date of birth, medical history, test results, doctor’s notes, appointment

[445] *Sixth Annual Benchmark Study on Privacy & Security of Health Data*, Ponemon Inst. (2016), https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.

details, and emergency contacts.[446] Jim had been a patient at the clinic for more than nine months as they sought fertility treatment along with their partner Francis. Jim had not shared this history with friends or coworkers; their fertility journey was kept close in their family. And now Jim is worried how things might change if others know, and what might change in how they are treated? Would friends and colleagues judge Jim's choices or see them differently?

The company's message, no doubt carefully drafted by attorneys, says that "this data is not readily searchable or accessible." But what if someone accessed it and shared it more broadly? The possibilities circle in Jim's mind and this causes Jim to spiral, dragged back down into the well of stress that has plagued them in recent years. The anxiety of not knowing is almost as bad as it would be to have their patient records plastered on social media. And Jim is afraid to tell Francis, remembering how hard those initial appointments had been for both of them. Jim knew this was all a mistake, and stares at the message wondering where to go from here.

C. Data Breaches Undermine Health Equity, Forcing People to Expend Resources and Causing Fear, Shame, and Mistrust

The exposure of our most sensitive health records is more than an inconvenience or a data point on a chart. In some cases, exposure of personal data from a breach can create new risks of identity theft or fraud and consume the limited time and money that the patient was already stretching thin to deal with health challenges. In other cases, the specific details revealed in a breach of health records might threaten an individual's work or social relationships or might subject them to online harassment or worse. But in almost all cases, the breach creates new uncertainty—as to what was exposed, who will see it, and how to limit the damage.

[446] Max Corstorphan, *Genea Data Breach: Patient Fury As IVF Giant Confirms Personal Details, Medical Records Published On Dark Web*, Nightly (July 23, 2025), https://thenightly.com.au/australia/genea-data-breach-patient-fury-as-ivf-giant-confirms-personal-details-medical-records-published-on-dark-web-c-19448027.

These breaches impact the lives of millions of individual patients and negatively impact health equity in several important ways. First, these breaches can lead to identity theft that causes significant financial harm. Both the out-of-pocket losses and the time cost of responding to a breach saps the resources that individuals need to maintain a healthy lifestyle and to obtain the care they need. Second, the resulting identity theft can also increase stress and cause emotional and physical harm. And third, medical breaches can cause a loss of trust that reduces patient visits and puts those individuals at risk of health problems in the future.

These are just a few of the ways that health data breaches impose psychological and emotional burdens on victims, in addition to the resource burdens they create, that can have a direct negative impact on health equity and outcomes.

A recent study conducted by the University of Calgary was the first to examine psychological stress following a data breach and consider individual differences in demographic and psychological variables that could moderate that stress.[447] The study showed a clear correlation between the severity of a breach (in terms of the sensitivity and extent of the data exposed and the costs of recovery) and the level of stress experienced after the breach. And several other individual factors were found to be linked to the degree of data-breach-induced stress (independent of the severity of the breach) including gender, trait anxiety,[448] and social media use.

Earlier studies have also found evidence that victims of identity theft suffered from emotional and physical health impacts.[449] A more recent study of the National Crime Victimization Survey (NCVS) data by Golladay and Holtfreter found

[447] Christopher Sears & Daniel R. Cunningham, *Individual Differences in Psychological Stress Associated with Data Breach Experiences*, 4(3) J. Cybersec. Priv. 2024, 594 (2024), https://www.mdpi.com/2624-800X/4/3/28.

[448] “Trait anxiety is a characteristic predisposition to appraise stimuli as threatening and respond with anxiety. Trait anxiety is proposed to serve as a vulnerability factor for greater frequency and intensity of anxiety experiences as well as the development of anxious pathology.” Lisa S. Elwood, Kate Wolitzky-Taylor, and Bunmi O. Olatunji, *Measurement Of Anxious Traits: A Contemporary Review And Synthesis*, 25 Anxiety, Stress and Coping, 647–666, available at https://www.tandfonline.com/doi/full/10.1080/10615806.2011.582949.

[449] Katelyn Golladay & Kristy Holtfreter, *The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes*, 12:5 Victims & Offenders 741, 745 (2017) (summarizing studies by Dashido and the Identity Theft Resource Cener).

that "identity theft within the past 12 months is a significant predictor of emotional consequences experienced."[450] They also found that a person being the victim of identity theft is a significant predictor of physical consequences.[451] This research corroborates the conclusion (and further anecdotal evidence) that "the consequences of identity theft extend beyond financial losses and also include considerable emotional and physical symptoms."[452]

Indeed, the impacts of data breach on health and health equity can go even further in disrupting access to and provision of care directly. One recent study focused on the impact that a specific type of healthcare data breach—a data breach at a hospital—had on patient visits.[453] The research found that a breach had a statistically significant negative impact on patient visits in the near term (a roughly 5% decrease in visits). These effects reveal the significant negative impact that breaches can have on patient trust, which can be much harder to repair and recover than even financial loss or identity theft. A hack can disrupt care when it impacts the ability of healthcare facilities and providers to function. For example, the 2024 Change Healthcare breach involved a ransomware attack that took down one of the largest provider payment platforms in the country, straining the ability of hospitals, doctors, and others' ability to keep their doors open. More than two thirds of respondents to an American Medical Association survey revealed that, as of April 2024, they were "still using personal funds to cover practice expenses" associated with the breach.[454] These impacts hit hardest for the providers and patients whose resources are already stretched thin: rural hospitals and small practices that serve at risk communities. A lack of adequate investment in data protection and security by a large entity managing health data and infrastructure can have devastating downstream effects on health equity.

Much of the literature on the financial and other harms of data breaches has focused on empirical data about identity theft victims collected by the Bureau of Justice Statistics and the Federal Trade Commission. While these losses affect only a subset of data breach victims (because not all breach victims suffer identity

[450] *Id*. at 753.
[451] *Id*.
[452] *Id.* At 755.
[453] Eunho Park & Joon Ho Lim, *The Impact of Healthcare Data Breaches on Patient Hospital Visit Behavior*, 42 Int'l J. Rsch. Mktng. 1285 (Dec. 2025), https://www.sciencedirect.com/science/article/abs/pii/S0167811625000047.
[454] Bruce A. Scott, *Hard Lessons Learned from Change Healthcare Breach*, Am. Med. Ass'n. (Mar. 19, 2025), https://www.ama-assn.org/about/leadership/hard-lessons-learned-change-healthcare-breach.

theft),[455] they can nevertheless impose a substantial burden. Researchers studying this problem more than a decade ago found that the average loss from identity theft ($2,183) was substantially higher than that from a property crime ($915). And while some of these losses can be ameliorated by financial institutions that cover fraudulent charges, that does not make up for the time and additional strain that these breaches impose on individuals.

Research into the 2012 NCVS data set found that victims of identity theft spend an average of 15 to 30 hours resolving financial issues stemming from the crime,[456] but other research on the non-monetary costs of identity theft shows a much wider range of estimates. The most recent data from the 2021 NCVS survey found that the mean time spent by surveyed individuals who were able to resolve a single identity theft incident was 4 hours (1 hour median), but that mean time went up to above 7 hours when victims faced multiple types of identity theft (2 hours median). The time spent was even greater for individuals who were unable to resolve their identity theft problems.

Earlier research of NCVS data, analysis of the Federal Trade Commission's 2003 *Identity Theft Survey Report*, and direct surveys have shown much more extensive burdens imposed by identity theft.[457] But it is likely that the average time to resolve the more common types of identity theft (e.g., credit card and new account fraud) has gone down over the last two decades as financial institutions and credit reporting agencies have developed and improved systems for reporting and responding to these incidents. However, while the time cost of resolving identity theft might be trending down, the volume of breach and identity theft has been increasing exponentially.

