

ARE YOUR SECRETS SAFE?: IMPOSING A FIDUCIARY DUTY ON HEALTHCARE AI DEVELOPERS DEALING WITH SENSITIVE HEALTH INFORMATION

Lauren Quinn*

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to establish standards for transmitting health information. For decades, the HIPAA Privacy Rule has operated as the primary regulation protecting health information in the United States. However, in the decades since HIPAA was enacted, new technologies have demonstrated the shortcomings of the Privacy Rule. In particular, the development of healthcare artificial intelligence (AI) has created new privacy concerns and exacerbated existing ones. This Note examines the current healthcare privacy framework in the United States and considers how healthcare AI complicates it. This Note also explores how AI developers need access to sensitive health information to build healthcare AI. To protect private health information while promoting AI development, this Note proposes a novel solution: impose a fiduciary duty on healthcare AI developers. Fiduciary relationships exist when one party has control over the other's affairs, like in doctor-patient or lawyer-client relationships. Instead of relying on consent, a fiduciary must act in the other party's best interest. Furthermore, imposing a fiduciary duty does not require the time or resources needed to create a new regulatory scheme. Ultimately, by requiring healthcare AI developers to act in the best interests of data subjects, fiduciary duties reinforce privacy protections without stifling access to data that is essential for AI development.

INTRODUCTION	385
I. PRIVACY LAW, HEALTHCARE AI, AND HOW HEALTHCARE AI UNDERMINES PRIVACY LAW	387
A. Privacy Laws for Health Information	387
1. HIPAA: What It Covers and What It Does Not	388
a. To Whom the Privacy Rule Applies	389

* J.D. Candidate, 2026, Fordham University School of Law; B.A., 2019, Georgetown University. I would like to thank Professor Chinmayi Sharma and the editors and staff of the *Fordham Law Review* for their guidance and assistance. I would also like to thank my family and friends for their support.

<i>b. What Information the Privacy Rule Covers</i>	390
<i>c. How HHS Enforces the Privacy Rule</i>	392
2. Privacy Policies and the FTC's Limited Powers of Enforcement.....	392
<i>a. Privacy Policies for Self-Regulation</i>	393
<i>b. The FTC's System of Quasi-Regulation</i>	394
3. Private Rights of Action Under State Law	396
<i>a. Privacy Torts</i>	396
<i>b. Healthcare Torts</i>	397
B. <i>The Rewards and Risks of Healthcare AI</i>	398
1. Overview of Healthcare AI.....	398
2. Privacy Concerns Posed by Healthcare AI.....	399
<i>a. Healthcare AI Requires and Creates Private Health Information</i>	400
<i>b. Healthcare AI Weakens De-Identification, and De-Identified Information Weakens Healthcare AI</i>	400
II. THE DEBATE OVER PROTECTING PRIVACY IN HEALTHCARE AI	402
A. <i>Proposals to Strengthen the Regulatory Regime</i>	403
1. Strengthen Regulators and Regulations.....	403
2. Update the Definition of Health Data to Apply More Broadly	405
3. Update the Standard for De-Identification	407
4. Require Technical Solutions.....	407
B. <i>Update and Strengthen the Notice-and-Choice Regime</i>	409
C. <i>Professionalize AI Developers</i>	411
1. Create a System of Self-Regulation Similar to Other Professions	411
2. Impose a Legal Duty on AI Developers	413
III. PROTECTING PRIVACY WHILE PROMOTING HEALTHCARE AI	415
A. <i>Courts Should Impose a Fiduciary Duty to Protect Health Information Without Impeding Healthcare AI</i> ...	415
1. A Fiduciary Duty Requires AI Developers to Protect Health Information	416
2. A Fiduciary Duty Allows AI Developers to Access High-Quality, Diverse Data	417
B. <i>Other Solutions Fall Short</i>	417
1. Proposals to Update the Regulatory Scheme Are Ineffective, Limited, or Untimely	418

2. Informed Consent Falls Short.....	419
3. How a Fiduciary Duty Can Complement Other Approaches	419
CONCLUSION.....	420

INTRODUCTION

On October 29, 2024, Elon Musk asked X users to submit their medical images to his artificial intelligence (AI) chatbot, Grok, to determine if Grok could accurately analyze the medical images.¹ Training an AI system to review medical images or predict aspects of a person's health requires "high-quality and diverse data."² By asking users to upload their photos voluntarily, Musk acquired the data for free.³ But that type of information, collected in that manner, is subject to very few privacy protections.⁴

Healthcare AI⁵ systems, like Grok, create and worsen privacy risks. Namely, AI developers require large volumes of identifiable data to build healthcare AI, and healthcare AI creates new health information, both of which present threats to privacy.⁶ This is problematic because the Health Insurance Portability and Accountability Act of 1996⁷ (HIPAA), the primary regulation establishing privacy standards for health information, does not apply to de-identified information or health information collected by social media or health apps.⁸ And even if the data is anonymized, AI can easily reidentify that information.⁹

Health privacy law exists to balance the sensitivity of health information with health providers' need for that information.¹⁰ Health information is sensitive because of stigmas surrounding health conditions, like lung

1. Elon Musk (@elonmusk), X (Oct. 29, 2024, 6:14 AM), <https://x.com/elonmusk/status/1851206080564773344> [<https://perma.cc/VH6U-UX5K>].

2. Elizabeth Passarella, *Elon Musk Asked People to Upload Their Health Data. X Users Obligated*, N.Y. TIMES (Nov. 18, 2024), <https://www.nytimes.com/2024/11/18/well/x-grok-health-privacy.html> (on file with the *Fordham Law Review*).

3. *See id.*

4. *See infra* Part I.A.1.b.

5. *See infra* note 144 and accompanying text for a definition of healthcare AI.

6. *See infra* Part I.B.2.a.

7. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code).

8. Passarella, *supra* note 2.

9. *See infra* Part I.A.2.b.