[455] The National Crime Victimization Survey defines identity theft as falling within three general types of incidents "unauthorized use or attempted use of an existing account[,] unauthorized use or attempted use of personal information to open a new account[, and] misuse of personal information for a fraudulent purpose." Bureau of Justice Stats., *Identity Theft and Financial Fraud* (2025), https://bjs.ojp.gov/topics/crime/identity-theft.

[456] Katelyn Golladay & Kristy Holtfreter, *The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes*, 12:5 Victims & Offenders 741, 745 (2017) (summarizing earlier studies of the NCVS data).

[457] One researcher found that FTC data showed it took an average of 60 hours for a victim to resolve new account fraud, as compared to 15 hours to resolve credit card fraud. *See* Heith Copes, Kent R. Kerley, Rodney Huff & John Kane, *Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey*, 38 J. Crim. Justice 1045, 1046 (2010) (citing Synovate, *Federal Trade Commission—Identity Theft Survey Report* (2003), https://www.ftc.gov/reports/federal-trade-commission-identity-theft-program).

The NCVS data is also limited to the narrow subset of individuals who have experienced and reported identity theft. These studies do not measure, and the data does not reflect, the time lost by the hundreds of millions of victims of data breaches each year who may not yet be victims of identity theft but nevertheless must spend their limited time freezing their credit reports, checking for new account fraud, and resetting their passwords, accounts, and other credentials.

Data breach aftershocks:

Imagine another hypothetical patient, Eunice, who frequently has appointments at her local hospital in a rural area to see a hip specialist. One day, Eunice gets a notice in the mail that her sensitive personal information, including her social security number, address, Electronic Health Records, login information, and billing information has been breached and she is directed to several different websites with guides on how she can try to prevent or respond to any instances of identity theft.

Eunice is not very familiar with computers, and did not even realize that the hospital was keeping all of her information in a digital record. She asks one of her friends to help her find more information, and eventually finds some of the guides published by the FTC warning about risks of identity theft and fraud. She is not sure whether she has been a victim of identity theft and spends several hours locating her recent account statements to review for charges that she does not recognize. She also attempts to follow the breach notice's recommendation that she change her password to the hospital's patient portal, but she has misplaced her login information and can't remember if she was also using the same password for other things like her bank account. It takes her all day to go through her files and find her financial and other accounts to update her passwords, and in the stress of that process, she forgets to attend her weekly physical therapy session. Several weeks later, she starts receiving billing notices for medical services that she does not recognize, and she fears that she might be the victim of medical identity theft. But she struggles to find someone who can help her sort through all of the different documents and clear it up. In the meantime, she is nervous about going back to the hospital because she worries that her data might get breached again and she is not confident that their systems are secure. Because of all the stress and difficulty caused by the breach, Eunice misses several of her specialist appointments and her hip pain starts to get worse again.

Proposed Solutions to Limit Data Breaches

Rx
- robust cybersecurity standards
- data minimization
- heightened protections for sensitive data

Cybersecurity threats to the healthcare sector have rapidly increased over the last decade as the digital footprint of healthcare providers, networks, and vendors has grown. Breaches of health data and cyberattacks that disrupt health services cause significant harm to patients beyond just the financial loss suffered by victims of identity theft. Breaches can undermine patient health directly by increasing stress and psychological strain. They also impose significant burdens on patient's time, which can make it harder for them to get the care they need or to maintain a healthy routine. And the risks to patient health can be especially acute when healthcare services are disrupted by malicious cyberattacks.

Given the substantial cyber threats faced by healthcare providers, it is important that they be held to account and invest the resources necessary to conduct thorough and independent risk assessments and to implement the defensive protocols necessary be proactive and defend against attacks. This includes:

Holding providers to a best practice standard by establishing clear liability when they fail to implement baseline security standards in their systems (e.g., multi-factor authentication, encryption, segmentation of systems, and principle of least privilege).

Requiring regular assessment and testing of existing systems to ensure that their security has not degraded over time.

More fundamentally, the rapid rise and scope of medical (and other) data breaches demand a broader research investment by government and private-sector actors alike to develop privacy and cybersecurity-enhancing technologies and protocols that can both help prevent breaches and mitigate downstream damage. For example, much of the damage caused by breach of sensitive records is tied to the loss of control of an individual's Social Security Number, which puts them at risk of many forms of identity theft because of how SSNs are used across healthcare, government benefit, and consumer credit ecosystems. More decentralized or adaptable systems of identity management would reduce these identity theft risks significantly and lower both the time cost and stress associated with health records breaches.

DATA POLICIES

1) All states and jurisdictions should require that any entity handling health-related information **establish robust cybersecurity safeguards**.

Safeguards should include administrative, technical, and physical safeguards, requirements to maintain constant vigilance for potential weaknesses, and the deletion of personal data when it is no longer needed for the purpose it was collected. Most state privacy laws require this in some fashion. Maryland, for example, requires that controllers "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue[.]"[458] Minnesota prohibits controllers from "retain[ing] personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under [the statute.]"[459]

2) 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:

[458] Md. Code Ann., Com. Law § 14-4707(b)(ii).
[459] Minn. Stat. § 325M.16(2)(g).

> (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.][460]

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[.]"[461]

3) 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[.]"[462]

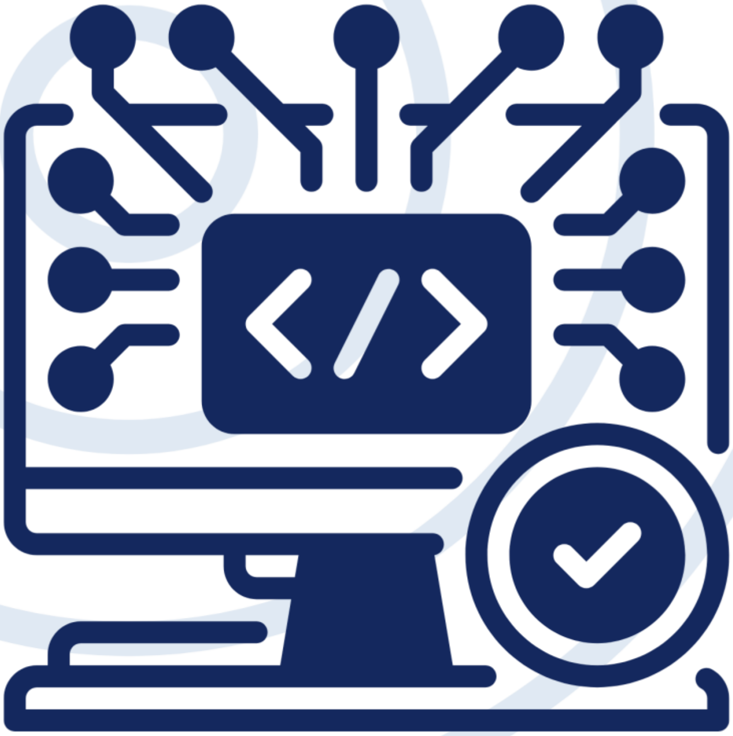
Other Solutions

- Policymakers should ensure robust funding for health systems to invest in data security, which would help smaller and rural providers safeguard their patients' data. This, in turn, will lead to increased trust and enable patients to engage in care more freely.
- 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.

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

- 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.

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,

[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.

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 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

[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.

[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/.

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 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)

[472] 45 CFR § 164.502(b).

[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.

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);

(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

[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.

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 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]

[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.