10. *See* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1442 (2002).

cancer,¹¹ abortion,¹² addiction,¹³ mental health,¹⁴ and obesity.¹⁵ Unwanted disclosures of health information—such as whether one has a sexually transmitted disease (STD) or is prone to a particular disease—can hurt relationships, cause embarrassment, or result in discrimination.¹⁶ But healthcare providers require access to such health information to diagnose and treat their patients.¹⁷ To address both concerns, health privacy laws promise the public that their doctor will not disclose their health information, which encourages an individual to speak honestly about their health with their provider.¹⁸

Yet healthcare AI promises to revolutionize the healthcare industry. Researchers at Stanford University developed an AI-powered program to predict genetic variations in breast cancers, which could improve clinical decision-making.¹⁹ Scientists at Boston University designed an AI program to predict whether a patient's dementia is associated with Alzheimer's disease.²⁰ Researchers at Harvard Medical School and the University of Oxford developed an AI tool that can predict new COVID-19 variants earlier than traditional methods.²¹ Healthcare AI can even make healthcare more accessible and affordable.²² Thus, the advent of healthcare AI creates two

11. See *Addressing Lung Cancer Stigma*, AM. LUNG ASS'N (June 7, 2024), <https://www.lung.org/lung-health-diseases/lung-disease-lookup/lung-cancer/living-with-lung-cancer/how-to-talk-about-your-cancer/addressing-lung-cancer-stigma> [https://perma.cc/DBC4-GG55].

12. See *Abortion Stigma*, PLANNED PARENTHOOD ADVOC. FUND OF MASS., <https://www.plannedparenthoodaction.org/planned-parenthood-advocacy-fund-massachusetts-inc/abortion-stigma> [https://perma.cc/AF48-E8W9] (last visited June 1, 2025).

13. See *Reducing the Stigma of Addiction*, JOHNS HOPKINS MED., <https://www.hopkinsmedicine.org/stigma-of-addiction> [https://perma.cc/P7T3-FPYW] (last visited June 1, 2025).

14. *Mental Health Stigma*, CTR. FOR DISEASE CONTROL & PREVENTION: MENTAL HEALTH, <https://www.cdc.gov/mental-health/stigma/index.html> [https://perma.cc/9NRD-9UD3] (last visited June 1, 2025).

15. Steve Hamm, *Stigma Adds Fuel to the Obesity Epidemic*, YALE MED. MAG., Autumn 2023, <https://medicine.yale.edu/news/yale-medicine-magazine/article/stigma-adds-fuel-to-the-obesity-epidemic/> [https://perma.cc/V6SJ-RVTR].

16. See Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOM. & TECH. L. REV. 1, 22 (2016); see also Gostin & Hodge, *supra* note 10, at 1470.

17. See Gostin & Hodge, *supra* note 10, at 1448.

18. See *id.*; see also Ford & Price, *supra* note 16, at 29.

19. See Sarah Williams, *AI Tool 'Sees' Cancer Gene Signatures in Biopsy Images*, STANFORD MED.: NEWS CTR. (Nov. 14, 2024), <https://med.stanford.edu/news/all-news/2024/11/cancer-gene-biopsy.html> [https://perma.cc/V337-DDPY].

20. Andrew Thurston, *New AI Program from BU Researchers Could Predict Likelihood of Alzheimer's Disease*, THE BRINK (June 25, 2024), <https://www.bu.edu/articles/2024/new-ai-program-could-predict-alzheimers-disease/> [https://perma.cc/5PM8-TBGN].

21. *New AI Tool Could Help Predict Viral Outbreaks*, UNIV. OF OXFORD: NEWS AND EVENTS (Oct. 19, 2023), <https://www.ox.ac.uk/news/2023-10-19-new-ai-tool-could-help-predict-viral-outbreaks> [https://perma.cc/ULQ7-WX3C].

22. See Sahil Gupta, *How AI Is Making Healthcare More Affordable and Accessible*, FORBES (Oct. 12, 2022, 08:30 ET), <https://www.forbes.com/councils/forbestechcouncil/2022/10/12/how-ai-is-making-healthcare-more-affordable-and-accessible/> [https://perma.cc/B795-NVG5] (discussing how AI can help healthcare become more affordable and equitable by reducing manual workload).

crucial but competing priorities: (1) supporting the development of healthcare AI and (2) protecting patient privacy.²³

President Joseph R. Biden Jr. declared that “to realize the promise of AI and avoid the risks, we need to govern this technology.”²⁴ To do just that, this Note suggests that courts should impose a fiduciary duty on AI developers with access to health information.²⁵ In reaching this conclusion, this Note proceeds in three parts. First, Part I details background information necessary to understand health privacy laws, healthcare AI, and how healthcare AI creates privacy risks. Next, Part II looks at proposals to better protect health information and assess arguments for and against those approaches. Finally, Part III advocates that courts impose a fiduciary duty on healthcare AI developers.

I. PRIVACY LAW, HEALTHCARE AI, AND HOW HEALTHCARE AI UNDERMINES PRIVACY LAW

The question of how to advance healthcare AI while protecting health information requires an understanding of existing privacy regulations and healthcare AI. Accordingly, Part I.A explains the primary statutes and legal regimes that currently govern the collection, use, and disclosure of health information. Part I.B then defines healthcare AI and examines how healthcare AI creates new privacy concerns and exacerbates existing ones.

A. Privacy Laws for Health Information

Information privacy law governs the collection, use, and disclosure of information.²⁶ The modern era of privacy law began in 1890, when Samuel D. Warren II and Justice Louis D. Brandeis published *The Right to Privacy*.²⁷ Warren and Justice Brandeis advocated for legal protection of privacy rights and created a new chapter of privacy law.²⁸ Since then, information privacy has grown into a body of law, including common law, statutory law, and international law, aimed at protecting personal information.²⁹

23. See generally W. Nicholson Price II, *Problematic Interactions Between AI and Health Privacy*, 2021 UTAH L. REV. 925.

24. Joseph Biden, President, & Kamala Harris, Vice President, Remarks on the Administration’s Commitment to Advancing the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Oct. 30, 2023, 14:45 ET), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/10/30/remarks-by-president-biden-and-vice-president-harris-on-the-administrations-commitment-to-advancing-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> [https://perma.cc/739F-BVXJ].

25. See *infra* Part III.

26. See DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (5th ed. 2014).

27. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

28. See generally *id.*

29. SOLOVE & SCHWARTZ, *supra* note 26, at 2, 10.

The United States' approach to data collection and privacy rights is sectoral in how the laws apply to specific industries³⁰ and permissive in that laws often permit data collection if the company obtained consent through notice-and-choice.³¹ Because of the fractured nature of U.S. privacy law, different laws and legal regimes apply to health information.³² Accordingly, this section examines the primary laws and enforcement mechanisms that can apply to health information. Part I.A.1 discusses HIPAA. Part I.A.2 explains how the Federal Trade Commission (FTC) enforces privacy policies. Finally, Part I.A.3 explores various common-law tort remedies.

1. HIPAA: What It Covers and What It Does Not

HIPAA is the principal federal legislation³³ that governs healthcare privacy in the United States.³⁴ As computers became more affordable and accessible, Congress passed HIPAA to establish standards for the electronic transmission of health information and to encourage health providers to use electronic health records (EHRs).³⁵ But switching to electronic systems increased concerns about loss of privacy.³⁶ In response, Congress created a privacy protection requirement and ordered the U.S. Department of Health and Human Services (HHS) to promulgate regulations to protect health information.³⁷

30. Nicolas Terry, *Of Regulating Healthcare AI and Robots*, 18 YALE J. HEALTH POL'Y, L. & ETHICS 133, 156 (2019).

31. Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 599 (2024). For a longer discussion on notice-and-choice, see *infra* notes 251–56 and accompanying text.

32. There is no one accepted definition for “health information,” but this Note adopts the European Union’s (EU) General Data Protection Regulation (GDPR) definition of health data as “data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.” Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

33. The U.S. Federal Drug Administration (FDA) is the premier agency that regulates medical devices. Terry, *supra* note 30, at 149. The FDA does not regulate the practice of medicine, such as when physicians use certain medical devices. *Id.*

34. See Leslie E. Wolf et al., *The Web of Legal Protections for Participants in Genomic Research*, 29 HEALTH MATRIX 1, 11 (2019).

35. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021 (codified as amended at 42 U.S.C. § 1320d note). Congress believed EHRs would improve the efficiency of the healthcare system by allowing easier storage and dissemination of health information. *Id.*; see also Gostin & Hodge, *supra* note 10, at 1444.

36. See Gostin & Hodge, *supra* note 10, at 1444; see also *Why Is the HIPAA Privacy Rule Needed?*, U.S. DEP’T OF HEALTH & HUM. SERVS. (Nov. 9, 2006), <https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html> [<https://perma.cc/Z675-Y48H>].

37. See 42 U.S.C. § 1320d-2(d); see also Gostin & Hodge, *supra* note 10, at 1444; U.S. DEP’T OF HEALTH & HUM. SERVS., *supra* note 36.

HHS issued the *Standards for Privacy of Individually Identifiable Health Information*³⁸ (the “Privacy Rule”) in 2002.³⁹ The Privacy Rule attempted to establish national privacy standards to guarantee a basic level of coverage for protected health information (PHI).⁴⁰ To do so, the Privacy Rule governs when and how certain entities may use or disclose PHI.⁴¹ This section explains to whom the Privacy Rule applies, what information it protects, and how it is enforced. It then explores how gaps in coverage leave certain health information unprotected.

a. To Whom the Privacy Rule Applies

The Privacy Rule only applies to covered entities and their business associates.⁴² Covered entities are healthcare clearinghouses,⁴³ health plans,⁴⁴ and healthcare providers⁴⁵ who electronically transmit health information.⁴⁶ Business associates are persons or organizations that provide services to or perform functions on behalf of a covered entity involving the use or disclosure of PHI.⁴⁷

This limited coverage means that data owners who are not covered entities or business associates can use PHI without complying with HIPAA.⁴⁸ This exemption created a loophole for data controllers that HIPAA did not anticipate. HIPAA does not typically bind mobile medical apps and data brokers.⁴⁹ For example, creators of period-tracking apps, which can contain

38. 45 C.F.R. §§ 160, 164 (2000).

39. See U.S. DEP’T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1–2 (May 2003), <https://www.hhs.gov/sites/default/files/privacysummary.pdf> [<https://perma.cc/3NCE-LRNA>]; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (codified as amended at 42 U.S.C. § 1320d-2 note).

40. See 45 C.F.R. §§ 160, 164 (2000).

41. See *How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?*, NAT’L INSTS. OF HEALTH (Feb. 2, 2007), http://privacyruleandresearch.nih.gov/pr_08.asp [<https://perma.cc/3KNT-W9Y8>].

42. See *Covered Entities and Business Associates*, U.S. DEP’T OF HEALTH & HUM. SERVS. (Aug. 21, 2024), <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html> [<https://perma.cc/56L7-YMAC>].

43. Healthcare clearinghouses are entities that exchange healthcare data between providers and payers by processing nonstandard health information into a standard. *Id.*

44. Health plans include health insurance companies, Medicare, and Medicaid. *Id.*

45. Healthcare providers include doctors, clinics, psychologists, dentists, and pharmacies. *Id.*

46. 45 C.F.R. § 164.500 (2025).

47. U.S. DEP’T OF HEALTH & HUM. SERVS., *supra* note 39, at 3. Business associates can include consultants who perform utilization reviews for hospitals, third-party administrators who assist covered entities with claims processing, and attorneys who provide legal services to a covered entity requiring access to PHI. *Business Associates*, U.S. DEP’T OF HEALTH & HUM. SERVS. (May 24, 2019), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html> [<https://perma.cc/W48R-RT8S>].

48. *Complying with FTC’s Health Breach Notification Rule*, FED. TRADE COMM’N (July 2024), <https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0> [<https://perma.cc/ZJ36-DNJL>] (“But many companies that collect people’s health information – whether it’s a fitness tracker, a diet app, a connected blood pressure cuff, or something else – aren’t covered by HIPAA.”).

49. Terry, *supra* note 30, at 157–58.

sensitive information about ovulation and when a pregnancy starts and ends, are not covered entities and can therefore legally share data.⁵⁰ Similarly, mental-health apps' privacy policies often permit the company to share data with third parties, which can lead to data controllers being able to access health information without complying with HIPAA.⁵¹

b. What Information the Privacy Rule Covers

The Privacy Rule only protects PHI⁵² that covered entities create or receive.⁵³ Conversations between doctors and nurses about a patient's treatment are PHI,⁵⁴ but health data collected on unregulated platforms, such as Facebook posts about vaccinations or WebMD search histories, are not.⁵⁵ This creates health privacy risks because information about social media use, purchases, and website visits can reveal sensitive health information.⁵⁶

Furthermore, de-identified information is not PHI, so the Privacy Rule does not apply.⁵⁷ De-identified data is health information that a covered entity reasonably believes is not individually identifiable.⁵⁸ Under the Privacy Rule, there are two ways to de-identify the data. First, a qualified individual can determine that the risk of reidentification is low.⁵⁹ Second, a

50. Geoffrey A. Fowler & Tatum Hunter, *For People Seeking Abortions, Digital Privacy is Suddenly Critical*, WASH. POST (June 24, 2022, 16:23 ET), <https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/> (on file with the *Fordham Law Review*).