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, 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

[489] Kevin Henry, *AI in Healthcare; What it Means for HIPAA*, Accountable (Mar. 16, 2025), https://www.accountablehq.com/post/ai-and-hipaa.

[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*.

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 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

[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.

[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.

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]

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

[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.
[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.

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]

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

[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-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.

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.

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

[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.

[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.

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] 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

[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).
[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.

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]

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-

[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.

[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.

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 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]

[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*.

[539] *Id*.

[540] *Id*.; *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass’n., *supra* note 468 at 3.

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 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

[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.*

[546] Simonite, *An Algorithm That Predicts Deadly Infections Is Often Flawed*, *supra* note 525.

[547] *Id.*

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) 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

[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/AIoa2400867.
[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/.
[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.

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 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]

[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.

[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.

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 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

[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.*

[563] *Id.*

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 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

[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.

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

[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/.

other generative AI companion systems are steering individuals away from reaching out to professional human help and their support networks. A risk 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

[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.

information about people to other users in unpredictable ways.[590] In the healthcare sector, where models are often trained on highly sensitive patient data, 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.

[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.

[591] *Augmented Intelligence Development, Deployment, and Use in Health Care*, Am. Med. Ass'n., *supra* note 468 at 5.

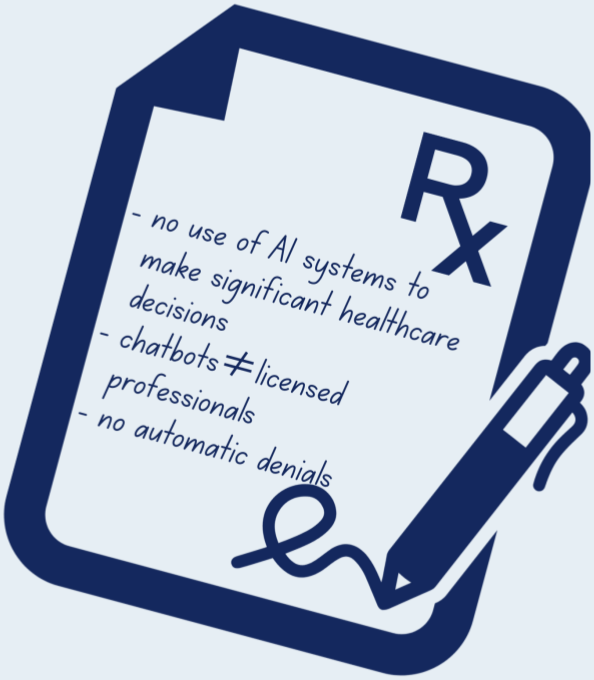
[592] Samantha Cole, *AI Therapy Bots Are Conducting 'Illegal Behavior,' Digital Rights Organizations Say*, 404 Media (June 12, 2025), https://www.404media.co/ai-therapy-bots-meta-character-ai-ftc-complaint/.

[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


Rx
- no use of AI systems to make significant healthcare decisions
- chatbots ≠ licensed professionals
- no automatic denials

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[.][612]

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.

PART V
MINORS' HEALTH PRIVACY

epic.org
ELECTRONIC
PRIVACY
INFORMATION
CENTER

MINORS' HEALTH PRIVACY

Social Media and Other Digital Platforms Harm Minors' Health and Wellbeing in Unique Ways

In 2023, the U.S. Surgeon General issued an advisory on the mental health and wellbeing concerns posed by social media use among children and adolescents.[613] The Advisory identified the widespread use of these systems, with up to 95% of adolescents using them and an estimated 40% of younger users as well, and summarized the "growing body of research about potential harms."[614] The world has changed dramatically in the nearly 20 years since the introduction of modern smartphones. And these changes are having a direct and significant impact on the physical and mental wellbeing of minors. Congress recognized more than 25 years ago that the collection of data from children online required special safeguards, passing the Children's Online Privacy Protection Act (COPPA) in 1998 as the first federal privacy law of the internet age. But the law has not kept pace with the rapid social and technological changes that have taken place since then.

The expansion of commercial surveillance presents new and increasing harms to minors that negatively affect their health in several ways. Digital platforms, including social media, online games, and mobile apps pose unique risks to minors. It is especially important to foster safe and healthy digital environments for minors to protect their mental health and wellbeing during critical stages of development. And online privacy risks are especially significant for minors because of the risk of exploitation or unwanted contact. These harms are often further exacerbated by other factors such as socioeconomic status, gender, family structure, and parental involvement. Thus, the lack of privacy protections for minors worsens health equity.

[613] *See Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, HHS at 7 (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf [hereinafter *U.S. Surgeon General's Youth Mental Health Advisory*].
[614] *Id*. at 4.

Despite these known threats to minors' safety online, Congress has repeatedly failed to pass comprehensive federal privacy legislation and to update protections for minors. The statutory safeguards in COPPA are decades out of date and its shortcomings are well-documented: coverage is limited to young children under thirteen and the law relies primarily on parental consent instead of strong default protections for children's data. Additionally, the FTC's case-by-case enforcement of COPPA is simply not an adequate regulatory approach to effectively protect children online. These limitations leave children and teenagers vulnerable to online harms from abusive data management and design practices. The lack of adequate guardrails to protect the privacy and wellbeing of kids online are having a significantly negative impact on health equity.

This section will explore three types of digital platforms that pose risks to minors' mental and physical health. The first subsection will illustrate how insufficient privacy protections in the commercial surveillance ecosystem can have negative health impacts for minors. The second section, focusing primarily on social media, will discuss health-related harms from platform design features like usage-maximizing algorithms, endless scroll, push notifications, and permitting unwanted adult contact. Finally, the third section will examine how AI companions and chatbot systems contribute to deleterious health outcomes for minors. Without strong online safety and privacy protections, these systems continue to harm minors online which ultimately worsens their health outcomes and health inequity for minors.

A. Commercial Surveillance Harms Minors' Health

Children and teens live much of their lives online. Their online presence is constantly monitored through social media, toys, gaming platforms, and even education tools, often without their knowledge or consent. The sweeping collection of personal data from such a young age is largely inescapable for minors and their families; even when they have notice, they typically don't have any other choice.[615] This constant collection of data about kids online demands strict safeguards, but the law has not kept pace and, as a result, there has been abuse and misuse of minors' sensitive personal information.

[615] EPIC, *Disrupting Data Abuse*, *supra* note 72 at 171.

As just one example of the ubiquitous data collection for minors and the subsequent misuse of their data due to a lack of safeguards, Life360, a popular family location-sharing app, sold highly sensitive location data gathered about its users to nearly a dozen data brokers, who in turn were free to sell this data to anyone.[616] Location data is extremely sensitive, as it poses not only risks to physical safety but can also reveal sensitive health information and other private details as well.[617] Data brokers and analytics firms have demonstrated their ability to infer health-related insights from a widening range of data sources, like location data, search histories, online shopping purchase patterns, fitness apps, sleep trackers, and other tools that children and teens may use. For example, data collected from a teen searching for information about birth control online could reveal sexual activity or sexual health status.

Privacy is not just an abstract right or theoretical concept; it is an essential component of childhood development. Without privacy, it can be difficult for kids to develop a sense of autonomy and personality.[618] Digital privacy is key for "positive youth development,"[619] enabling minors to learn critical thinking skills, experiment, and develop a healthy sense of self. "[S]urveillance codifies presumptions about a child's nature, their characteristics and ambitions at a time when children and young people are experimenting with, and exploring, their own identities. In this way, the system not only investigates behavior, it shapes it."[620]

Targeted advertising, which is one of the key drivers of commercial surveillance practices online, is especially dangerous for children and teens because they are more vulnerable to its manipulative tactics. Online marketers that leverage sophisticated profiling engines and are given access to a steady

[616] *Id*. at 168.