51. Tatum Hunter & Jeremy B. Merrill, *Health Apps Share Your Concerns with Advertisers. HIPAA Can't Stop It*, WASH. POST (Sep. 22, 2022), <https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/> (on file with the *Fordham Law Review*).

52. Health information is information that "[r]elates to the past, present, or future . . . health or condition of an individual . . . or [the] future payment for the provision of health care to an individual." 45 C.F.R. § 160.103 (2025). PHI is the health information that is "individually identifiable" and "[t]ransmitted or maintained in any form or medium," including electronic media. *Id.*

53. *Id.* Public health authorities, employers, life insurers, and schools or universities are also entities that can create or receive health information, but this Note focuses on the covered entities. *Id.*

54. *Your Rights Under HIPAA*, U.S. DEP'T OF HEALTH & HUM. SERVS. (May 30, 2025), <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html> [<https://perma.cc/LYL6-PEXZ>].

55. See Sara Morrison, *HIPAA, The Health Privacy Law That's More Limited Than You Think, Explained*, VOX (July 30, 2021, 08:41 ET), <https://www.vox.com/recode/22363011/hipaa-not-hippa-explained-health-privacy> [<https://perma.cc/Z23G-Q27H>]. This health information would become PHI if shared with a covered entity. *Id.*

56. Hoag Levins, *Why HIPAA Is No Longer Enough to Guard Health Data*, PENN LEONARD DAVIS INST. OF HEALTH ECON. (Feb. 6, 2024), <https://ldi.upenn.edu/our-work/research-updates/why-hipaa-is-no-longer-enough-to-guard-health-data/> [<https://perma.cc/65NT-BKQ3>]; see Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Aug. 11, 2022, 04:17 ET), <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (on file with the *Fordham Law Review*) (describing how Target analyzes customers' purchase history to predict when a customer is pregnant).

57. 45 C.F.R. § 164.502(d)(2).

58. *Id.* § 164.514(a).

59. See *id.* § 164.514. A qualified person has "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering

covered entity can remove eighteen listed identifiers of the patient or their relatives, employers, or household members.⁶⁰ However, de-identifying data is an imperfect solution because it hinders research and does not sufficiently protect privacy. Practically, combining de-identified datasets without an identifier is difficult,⁶¹ and, as a result, the datasets are less valuable to researchers.⁶²

De-identification also does not sufficiently anonymize data⁶³ because the data can be easily reidentified.⁶⁴ Researchers can reidentify data by reviewing the dataset and finding unique data points about a data subject.⁶⁵ Then, researchers combine the unique data points with outside information.⁶⁶ When the data matches, it reveals the identity of the data subject.⁶⁷ As the amount of data available increases, it becomes easier for researchers to find data that unlocks anonymized data quickly.⁶⁸ For example, in 2018, researchers used newspaper data to match names to patient records.⁶⁹ Even when the data was de-identified according to HIPAA's standards, the researchers had a 3.2 percent reidentification rate for Maine records and a 10.6 percent reidentification rate for a single state's records.⁷⁰ Today, researchers estimate that between 63 percent and 87 percent of the U.S. population could be identified using gender, zip code, and date of birth.⁷¹

information not individually identifiable." *Id.* The qualified person must also document the methods that justify their determination. *Id.*

60. *See id.* These identifiers include names, geographic identifiers smaller than a state, dates (such as birth date, admission and discharge data, and dates indicative of age), and email addresses, among others. *Id.*

61. *See* INST. OF MED. COMM. ON HEALTH RSCH. & THE PRIV. OF HEALTH INFO., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 177–79 (Sharyl J. Nass, Laura A. Levit & Lawrence O. Gostin eds., 2009) (“[B]ecause datasets from multiple sources cannot be linked to generate a more complete record of a patient’s health history without a unique identifier, such datasets often are of minimal value to researchers and are not frequently used.”); *see also* Ford & Price, *supra* note 16, at 23.

62. *See* Ford & Price, *supra* note 16, at 23 n.75.

63. *See* Price, *supra* note 23, at 926; David M. Parker, Steven G. Pine & Zachary W. Ernst, *Privacy and Informed Consent for Research in the Age of Big Data*, 123 PENN. ST. L. REV. 703, 727 (2019).

64. Parker et al., *supra* note 63, at 727–28.

65. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1723 (2010).

66. *Id.* at 1723–24.

67. *Id.*

68. *Id.*

69. Ji Su Yoo, Alexandra Thaler, Latanya Sweeney & Jinyan Zang, *Risks to Patient Privacy: A Re-Identification of Patients in Maine and Vermont Statewide Hospital Data*, TECH. SCI. (Oct. 8, 2018), <https://techscience.org/a/2018100901/> [<https://perma.cc/BED5-VV T2>].

70. *Id.*

71. Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, AM. J. BIOETHICS, Sep. 2010, at 5.

c. How HHS Enforces the Privacy Rule

HHS's Office for Civil Rights (OCR) enforces the Privacy Rule.⁷² Typically, OCR investigates complaints filed by the public.⁷³ When OCR believes that a covered entity or business associate violated the Privacy Rule, it attempts to resolve the case through voluntary compliance, corrective actions, or resolution agreements.⁷⁴ OCR may also impose civil money penalties.⁷⁵ However, it rarely imposes civil penalties.⁷⁶ Although OCR received over 374,321 HIPAA complaints, it only settled or imposed a civil money penalty in 152 cases.⁷⁷

Because HIPAA does not create a private cause of action, enforcement is left exclusively to OCR.⁷⁸ Thus, individuals harmed by HIPAA violations can only seek redress by filing a complaint with HHS.⁷⁹ Even if HHS pursues the complaint, the victim may never receive compensation for those harms.⁸⁰

2. Privacy Policies and the FTC's
Limited Powers of Enforcement

Other privacy protections may apply even if HIPAA does not.⁸¹ Part I.A.2.a discusses how privacy policies led to a system of self-regulation. Part I.A.2.b explains how the FTC enforces those privacy policies.

72. *HIPAA Enforcement*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 25, 2017), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html> [https://perma.cc/TU6N-79R7]; Parker et al., *supra* note 63, at 708.