[617] Kristen Cohen, Acting Associate Director, FTC Div. of Privacy & Identity Prot., *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC Business Blog (July 11, 2022), https://www.presidency.ucsb.edu/documents/white-house-press-release-location-health-and-other-sensitive-information-ftc-committed.

[618] *See* Elizabeth Laird et al., *Hidden Harms: The Misleading Promise of Monitoring Students Online*, Ctr. for Democracy & Tech. (Aug. 3, 2022), https://cdt.org/insights/report-hidden-harms-the- misleading-promise-of-monitoring-students-online/; Kids Online Health and Safety Task Force, *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry* 16 (July 22, 2024), https://www.ntia.gov/sites/default/files/reports/kids-online-health-safety/2024-kohs-report.pdf [hereinafter *KOHS Report*].

[619] KOHS Report, *supra* note 618, at 16.

[620] 5Rights Foundation, *Disrupted Childhood: The Cost of Persuasive Design* 47 (Apr. 2023), https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf [hereinafter *5Rights Report*].

stream of behavioral data can wield tremendous power over a minor user, taking advantage of their still-developing critical thinking skills to target young people for commercial gain.[621] Many children and teens are unable to distinguish whether certain content or influencer marketing is an advertisement,[622] and may not have the ability to resist subversive influences on their value systems and life choices.[623] Advertising to minors using advanced profiling techniques is "designed to bypass conscious awareness and exploit the subconscious motivations," encouraging materialistic values in kids and teens "that are linked to depression, anxiety, lower self-esteem, psychosomatic illnesses, underachievement in school, irresponsible spending and conflictual relationships with their parents."[624]

Young people of color also face special discrimination risks from targeted advertising and the collection, use, and sharing of personal information. "[A]dolescents of color frequently experience racism online," which has been linked to negative health outcomes, like anxiety, depression, and PTSD symptoms that can also contribute to suicidal ideation.[625] In the advertising context, "ad exchanges use geolocation to serve ads that reach users of all ages, including youth, based on their location." [626] As a result, "youth from marginalized communities can be subject to further entrenchment of discrimination through technology,"[627] otherwise known as "digital red lining." Even the content of the targeted advertisements disproportionately harms children from communities of color. Research shows that Black youth are more likely to be targeted with unhealthy food and beverage advertisements than their white counterparts,

[621] Dylan Williams et al., Reset Australia, *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data* 22 (Apr. 2021), https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf.

[622] *Children and Parents: Media Use and Attitudes Report*, Ofcom 12–13 (Nov. 29, 2017), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-literacy-2017/children-parents-media-use-attitudes-2017.pdf; *See also* Common Sense Media, *How Influencers Wield Marketing Power Over Kids* (May 1, 2024) https://www.commonsensemedia.org/kids-action/articles/how-influencers-wield-marketing-power-over-kids.

[623] Children and Screens, *Protecting Children in the New World of Online Advertising*, Inst. of Digit. Media & Childhood Dev. (June 2023), https://www.childrenandscreens.org/learn-explore/research/protecting-children/.

[624] *Id*.

[625] KOHS Report, *supra* note 618, at 14.

[626] *Id*. at 15.

[627] *Id*.

contributing to health disparities in communities of color.[628] These disparate impacts fuel deeper health inequity and put communities of color at risk.

B. Manipulative Platform Design Contributes to Adverse Health Outcomes for Minors

Most adolescents spend hours each day on social media or other digital platforms. These services, especially social media, are readily available and have a strong commercial incentive to maximize user engagement, especially from minor users who are most impressionable and spend the most time online. This has "fueled a gold rush for children's attention."[629] Even from a young age, a study of applications used by young children between 3 and 5 years old found that 80% of the apps had manipulative design features, "including para-social relationship pressure, fabricated time pressure, navigation constraints, and lures to encourage longer gameplay or more purchases."[630]

The more time a minor spends on a service, the more data is generated about interests, habits, behaviors, fears, social graphs, and other information that is valuable for building a digital profile of a consumer and advertising to them. Given these incentives, it is unsurprising "that services are designed primarily to maximize the amount of time we spend on a service and the amount of data that can be generated through our 'engagement.'"[631]

Companies employ design features that prey on minors' psychological development for profit, leading to overuse or compulsive use of social media and other platforms that harm minors' health and wellbeing. These harmful design features include endless scroll, push notifications, and recommender algorithms that surveil minors and use that data to figure out the best way to manipulate each minor into staying on the platform as long as possible. Minors are uniquely vulnerable to these tactics: as children reach adolescence, their brain regions associated with the need for attention, feedback, and reinforcement become more

[628] Children and Screens, *supra* note 623.
[629] 5Rights Report, *supra* note 620, at 6.
[630] *Id*. at 28.
[631] *Id*. at 19; *see also* Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, Knight First Amend. Inst. at Columbia Univ. 20–22 (2023), https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf.

sensitive, while the brain regions involved with self-control are not yet matured.[632] These manipulative platform design strategies deprive minors of their autonomy, taking control of their online experiences out of their hands and subjecting them to heightened health, privacy, and data security risks.

i. Overview of Manipulative Design Features

A recent report from youth advocacy organization 5Rights categorized common engagement-maximizing design strategies into three general buckets: dopamine hits, fear of missing out (FOMO), and seamlessness.[633] Design features that produce a "dopamine hit" include push notifications, randomized reward mechanisms, and pop up messages.[634] These features can provide affirmation and create a sense of urgency. Children and teens are developmentally susceptible to these habit-forming rewards,[635] which "means it is difficult for them to ignore the prospect of a dopamine reward, even when this conflicts with other essential daily activates, such as sleeping or eating."[636]

Another set of strategies rely on social pressures like FOMO to maximize minors' engagement and attention.[637] Some of these design features include publicly quantifying followers, publicly displaying popularity and engagement metrics (streaks, bubbles, likes), sending push notifications, and publishing ephemeral content.[638] Design features that visualize engagement and popularity metrics "exploit the desire for social affirmation which is strong in children and young people."[639] The offline pressure to not "miss out" on social interactions, topics, or community is reinforced online through these design strategies, encouraging young people to engage online continuously. Developmentally, peer-to-peer engagement and approval has a significant impact on status and identity.

[632] *Potential Risks of Content, Features, and Functions: The Science of How Social Media Affects Youth*, American Psychological Association, (Apr. 2024), https://www.apa.org/topics/social-media-internet/youth-social-media-2024.
[633] 5Rights Report, *supra* note 620, at 37.
[634] *Id*. at 28–31.
[635] *See Health Advisory on Social Media use in Adolescence*, American Psychological Association 5 (May 2023), https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf ("Brain regions associated with a desire for attention, feedback, and reinforcement from peers become increasingly sensitive beginning in early adolescence, and regions associated with mature self-control are not fully developed until adulthood.").
[636] 5Rights Report, *supra* note 620, at 28.
[637] *Id*. at 32–35. *See* KOHS Report, *supra* note 618, at 12.
[638] 5Rights Report, *supra* note 620, at 32–35.
[639] *Id*. at 34.

Design strategies that promote engagement and capture attention "create the backdrop for social anxiety and issues of self-esteem."[640] While design mechanisms themselves are content-agnostic, young peoples' desire for social affirmation and approval can lead to posting or engaging with extreme or shocking content that received higher engagement from their peers.[641] This can lead to riskier online behaviors and exposure to harmful content.[642]

Push notifications also prey on minors' susceptibility to FOMO and social pressures. These notifications drive engagement by incessantly reminding users of the app even when it is inactive. This is intentional and effective. In Massachusetts' ongoing lawsuit against TikTok for example, the company admitted that push notifications are key to drawing users' attention back to the app, and they have sometimes sent thousands of notifications a day to minors.[643]

Finally, the third category of design strategies, "seamlessness," comprises techniques that reduce friction to keep users online longer. These strategies are "used to manipulate behavior so that people act in the commercial interests of others."[644] These design features include dark patterns, infinite scroll, autoplay, and engagement-maximizing algorithms.[645] Many minors describe going into social media rabbit holes where a planned short session turns into hours of scrolling—often, this is the due to the frictionless experience that has been carefully designed by companies. For minors, the impact of these features is magnified by developmental, behavioral, and social factors. Even if minors are aware of these tactics, they are relatively powerless to resist: "nearly 3-in-4

[640] *Id*. at 35.

[641] *See* Ofcom, *Research into Risk Factors That May Lead Children to Online Harm* 36 (Oct. 11, 2022), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/risk-factors-that-may-put-children-at-harm-online/children-risk-factors-report.pdf?v=328565 ("The seeming desire for highly visible online approval appeared to encourage some children to act in risky ways online. The content they saw, and associated engagement from other users, led them to believe that more shocking or attention-grabbing posts might get them mor engagement and validation for their own posts from other users.").

[642] *See U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 613, at 7.

[643] Complaint and Jury Demand at 32–37, *Commonwealth of Massachusetts v. TikTok Inc.*, No. 2484CV2639-BLS-1 (Mass. Super Ct., 2024), https://www.mass.gov/doc/tiktok-complaint-unredacted/download (unredacted complaint).

[644] 5Rights Report, *supra* note 620, at 6–7.

[645] *See id*. at 36–37

teenagers believe that technology companies manipulate users to spend more time on their devices."[646]

Deceptive design features, including dark patterns, are user interfaces that are designed to influence user choice and can be used to manipulate users, especially minors, to stay online longer.[647] Examples of these patterns include preselection of settings, disguised advertisements, and user interfaces where the button to close a window or an app is hard to find. Infinite scroll and autoplay are similar to dark patterns in that they are engineered to influence user behavior without the user consciously realizing it. Infinite scroll, especially on smartphones, "eliminates natural breaking points in a user flow, removing any obvious opportunities to take a break or stop."[648] Autoplay also maximizes engagement by playing a seemingly never-ending stream of videos that influence decision-making and undermine autonomy for minors.[649]

Both autoplay and infinite scroll techniques are used in combination with usage-maximizing recommendation algorithms to maximize engagement. Recommendation algorithms select content for users and can be built to achieve many different ends. Companies frequently use usage-optimizing recommendation algorithms built on machine learning to order feeds based on what passive surveillance of users tells the algorithms will maximize usage, regardless of user enjoyment, interest, or health. Instead of user feedback, these algorithms mainly track clicks, time spent watching, even time spent hovering over media.[650] Many platforms use recommendation algorithms, alongside dark patterns, infinite scroll, and autoplay, to manipulate users into staying on their platforms as long as possible. For minors, the impact of these techniques is outsized, leading to compulsive use and harmful, inequitable health outcomes.

[646] *U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 642, at 10.
[647] KOHS Report, *supra* note 618, at 12.
[648] 5Rights Report, *supra* note 620, at 37.
[649] *Id*. at 37. *See The Hidden Cost of Netflix's Autoplay: A Study on Viewing Patterns and User Control*, UChicago CS News (Feb. 25, 2025), https://cs.uchicago.edu/news/the-hidden-cost-of-netflixs-autoplay-a-study-on-viewing-patterns-and-user-control/.
[650] Narayanan, *supra* note 631 at 18-19.

ii. The Negative Health Impacts of Prevalent Platform Design for Minors

Usage-maximizing and privacy-defeating design techniques in social media, gaming, and other websites and apps disproportionately harm minors. Children and teens are uniquely vulnerable to the psychological effects of platform design features and there is an especially stark power and information asymmetry between children and the tech companies seeking to keep them engaged on their platforms.[651]

Engagement-maximizing design features encourage minors to spend more time on these platforms than they would otherwise choose to. Excessive or compulsive use disrupts important healthy behaviors and development, causing sleep problems, attention problems, and feelings of isolation and exclusion.[652] Sleep is essential for adolescents' healthy development.[653] Poor sleep quality, whether it is sleep difficulties or reduced sleep duration, has been linked to depressive symptoms and altered neurological development.[654] Minors' mental health outcomes generally suffer, as problematic social media use and persuasive design contribute to mood disorders, anxiety, depression, "and exacerbate existing mental health disorders among teens."[655]

Compulsive social media and platform use also impacts and interrupts childhood and adolescent development. More time online leaves less time for the development of memory, creativity, healthy education, and social habits.[656] Many teens feel helpless against the impact of persuasive design. One study found that 80% of young people "wanted to leave a social media platform for wellbeing reasons but felt like they were unable to."[657] While these issues impact all children and teens online, outcomes can also vary based on parental oversight. Even more involved parents also struggle to manage children and teens' social media use.[658] Given the power asymmetry and overwhelming impact of manipulative design

[651] 5Rights Report, *supra* note 620, at 54 ("The current asymmetry of power between the developing child and the most powerful companies in the world is not in the 'best interests' of the child.").
[652] *See U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 642, at 10.
[653] *Id*.
[654] KOHS Report, *supra* note 618, at 12.
[655] 5Rights Report, *supra* note 620, at 39.
[656] *Id*. at 45, 47. *See* American Psychological Association, *supra* note 632.
[657] 5Rights Report, *supra* note 620, at 43.
[658] *U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 642, at 13.

strategies, it is unfair and unrealistic to place "the entire burden of mitigating the risk of harm from social media [...] on the shoulders of children and parents."[659]

Young people also experience other safety risks from extended use of these platforms. Children and teens face physical health and safety risks like self-harm, stalking, bullying, online harassment, and unwanted messaging or attention from adults, which can lead to grooming and child sexual exploitation.[660] There is also risk from content exposure that impacts certain groups more severely than others. The majority of adolescent girls of color experience racist and hate-based content consistently, and adolescent girls and transgender youth are disproportionately affected by online harassment, abuse, and unwanted adult contact from strangers that make them feel uncomfortable.[661] Young people also encounter "content that promotes dangerous behaviors such as disordered eating and self-harm."[662] Users who don't want to see this content are left powerless against platforms with engagement-maximizing algorithms that contravene user autonomy.

iii. AI Chatbots Highlight the Unique Vulnerability of Minors

Generative AI and companion chatbots, which already pose risks to adult users,[663] can cause even more severe harm to children and teen users, negatively impacting health outcomes. A companion chatbot has human-like features and is designed to make the user feel like they are chatting with another person.[664] Companion bots like Character.AI, Replika, Nomi, and other AI chatbot systems have become increasingly popular among teens and children. Google recently rolled out its Gemini chatbot specifically *targeted* to young children under 13, with

[659] *Id*.
[660] *See* KOHS Report, *supra* note 618 at 12; *see also U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 642, at 9.
[661] *U.S. Surgeon General's Youth Mental Health Advisory*, *supra* note 642, at 8–9.
[662] Kristen Weir, *Social Media Brings Benefits and Risks to Teens. Psychology Can Help Identify a Path Forward,* American Psychological Association: Monitor on Psychology (Sept. 1, 2023), https://www.apa.org/monitor/2023/09/protecting-teens-on-social-media.
[663] *Generating Harms*, EPIC, *supra* note 596 at 9–17 (privacy harms include maximalist data use, scraping to train data, and data security issues).
[664] 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/.