73. See U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 72; Parker et al., *supra* note 63, at 708.

74. *How OCR Enforces the HIPAA Privacy & Security Rules*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Nov. 20, 2023), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html> [https://perma.cc/N6CB-4P8S]. A resolution agreement is a settlement between HHS and a covered entity or business associate. *Resolution Agreements*, U.S. DEP'T OF HEALTH & HUM. SERVS. (May 30, 2025), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html> [https://perma.cc/TB5M-NQ8X]. The covered entity or business associate agrees to perform certain obligations and report to HHS, and HHS oversees the entity's compliance. *Id.*

75. 42 U.S.C. § 1302d-5; see also U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 72; Parker et al., *supra* note 63, at 708.

76. See *Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Nov. 21, 2024), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html> [https://perma.cc/L73B-TDDQ].

77. See *id.*

78. See *Meadows v. United Servs., Inc.*, 963 F.3d 240, 244 (2d. Cir. 2020) (noting that HIPAA does not expressly create a private cause of action nor does it imply one); see also *Wassef v. Tibben*, 68 F.4th 1083, 1089 (8th Cir. 2023); *Payne v. Taslimi*, 998 F.3d 648, 660 (4th Cir. 2021).

79. Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 200, 201–02 (2007).

80. *Id.*

81. The Privacy Rule permits states to pass legislation that implements stronger privacy protections for PHI. *Infra* note 110.

a. *Privacy Policies for Self-Regulation*

U.S. consumer privacy law relies on a form of self-regulation effectuated through privacy policies.⁸² Privacy policies govern the collection, use, and disclosure of personal data and notify data subjects of such activities.⁸³ Companies create privacy policies to promote transparency, explain why they collect information, or empower users to control how their data is collected.⁸⁴

However, this type of self-regulation does not adequately protect privacy. First, privacy policies do not promise high levels of protection because they allow companies to curate policies to shield themselves from liability.⁸⁵ Companies use their privacy policies to notify consumers that the company may use and share personal data at their discretions.⁸⁶ This notice provision helps shield the company from litigation.⁸⁷ However, the privacy policies are often dense, long, and wide-ranging.⁸⁸ Users are supposed to read the policies and then decide whether to consent to the data collection.⁸⁹ But if a

82. See Thorin Klosowski, *Here's What You're Actually Agreeing to When You Accept a Privacy Policy*, N.Y. TIMES (Apr. 14, 2023), <https://www.nytimes.com/wirecutter/blog/what-are-privacy-policies/> (on file with the *Fordham Law Review*) (noting that because there is no U.S. national privacy law, there are no requirements for what a company includes in their privacy policy). But certain statutes—like the EU's GDPR or the California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–199.100 (West 2025), (CCPA)—require certain information in privacy policies. See CAL. CIV. CODE § 1798.100(a)(1) (requiring that businesses provide consumers with notice of what information they collect, how they use it, if it is sold or shared, and if they collect sensitive personal information); Regulation 2016/679 of Apr. 27, 2016, art. 7(2), On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (“[T]he request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.”).

83. See Klosowski, *supra* note 82.

84. See *The New York Times Company Privacy Policy*, N.Y. TIMES (Mar. 3, 2025), <https://help.nytimes.com/hc/en-us/articles/10940941449492-The-New-York-Times-Company-Privacy-Policy> [<https://perma.cc/N9N5-X7HJ>] (“We want you to understand how we handle your personal information. We also want you to know your rights and choices.”); see also *Privacy Policy*, LINKEDIN (Sep. 18, 2024), <https://www.linkedin.com/legal/privacy-policy> [<https://perma.cc/6PZ2-9RD7>] (“Central to [LinkedIn’s] mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared.”); *Lyft Privacy Policy*, LYFT (Dec. 13, 2024), <https://www.lyft.com/privacy> [<https://perma.cc/M7CA-9PXE>] (“[To operate,] we need to collect, use, and share some of your personal information. This Privacy Policy is meant to help you understand how Lyft does that and how to exercise the choices and rights you have in your information.”).

85. See Klosowski, *supra* note 82.

86. *Id.*

87. *Id.*

88. *Id.*; see also Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words.*, WASH. POST (May 31, 2022), <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/> [<https://perma.cc/Y7QH-JV2J>]; Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES, <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> [<https://perma.cc/UP82-D5UH>] (last visited June 1, 2025).

89. JOSEPH TUROW, YPHTACH LELKES, NORA A. DRAPER & ARI EZRA WALDMAN, UNIV. OF PA.: ANNENBERG SCH. FOR COMM’N, AMERICANS CAN’T CONSENT TO COMPANIES’ USE OF

user cannot read the long, technically worded policies—and *understand* them enough to provide genuine consent—then this self-regulatory approach fails to adequately inform consumers of the privacy concerns.⁹⁰

*b. The FTC's System of
Quasi-Regulation*

Recognizing the shortcomings of pure self-regulation, the FTC began enforcing privacy policies in the 1990s.⁹¹ The Federal Trade Commission Act⁹² (FTCA) authorizes the FTC to investigate and prohibit unfair or deceptive acts or practices affecting commerce.⁹³

Violations of privacy policies can constitute unfair or deceptive practices.⁹⁴ If there is a violation, the FTC can enforce the privacy policy and require companies to safeguard personal data.⁹⁵ Recently, the FTC has taken a more aggressive approach, focusing less on the standards in the privacy policy and more on whether a company exploited consumers' expectations of privacy.⁹⁶ The FTC's enforcement has created a "quasi-self-regulatory" state.⁹⁷

The FTC can investigate companies that collect and use health information, even if those companies or that data are not restricted by the Privacy Rule.⁹⁸ For example, the FTC charged Cerebral, Inc. ("Cerebral") under the FTCA with unfair and deceptive privacy and data security

THEIR DATA 4 (2023), [https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t Consent.pdf](https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t%20Consent.pdf) [<https://perma.cc/LCP6-6FZ2>].

90. *Id.* at 3–4; *see also* Fowler, *supra* note 88. Furthermore, even when consumers want to opt out, they may have no real choice but to use certain websites because the modern world relies on technology. *See id.*

91. *See* Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), <https://www.brookings.edu/articles/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/> [<https://perma.cc/V4RR-4QCX>].

92. 15 U.S.C. §§ 41–58.

93. *Id.* § 45(a)(1). An unfair act or practice is one that "is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.* § 45(n). A deceptive act is "a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.'" Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) (quoting letter from James C. Miller III to Hon. John D. Dingell, Chairman, H. Comm. on Energy & Com. (Oct. 14, 1983)).

94. Solove & Hartzog, *supra* note 93, at 583.

95. *See* Hoofnagle, Hartzog & Solove, *supra* note 91; *see also* *The FTC Is Currently the Primary Privacy Enforcer but Its Authority Is Limited*, NEW AM., <https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/the-ftc-is-currently-the-primary-privacy-enforcer-but-its-authority-is-limited/> [<https://perma.cc/EP33-3HDY>] (last visited June 1, 2025).