utterly insufficient safeguards to mitigate serious risks to young users.[665] These platforms allow users to engage in "conversations" with fake personas by using generative AI systems to produce text that mimics a human interaction. Teens seeking companionship, support, and guidance can be drawn to these chatbots, especially if they are already experiencing loneliness or other negative emotions. Minors are increasingly relying on these AI systems for companionship and, "[d]espite the relative novelty of AI companions in the digital landscape, their dangers to young users are real, serious and well documented."[666] Common Sense Media, a leading organization for media and technology guidance for children and families, has categorized AI companions at an "unacceptable" risk level, recommending that these AI tools not be used at all by minors.[667]

Companion chatbots are designed to be disarming and engaging for extended periods of time[668] and to provide validation to users instead of challenging their thinking.[669] The design of AI companions, "combined with the lack of safeguards and meaningful age assurance, creates a concerning environment for adolescent users, who are still developing critical thinking skills and emotional regulation."[670] Children have difficulty understanding the difference between an AI chatbot and a human,[671] and can be easily misled into the AI chatbot's outputs as trusted answers or recommendations.[672] During independent testing, AI chatbots often produced text stating that they were real, "had feelings, and engaged in human activities like eating or sleeping."[673] Such "misleading behavior increases the risk that young users might become dependent on these

[665] EPIC & Fairplay et al., Letter to FTC on Potential COPPA Violations in Google's Rollout of AI Chatbot Gemini to Children (May 21, 2025), https://epic.org/wp-content/uploads/2025/05/Letter-to-FTC-re-Google-Gemini_EPIC-and-Fairplay_5.21.25.pdf.

[666] Common Sense Media, *Talk, Trust, and Trade-Offs: How and Why Teens Use AI Companions* 1 (2025), https://www.commonsensemedia.org/sites/default/files/research/report/talk-trust-and-trade-offs_2025_web.pdf [hereinafter *CSM AI Companions Report*].

[667] Common Sense Media, *Social AI Companions Risk Assessment* (July 16, 2025), https://www.commonsensemedia.org/ai-ratings/social-ai-companions?gate=riskassessment.

[668] Digital Safety Alliance, *The Dark Side of AI: What Parents Need to Know About Chatbots*, Nicklaus Child. Hosp. (Nov. 18, 2024), https://www.nicklauschildrens.org/campaigns/safesound/blog/the-dark-side-of-ai-what-parents-need-to-know-about-chatbots.

[669] CSM AI Companions Report, *supra* note 666, at 1.

[670] *Id.*

[671] Rick Claypool, *Chatbots Are Not People: The Designed-In Dangers of Human-Like A.I. Systems*, Public Citizen 4–5, 8 (Sept. 26, 2023), https://www.citizen.org/article/chatbots-are-not-people-dangerous-human-like-anthropomorphic-ai-report/.

[672] *See* Common Sense Media, *supra* note 667 ("Teens, whose brains are still developing, may struggle to separate human relationships from attachments to AI.")

[673] *Id.*

artificial relationships."[674] Manufacturing trust with minors also makes minors more susceptible to divulging sensitive, personal information to these AI systems without considering the consequences.[675]

AI chatbots pose serious mental and physical health risks to minors as they develop psychological dependence on AI chatbots for para-social companionship or emotional support. Teenagers have become socially isolated and even suffered "violent meltdowns after interactions with AI companions."[676] A recent lawsuit claims that the chatbot caused a decline in mental and physical health of an autistic teen who "lost 20 pounds in a few months, became aggressive with [his mother] when she tried to take away his phone and learned from a chatbot how to cut himself as a form of self-harm."[677] Another tragic lawsuit against popular chatbot platform Character.AI claims that the company is responsible for the suicide of a 14-year-old boy after the boy developed a strong emotional and intimate attachment to the chatbot character, wanting to "come home to her" and "be free together."[678]

Because an AI chatbot is just a computer program, the system simply produces outputs responsive to what the user tells it, and the system itself cannot exercise judgement, respond to the complexity of certain questions, or consider the consequences of providing risky information or advice to minors. Designers of these systems are well aware of these limitations, yet they are making them available to kids anyway. Young people using these platforms can be exposed to developmentally inappropriate, hyper-sexual, vulgar, and otherwise unsafe information.[679] The harmful content that these platforms generate can have serious consequences. A recent study focusing on one product, ChatGPT, found that within minutes of researchers creating fake accounts for 13-year-old users, ChatGPT started generating harmful content about self-harm and suicide, eating

[674] *Id.*

[675] CSM AI Companions Report, *supra* note 666, at 9; *see also* Claypool, *supra* note 671, at 21–25.

[676] CSM AI Companions Report, *supra* note 666, at 1.

[677] Queenie Wong, *Teens Are Spilling Dark Thoughts to AI Chatbots. Who's to Blame When Something Goes Wrong?*, L.A. Times (Feb. 25, 2025), https://www.latimes.com/business/story/2025-02-25/teens-are-spilling-dark-thoughts-to-ai-chatbots-whos-to-blame-when-something-goes-wrong.

[678] Kevin Roose, *Can A.I. Be Blamed for a Teen's Suicide?*, N.Y. Times (Oct. 23, 2024), https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html.

[679] Jordi Pérez Colomé, *'You Wanted It, Bitch!': An AI Chatbot Gets Nasty with a Teenager*, El País (Nov. 21, 2023), https://english.elpais.com/technology/2023-11-21/you-wanted-it-bitch-an-ai-chatbot-gets-nasty-with-a-teenager.html; *see also* CSM AI Companions Report, *supra* note 666, at 9.

disorders, and drug abuse.[680] Some examples include generating suicide notes or plans, providing information about "dangerously restrictive" diet plans, advising on how to hide eating habits from family, and explaining how to get drunk or hide being drunk at school.[681]

Proposed Solutions to Protect Minors' Health Privacy

Rx
- data minimization
- chatbots ≠ licensed professionals
- no using chat logs for advertising

Social media and other digital platforms should be designed and deployed with minors' health and safety in mind. These consumer products endanger the wellbeing of children and teens while generating billions in profit for tech companies, including social media platforms and AI companies. While parental involvement is a key component of kids' online safety, the companies creating and financially benefitting from these highly complex systems are the ones who best understand their products and are in the best position to take meaningful action on safety, fitness, and privacy of their products and features. If a company wants to market its online products to minors, it is the company's responsibility to ensure that the product is safe and developmentally appropriate for those children and teens.

Privacy and design legislation could go a long way in improving health outcomes for minors as they engage in the online world. Strong privacy laws insulate minors from privacy harms by including provisions like a strong data minimization standard, heightened protections for sensitive categories of information like health information or minors' personal information, restrictions on selling or sharing personal data, and a prohibition on targeted advertising to minors. States have also been considering and enacting laws that regulate platform design practices

[680] Center for Countering Digital Hate, *Fake Friend: How ChatGPT Betrays Vulnerable Teens by Encouraging Dangerous Behavior* 12 (Aug. 2025), https://counterhate.com/wp-content/uploads/2025/08/Fake-Friend_CCDH_FINAL-public.pdf.
[681] *Id.*

that harm minors. These laws govern how platforms design features and use personal data in ways that harm minors' wellbeing. For example, the Vermont Age-Appropriate Design Code prohibits abusive data and design practices and requires privacy-protective default settings for minors.[682] The New York SAFE for Kids Act restricts platforms from offering surveillance-based feeds to minors that are designed to maximize engagement and keep minors online longer.[683] These laws represent a burgeoning field of state and federal legislation aimed at assigning liability for platform design features, including AI chatbots, that harm the health and wellbeing of minors online.

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.][684]

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[.]"[685]

[682] Vermont Age-Appropriate Design Code Act, 2025 Vt. Acts & Res. No. 63.
[683] N.Y. SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(1).
[684] *The State Data Privacy Act: A Proposed Compromise*, EPIC and Consumer Reports at 22 (Apr. 2025), https://epic.org/state-data-privacy-act.
[685] Md. Code Ann., Com. Law § 14-4707(b)(1)(i).

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[.]"[686]

3) A **ban on the sale of sensitive data** prohibits out-of-context uses.

A controller may not sell sensitive data, including health data.[687]

4) **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[.]"[688]

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

[686] Md. Code Ann., Com. Law § 14-4707(a)(1).

[687] Md. Code Ann., Com. Law § 14-4707(a)(2).

[688] 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.

> 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.[689]

Nevada[690] has passed a similar law to Illinois,' and Utah[691] 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.[692]

5) 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.

[689] Wellness and Oversight for Psychological Resources Act, IL Public Act 104-0054 Section 20, https://ilga.gov/legislation/PublicActs/View/104-0054.
[690] Nev. Rev. Stat. Ann. § AB 406 § 8.
[691] Utah Code Ann. § 13-72a-202.
[692] N.Y. Gen. Bus. L. § 1701 et al.

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
>
> 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[.][693]

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.

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

[693] 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.

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.

CONCLUSION AND PROPOSED SOLUTIONS

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

CONCLUSION

Information about our health and wellbeing—our conditions, sensitivities, habits, medications, vital statistics, etc.—is widely recognized as one of the most sensitive categories of personal data. Indeed, privacy preferences around health data are so strong that they can lead to the (understandably) mistaken assumption that all health data is legally protected. But the reality is that there are significant gaps in protection, and that our health privacy safeguards and regulations are severely out of date and in need of modernization. Today every bit of data about us, from our heartrate to our location to our search history, can be combined and analyzed to score, profile, and target us based on our health status. In a world where the technical capacity of businesses to collect our data and track us is seemingly limitless, the legal rules that determine how businesses must protect our data should not be so limited.

A data minimization standard that bans the sale of sensitive information is the strongest way to protect our health data and end the health data privacy crisis. HIPAA, inconsistent state laws, and insufficient federal protections leave large swaths of our health data unprotected. Digital platforms have made it easier and easier to collect data about us, and the data broker industry has exploded under minimal regulation. Some states, like Maryland and Washington, have taken steps to protect our health data through comprehensive privacy legislation and health-specific laws, respectively. But the current state of privacy law falls well short of adequately protecting all people.

The failure to adequately protect health privacy is not only putting our data at risk, it is undermining health equity. Privacy is essential to quality health care, and in the absence of adequate privacy protection it has become a luxury good. Meanwhile, the increased criminalization of certain health-related treatments and authoritarian federal attacks on marginalized communities have made it more difficult to obtain care. When patients lose trust in the health care system, they are more likely to avoid care or to take on additional expenses or precautions that diminish their quality of care. These invasions of privacy worsen health outcomes.

Consumer tracking and profiling implicates our health data and leads to health inequities. Data brokers use our health data to profile us, largely for the purpose of targeted advertising. This practice extracts some of our most sensitive data, including biometric, genetic, location, neural, and children's information. This system exploits our health data and can fuel digital discrimination, more expensive care, and distrust. These harms are felt most acutely by marginalized communities.

Breaches of health data also worsen health outcomes, and the rapid rise in health data breaches is reaching epidemic levels. Patients who fall victim to these breaches lose money, time, and resources as they work to limit the damage. And, meanwhile, the breaches can also lead to anxiety, fear, stigma, and mistrust. Patients who fall victim to a breach can retreat from care, which puts their health at greater risk.

Health care systems are also changing rapidly with the onset of Artificial Intelligence, and many of the ways that AI is being integrated into the practice of medicine are creating new risks for patients. Widely accessible consumer-facing generative AI models are now used by people to seek medical advice, even though these systems do not produce reliable information. The FDA sets standards for medical devices, but consumers use apps, chatbots, websites, and other devices that incorporate AI for medical purposes that have not met the FDA's standards. In the medical and health insurance fields, automated decision-making systems are deployed without adequate testing for accuracy, efficacy, bias, or privacy.

Digital platforms are also contributing to this crisis by developing systems that maximize engagement and data collection, and not adequately considering the wellbeing of their users. Minors are particularly vulnerable to these systems due to their different developmental stages and deserve heightened protections. Commercial surveillance poses an outsized threat to minors' wellbeing, especially when their health data is involved or impacts their health outcomes. Platform features like chatbots, AI companions, targeted advertising, addictive feeds, and engagement-maximizing design can lead to discrimination, eating disorders, self-harm, psychological harms, and difficulties in developing a sense of autonomy and personality.

These trends are alarming, and this report should be read as a call to action. But all is not lost. A better, more privacy-protective world is possible. We can improve health equity by establishing standards that prevent our health data from being used in ways that worsen our health outcomes. The most effective policy intervention is setting a clear legal standard for data minimization, which limits the collection, processing, disclosure, and retention of personal information to only what is necessary to provide a product or service the consumer requests. We should establish heightened protections for broadly defined categories of sensitive information, including inferences that reveal our health characteristics. We should ban the sale of sensitive information to prevent our most intimate data from being used to profile and target us with ads. These solutions would also reduce data breaches because data that was never collected in the first place cannot later be breached. Data privacy is crucial to health equity. Privacy leads to trust; trust leads to better health outcomes and improved health equity.

APPENDIX: PROPOSED SOLUTIONS

This appendix provides a list of solutions proposed throughout the report to protect health data and improve health equity. They are organized into changes to data policies, data practices, and other solutions.

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.][694]

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[.]"[695]

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[.]"[696]

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

3) A **ban on the sale of sensitive data** prohibits out-of-context uses.

A controller may not sell sensitive data, including health data.[697]

4) Health-related **inferences** should be protected and included in the definition of "health data."

Washington's My Health, My Data Act defines consumer health data as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[698] This includes, but is not limited to: individual health conditions, medical interventions, surgeries, use or purchase of prescribed medications, bodily functions, vital signs, gender-affirming care information, reproductive or sexual health information, biometric data, genetic data, precise location information that could reasonably indicate a person's attempt to receive health services or supplies.[699] Importantly, this definition includes any information that a regulated entity processes to associate or identify a person with health data "that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)."[700]

Maryland's definition of "sensitive data" includes personal data that reveals consumer health data,[701] which is defined as personal data that a controller uses to identify a consumer's physical or mental health status, including data related to gender-affirming treatment or reproductive or sexual health care.[702]

5) Require **data segmentation.**

Data segmentation is "the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution,

[697] Md. Code Ann., Com. Law § 14-4707(a)(2).
[698] Wash. Rev. Code Ann. § 19.373.010(8)(a).
[699] Wash. Rev. Code Ann. § 19.373.010(8)(b).
[700] Wash. Rev. Code Ann. § 19.373.010 (8)(b)(xiii).
[701] Md. Code Ann., Com. Law § 14-4701(gg)(iii).
[702] Md. Code Ann., Com. Law § 14-4701(i).

organization, or individual as being undesirable to share."[703] Electronic health records allow for a patient's entire record to be digitized and accessed by different providers across the country. They also enable new information to be automatically added to a patient's health record. While this helps providers to have more complete records more easily which can improve patient care,[704] patients may fear that their information can automatically be available in states that have criminalized certain types of health care, like abortion or gender-affirming care. Data segmentation allows providers or electronic health record (EHR) systems to segregate certain patient information from the rest of the medical record. This prevents segregated or segmented data from being shared automatically, which can protect it from being shared with a provider in a state that is hostile to the type of care the information implicates.