96. Solove & Hartzog, *supra* note 93, at 667.

97. *See* Leslie Francis, *Health Information Beyond Pandemic Emergencies: Privacy for Social Justice*, 70 AM. U.L. REV. 1629, 1664 (2021).

98. *Id.* This type of health information can include a person's posts on Facebook about their vaccination status, trips to their doctor's office, and their wearable devices, like Fitbits, that track activity levels and sleep. *Id.*

practices.⁹⁹ Cerebral promotes and sells subscription services offering online health treatment and medication management.¹⁰⁰ In its complaint, the FTC alleged that Cerebral disclosed consumers' PHI to third parties for marketing purposes without express consent; the FTC also alleged that Cerebral failed to employ reasonable measures to protect consumers' personal information, which resulted in improper and unauthorized disclosures to third parties.¹⁰¹ The FTC claimed that those practices were unfair and thus violated the FTCA.¹⁰²

Although the FTC can bring these actions, its ability to protect private health information is limited by a lack of resources and statutory authority. Compared to other data protection agencies, the FTC has limited resources and is short-staffed.¹⁰³ As of 2020, the agency had no more than forty-five employees working in the Division of Privacy and Identity Protection.¹⁰⁴

Additionally, because the FTCA only authorizes the FTC to bring actions against unfair or deceptive practices, many privacy cases fall outside its enforcement scope.¹⁰⁵ For example, the FTC has indicated that a company acts unfairly or deceptively when it changes its privacy policy to collect more data and only notifies consumers through a surreptitious, retroactive change to the policy.¹⁰⁶ But this standard only applies to how the company provides notice, not to data the company collected.¹⁰⁷

Like HIPAA, the FTCA does not provide for private causes of action.¹⁰⁸ As a result, when the FTC does not have the resources to file a lawsuit, an individual cannot bring a case and will not be compensated for any harms they experience.¹⁰⁹

99. *See generally* Amended Complaint, United States v. Cerebral, Inc., No. 24-cv-21376, 2024 WL 3680027 (S.D. Fla. May 31, 2024).

100. *Id.* at 6.

101. *Id.* at 50.

102. *Id.*

103. *See FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security*, FED. TRADE COMM'N (2020), <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf> [<https://perma.cc/4C3Y-DTMP>]. In comparison, the United Kingdom's (U.K.) Information Commissioner's office, which is the equivalent data protection authority, has approximately 700 employees. *Id.* at 1. "The population of the U.K. is approximately 66 million." *Id.* at 1 n.1.

104. *Id.*

105. *See* Solove & Hartzog, *supra* note 93, at 583.

106. *AI (and Other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, FED. TRADE COMM'N (Feb. 13, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive> [<https://perma.cc/BC5Q-64C3>].

107. *Contra id.* (noting that companies engage in deceptive practices when they change their privacy policies without notifying consumers but not when they collect certain types of data).

108. Allan Bruce Currie, *A Private Right of Action Under Section Five of the Federal Trade Commission Act*, 22 HASTINGS L.J. 1268, 1268 (1971).

109. *See id.*

3. Private Rights of Action Under State Law

Although a plaintiff cannot bring a private suit under HIPAA or the FTCA, a plaintiff can bring a tort claim to enforce their privacy rights.¹¹⁰ This section explores privacy within the healthcare torts realm. Part I.A.3.a discusses traditional privacy torts, and Part I.A.3.b discusses healthcare-specific torts.

a. Privacy Torts

In response to concerns about sensational journalism and instant photography in the late nineteenth century, the common law developed tort remedies to address privacy harms.¹¹¹ Today, the Restatement (Second) of Torts recognizes four invasion of privacy torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation.¹¹² Certain jurisdictions also recognize a breach of confidence tort.¹¹³

But plaintiffs often face challenges proving certain elements in privacy torts, which makes this remedy ineffective for protecting privacy. For example, in *Purcell v. American Legion*,¹¹⁴ the plaintiff alleged that the defendant, their employer, discussed the plaintiff's health information with another employee.¹¹⁵ The court dismissed the case as a matter of law because the disclosure was not communicated to the public at large nor was it highly offensive.¹¹⁶ Likewise, in *Steinberg v. CVS Caremark Corp.*,¹¹⁷ the court found that the plaintiffs could not state a claim for intrusion upon seclusion when CVS sold their health data because the plaintiffs had voluntarily disclosed the information.¹¹⁸

110. See *Does the HIPAA Privacy Rule Preempt State Laws?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 28, 2022), <https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html> [<https://perma.cc/EP5U-TEEZ>] ("The HIPAA Privacy Rule provides a Federal floor of privacy protections."); see also *Sheldon v. Kettering Health Network*, 40 N.E. 3d 661, 671 (Ohio Ct. App. 2015) (holding that common-law torts are not preempted by HIPAA).

111. Warren & Brandeis, *supra* note 27, at 195; see SOLOVE & SCHWARTZ, *supra* note 26, at 11–12.

112. RESTATEMENT (SECOND) OF TORTS § 652A (A.L.I. 1977).

113. *Thomas v. TOMS King (Ohio), LLC*, 997 F.3d 629, 640 (6th Cir. 2021).

114. 44 F. Supp. 3d 1051 (E.D. Wash. 2014).

115. See *id.* at 1053. Specifically, the defendant told the employee that the plaintiffs had "mental problems" and "Post Traumatic Stress Disorder." *Id.*

116. See *id.* at 1061; see also *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1126–27 (S.D. Cal. 2023) (concluding that sharing browsing data does not reach the level of highly offensive).

117. 899 F. Supp. 2d 331 (E.D. Pa. 2012).

118. *Id.* at 342–43. See generally *Brown v. Google LLC*, 685 F. Supp. 3d 909 (N.D. Cal. 2023) (declining to conclude as a matter of law whether Google's collection of plaintiff's information was highly offensive and noting that Google's employees found the data collection problematic).