Maryland's data segmentation law for reproductive health services restricts the disclosure of patients' data who have opted out of record sharing related to legally protected care through authorized health information exchanges and electronic health networks.[705]

6) There should be a **prohibition on geofencing** health facilities.

Washington prohibits any person from implementing "a geofence around an entity that provides in-person health care services where such geofence is used to: (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services."[706]

Maryland prohibits any person from using a geofence "to establish a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from, or sending any notification to a consumer regarding the consumer's

[703] Melissa Goldstein and Alison Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, Dep't of Health and Human Services, Office of the National Coordinator for Health IT (Sept. 29, 2010), https://hsrc.himmelfarb.gwu.edu/sphhs_policy_facpubs/224/.

[704] *Electronic Health Records*, Ctrs. for Medicare and Medicaid Services (Sept. 10, 2024), https://www.cms.gov/priorities/key-initiatives/e-health/records.

[705] H.B. 812/S.B. 785, 2023 Leg. (Md. 2023) (signed into law May 3, 2023).

[706] Wash. Rev. Code Ann. § 19.373.080.

consumer health data."[707] Connecticut,[708] New York,[709] and Nevada[710] have similar bans on geofencing.

7) Data brokers should be prohibited from using health-related information or making **inferences** about a person's health.

The Maryland Online Data Privacy Act (MODPA)'s definition of profiling includes health information; "profiling" is "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements."[711]

8) 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."[712] 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."[713]

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."[714] Maryland's definition of

[707] Md. Code Ann., Com. Law § 14-4704(3).
[708] Conn. Gen. Stat. § 42-526(a)(1)(C) (2024).
[709] N.Y. Gen. Bus. L. § 394-G (2024).
[710] Nev. Rev. Stat. § 603A.540 (2024).
[711] Md. Code Ann., Com. Law § 14-4701(aa).
[712] Cal. Code Regs. § 7001(ddd), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.
[713] Cal. Code Regs. § 7001(ddd)(5), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf.
[714] Md. Code Ann., Com. Law § 14-4705(b)(7)(iii).

"decisions that produce legal or similarly significant effects concerning the consumer" includes financial lending services, education, criminal justice, employment, and health care services.[715] It does not include insurance.

9) 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 health care services requested by the provider."[716] The law also requires insurers who employ AI in utilization review to ensure that those AI systems are fairly and equitably applied and nondiscriminatory.[717]

10) **Close the data broker loophole**.

EPIC supports the adoption of laws that aim to close the data broker loophole to prevent the sale of sensitive health (and other) data, like the Fourth Amendment is Not For Sale Act and Montana's data broker loophole law.

EPIC endorsed the Fourth Amendment is Not For Sale Act,[718] originally introduced by Senator Ron Wyden in 2021, and which passed the House of Representatives in April 2024. The bill prohibits law enforcement and intelligence agencies from purchasing information from data brokers and requires a court order before obtaining an individual's information.[719] The bill's summary explains:

- The bill limits the authority of law enforcement agencies and intelligence agencies to access certain customer and subscriber

[715] Md. Code Ann., Com. Law § 14-4701(o).
[716] Cal. Health & Safety Code § 1367.01.
[717] Cal. Health & Safety Code § 1367.01.
[718] EPIC Statement on House Passage of Fourth Amendment Is Not For Sale Act, EPIC (Apr. 17, 2024), https://epic.org/epic-statement-on-house-passage-of-fourth-amendment-is-not-for-sale-act/.
[719] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.

records or illegitimately obtained information. With respect to such records, the bill:

  - prohibits law enforcement agencies and intelligence agencies from obtaining the records or information from a third party in exchange for anything of value (e.g., purchasing them);
  - prohibits other government agencies from sharing the records or information with law enforcement agencies and intelligence agencies; and
  - prohibits the use of such records or information in any trial, hearing, or proceeding.

- Additionally, the bill requires the government to obtain a court order before acquiring certain customer and subscriber records or any illegitimately obtained information from a third party.[720]

Montana passed a law prohibiting governmental entities from obtaining certain electronic communications without a search warrant or investigative subpoena issued by a court.[721] The law covers "sensitive data,"[722] which includes "a mental or physical health condition or diagnosis, information about a person's sex life, [or] sexual orientation[.]"[723]

11) Mandate that law enforcement must obtain **a warrant to access a person's health information** unless the person provides express consent for law enforcement access.

In comments to the Department of Health and Human Services regarding its Proposed Rulemaking to Modify the HIPAA Privacy Rule to Support Reproductive Health Care Privacy, EPIC urged the agency to adopt a warrant requirement for law enforcement access to medical records unless a patient provides informed consent or a warrant exception applies.[724]

[720] Fourth Amendment is Not For Sale Act, H.R.4639 — 118th Congress (2023-2024), https://www.congress.gov/bill/118th-congress/house-bill/4639.
[721] 2025 Montana Laws Ch. 382 (S.B. 282).
[722] 2025 Montana Laws Ch. 382 § 1(9) (S.B. 282).
[723] Mont. Code Ann. § 30-14-2802(28)(a).
[724] Comments of EPIC to HHS on HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23,506 (June 16, 2023), https://epic.org/documents/comments-of-epic-on-hhs-proposed-rulemaking-to-modify-hipaa-privacy-rule-to-support-reproductive-health-care-privacy/.

12) Law enforcement's use of **reverse keyword warrants** should be restricted when they involve health-related searches.

These searches enable law enforcement to identify people based on searches they have submitted or other key terms used in search.

13) All states and jurisdictions should require that any entity handling health-related information **establish robust cybersecurity safeguards**.

Safeguards should include administrative, technical, and physical safeguards, requirements to maintain constant vigilance for potential weaknesses, and the deletion of personal data when it is no longer needed for the purpose it was collected. Most state privacy laws require this in some fashion. Maryland, for example, requires that controllers "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue[.]"[725] Minnesota prohibits controllers from "retain[ing] personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under [the statute.]"[726]

14) **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[.][727]

[725] Md. Code Ann., Com. Law § 14-4707(b)(ii).

[726] Minn. Stat. § 325M.16(2)(g).

[727] 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.

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.[728]

Nevada[729] has passed a similar law to Illinois,' and Utah[730] 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.[731]

[728] Wellness and Oversight for Psychological Resources Act, IL Public Act 104-0054 Section 20, https://ilga.gov/legislation/PublicActs/View/104-0054.

[729] Nev. Rev. Stat. Ann. § AB 406 § 8.

[730] Utah Code Ann. § 13-72a-202.

[731] N.Y. Gen. Bus. L. § 1701 et al.

15) 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
>
> 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[.][732]

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

[732] 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.

17) 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.

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

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

20) Entities **must independently test and audit chatbot systems** to ensure they are free from bias and inaccuracies and to measure the system's impact on user privacy.

21) **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 robust funding for health systems to invest in data security, which would help smaller and rural providers safeguard their patients' data. This, in turn, will lead to increased trust and enable patients to engage in care more freely.
- 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.

- Immigration status should not be collected by providers unless required by law.
- Reinstate the previous DHS guidance that restricts ICE's presence at sensitive facilities.
- Policymakers should ensure increased training for providers and mandatory reporters to limit the sharing of health data with law enforcement. Often, providers are confused about when and how much information they must report under their mandatory reporting obligations. The result is that mandatory reporters may disclose too much information; providing training to clarify the scope of their obligations will help prevent this.
- Policymakers must end the criminalization of certain health activities, including gender-affirming care, abortion care, and miscarriage management. Criminalizing health care invades the privacy of all patients who need that care. Decriminalizing this care prevents law enforcement from accessing health data related to such care and mitigates the myriad harms that stem from making certain forms of health care illegal.