For a breach of confidence tort, it can be difficult for the plaintiff to show that a confidential relationship¹¹⁹ existed. In *Thomas v. TOMS King (Ohio), LLC*,¹²⁰ the court held that a confidential relationship did not exist between a restaurant and a customer, even though the restaurant must protect a customer's credit card information.¹²¹

Finally, to bring a privacy tort, a plaintiff may need to prove that the defendant intentionally disclosed the information.¹²² As a result, it is difficult for plaintiffs to bring a claim against a company when an unauthorized person accessed the data.¹²³

b. Healthcare Torts

Healthcare torts recognize the value of confidential patient-doctor relationships.¹²⁴ Confidentiality contributes to effective treatment by creating trust and facilitating open communication between patients and their doctors.¹²⁵ Some courts have held that *physicians and medical providers owe a fiduciary duty or quasi-fiduciary duty to their patients*.¹²⁶ A fiduciary is an individual or entity that has “a duty to act for the benefit of another on matters within the scope of the parties’ relationship.”¹²⁷ A fiduciary role develops when the individual or entity has control over an individual's person, property, or affairs, and the person must trust or rely on the fiduciary.¹²⁸ Generally, a fiduciary has the highest duty of loyalty to the party and must avoid self-dealing and conflicts of interest.¹²⁹

Other jurisdictions impose a duty of confidentiality on doctors, which resembles fiduciary duties.¹³⁰ For example, the Restatement (Third) of Torts provides that healthcare providers have a duty to use reasonable care in protecting confidential patient information from release without justification within the scope of any patient-care relationship.¹³¹

119. A confidential relationship is a relationship of trust that traditionally arises in close professional relationships, like a relationship with a doctor or financial institution. *Thomas v. TOMS King (Ohio), LLC*, 997 F.3d 629, 641 (6th Cir. 2021). Confidential relationships are usually professional relationships. *Id.*

120. 997 F.3d 629 (6th Cir. 2021).

121. *Id.* at 641.

122. *See Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1188 (M.D. Fla. 2022) (finding that a company's failure to protect information does not constitute intentional disclosure for the invasion of privacy tort).

123. *See id.* But the plaintiff could consider negligence claims. *See id.*

124. RESTATEMENT (THIRD) OF TORTS: CONCLUDING PROVISIONS § 3 (A.L.I. 2022).

125. *Id.*

126. *Id.*

127. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 16 (A.L.I. 2020).

128. *Id.*

129. *Id.*

130. RESTATEMENT (THIRD) OF TORTS: CONCLUDING PROVISIONS § 3 (A.L.I. 2022). Under federal regulations, a healthcare provider can include a doctor of osteopathy authorized to practice medicine or surgery or others who can provide healthcare services. 29 C.F.R. § 825.125. Others capable of providing these services include podiatrists, dentists, optometrists, nurse practitioners, clinical social workers, and more. *Id.*

131. RESTATEMENT (THIRD) OF TORTS: CONCLUDING PROVISIONS § 3 (A.L.I. 2022).

*B. The Rewards and Risks
of Healthcare AI*

Healthcare AI creates unique privacy concerns for health information. To elucidate the specific privacy concerns that healthcare AI generates, Part I.B.1 defines healthcare AI and how it works. Part I.B.2 then discusses how healthcare AI can create or worsen privacy risks.

1. Overview of Healthcare AI

U.S. law defines AI¹³² as a “machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.”¹³³ In other words, AI machines perform intelligently by acquiring information, interpreting the information, and approximating conclusions or completing tasks.¹³⁴

Both AI development and AI systems require large volumes of data.¹³⁵ When developing the AI model, developers need a significant amount of training data to teach the model how to make predictions.¹³⁶ An AI system designed to detect cancer, for example, required over one million images for training.¹³⁷ Furthermore, training data must be representative of the population to reduce bias.¹³⁸

Once trained, the AI model can analyze the data to identify patterns and make predictions.¹³⁹ Developers must keep “feeding” the systems with high-quality data to ensure the machines are up to date.¹⁴⁰ The AI model will

132. Machine learning is a subset of artificial intelligence. This Note uses AI to refer to all types of AI.

133. 15 U.S.C. § 9401(3).

134. ARTIFICIAL INTELLIGENCE: TECHNOLOGIES, APPLICATIONS, AND CHALLENGES 3–4 (Lavanya Sharma & Pradeep Kumar Garg eds., 1st ed. 2022); JULIE E. MEHAN, ARTIFICIAL INTELLIGENCE: ETHICAL, SOCIAL, AND SECURITY IMPACTS FOR THE PRESENT AND THE FUTURE 36 (IT Governance Publ’g ed., 2022). An algorithm is a list of instructions for solving a problem. *Id.*

135. *Defining AI and Chatbots*, STANFORD: TEACHING COMMONS, <https://teachingcommons.stanford.edu/teaching-guides/artificial-intelligence-teaching-guide/defining-ai-and-chatbots> [<https://perma.cc/G278-CHNK>] (last visited June 1, 2025).

136. See Parker et al., *supra* note 63, at 704–05; see also Ford & Price, *supra* note 16, at 7 (“Black-box medicine would not be possible without this mass of health data.”); *Defining AI and Chatbots*, *supra* note 135.

137. See generally Karin Dembrower, Peter Lindholm & Fredrik Strand, *A Multi-Million Mammography Image Dataset and Population-Based Screening Cohort for the Training and Evaluation of Deep Neural Networks—the Cohort of Screen-Aged Women (CSAW)*, 33 J. DIGIT. IMAGING 408 (2020).

138. NAT’L ACAD. OF MED., ARTIFICIAL INTELLIGENCE IN HEALTH CARE: THE HOPE, THE HYPE, THE PROMISE, THE PERIL 21–22 (Michael Matheny, Sonoo Thadaney Israni, Mahnoor Ahmed & Danielle Whicher eds., 2022).

139. See Parker et al., *supra* note 63, at 704; Ford & Price, *supra* note 16, at 7 (“Black-box medicine would not be possible without this mass of health data.”).

140. Kevin Roose, *The Data That Powers A.I. Is Disappearing Fast*, N.Y. TIMES (July 19, 2024), <https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html> (on file with the *Fordham Law Review*).

adapt to the input of new data.¹⁴¹ Researchers are excited about the application of AI to healthcare given the volume of health data.¹⁴² Data from electronic medical records, research studies, genetic information, radiology images, medical device sensing and surveillance, fitness trackers, period-tracking apps, clinical visits, pharmacy records, and insurance claims all reveal aspects of a person's health.¹⁴³

"Healthcare AI" refers broadly to any AI system that can aggregate, synthesize, and interpret health data or complete health-related tasks.¹⁴⁴ Healthcare AI can predict what treatment is likely to work for a specific patient, diagnose diseases, develop drugs and therapies, and complete administrative tasks.¹⁴⁵ The systems can identify subtle correlations between patients, medical diagnoses, and treatments that a doctor or researcher may not see.¹⁴⁶ Finally, researchers can even use AI to analyze social media data and identify social and economic factors affecting community health.¹⁴⁷

2. Privacy Concerns Posed by Healthcare AI

Certain privacy challenges persist with healthcare AI. For example, if healthcare AI creates an unwanted or unauthorized disclosure of information, plaintiffs will still have trouble proving certain elements in privacy torts or establishing a confidential relationship with the AI developer.¹⁴⁸ Healthcare theories of liability focus on the relationship between the physician and patient; however, an AI developer does not provide direct services like a

141. ARTIFICIAL INTELLIGENCE: TECHNOLOGIES, APPLICATIONS, AND CHALLENGES, *supra* note 134, at 6.

142. NAT'L ACAD. OF MED., *supra* note 138, at 16.

143. Parker et al., *supra* note 63, at 704; *see also* Ford & Price, *supra* note 16, at 7; ARTIFICIAL INTELLIGENCE: AN EMERGING APPROACH IN HEALTHCARE 88–89 (Yash Tyagi & Pardeep Kumar Sharma eds., 1st ed. 2021) ("The AI system relies on massive medical data such as EHRs, insurance claim records, sexual preference, genetic information, dietary habits, etc.").

144. *See* NAT'L ACAD. OF MED., *supra* note 138, at 16–17; *see also* Thomas Davenport & Ravi Kalakota, *The Potential for Artificial Intelligence in Healthcare*, 6 FUTURE HEALTHCARE J. 94, 94 (2019). *See generally* ARTIFICIAL INTELLIGENCE: AN EMERGING APPROACH IN HEALTHCARE, *supra* note 143.

145. Davenport & Kalakota, *supra* note 144, at 94; *Artificial Intelligence for Drug Development*, FDA (Oct. 31, 2024), <https://www.fda.gov/science-research/science-and-research-special-topics/artificial-intelligence-and-machine-learning-aiml-drug-development> [<https://perma.cc/AAK2-538A>]. Machine-learning algorithms analyze medical data to discover connections between specific patient attributes and specific symptoms, diseases, or treatments. *See* Ford & Price, *supra* note 16, at 5.

146. *See* Ford & Price, *supra* note 16, at 26. For example, researchers at Northwestern University and the University of Cincinnati created a predictive model using machine-learning algorithms to inform COVID-19 vaccine campaigns. Win Reynolds, *AI Tool Predicts COVID-19 Vaccine Uptake*, NW NOW (Mar. 18, 2024), <https://news.northwestern.edu/stories/2024/03/ai-vaccine-uptake/> [<https://perma.cc/J92S-WNS2>]. The researchers noted that behavioral and emotional factors contribute to public health research. *Id.* To identify these patterns, the researchers had access to respondents' demographics, their interests in hobbies, and more to predict vaccine uptake. *See id.*

147. NAT'L ACAD. OF MED., *supra* note 138, at 21.

148. *See supra* Part I.A.3.a.

doctor, and therefore the relationship may not be considered a doctor-patient relationship.¹⁴⁹

Most concerning is that developing and deploying healthcare AI creates new privacy issues, and existing privacy protections weaken healthcare AI.¹⁵⁰ This section explores that dilemma. Part I.B.2.a discusses how healthcare AI creates new privacy risks by requiring significant amounts of data and generating new information. Part I.B.2.b examines how healthcare AI makes reidentification easier and how de-identification weakens AI's usefulness.

*a. Healthcare AI Requires and Creates
Private Health Information*

Because healthcare AI requires a lot of high-quality, detailed data,¹⁵¹ companies developing healthcare AI are incentivized to collect additional data.¹⁵² To collect that data, organizations can update their privacy policies to allow for increased use, collection, and sharing of information, making the policies even less protective.¹⁵³ Furthermore, because AI developers need sensitive health data to create healthcare AI,¹⁵⁴ they become another group with access to the data, which could lead to more people overall seeing this information.¹⁵⁵

As certain types of healthcare AI aim to identify patterns or predict predispositions, they may generate new health information that individuals do not want disclosed.¹⁵⁶ For instance, an AI system might predict that a patient is likely to develop heart disease.¹⁵⁷ Although the patient's insurer would likely want that information, the patient would likely not want to share it.¹⁵⁸

*b. Healthcare AI Weakens De-Identification,
and De-Identified Information
Weakens Healthcare AI*

HIPAA assumes that de-identification guarantees privacy,¹⁵⁹ but healthcare AI challenges that premise. At the same time, de-identification

149. See Jessica S. Allain, *From Jeopardy! to Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems*, 73 LA. L. REV. 1049, 1062, 1072 (2013) (expressing doubt about whether AI can form a physician-patient relationship, given most consulting physicians do not have a physician-patient relationship themselves).

150. See Price, *supra* note 23, at 925–26.

151. See *supra* Part I.B.1.

152. See FED. TRADE COMM'N, *supra* note 106.

153. See *id.*

154. NAT'L ACAD. OF MED., *supra* note 138, at 20.

155. See Ford & Price, *supra* note 16, at 25.

156. *Id.* at 21.

157. See *id.* at 26.

158. See *id.*

159. See 45 C.F.R. § 164.502(d)(2).

can undermine the utility of AI. The three key issues that arise when using de-identified data in healthcare AI are: inadequacy of de-identification as a privacy safeguard, biased training datasets, and removal of necessary information.

First, AI makes it even easier to reidentify de-identified information.¹⁶⁰ Because HIPAA does not apply to de-identified data,¹⁶¹ a covered entity can transfer de-identified health information to AI developers without restriction.¹⁶² Then, the AI system can find patterns in the data and reidentify the data.¹⁶³ In fact, researchers used AI to reidentify patients from a dataset of physical activity collected from wearable fitness trackers.¹⁶⁴ AI systems can even extract identifiable data from purely synthetic datasets.¹⁶⁵

Second, de-identified data may lead to biased results. De-identification is expensive, which means only well-resourced institutions can afford it.¹⁶⁶ Because of this, AI developers may only have access to training data from high-resourced patients and communities.¹⁶⁷ These AI systems may reflect those care patterns and perform poorly in less-resourced contexts, thus leading to biased AI systems.¹⁶⁸ Additionally, health information from nonhealth data sources, like Google and Apple products, can contribute to bias because their user communities do not represent the general populace.¹⁶⁹ Without access to broad, diverse datasets that are representative of the population, AI systems can encode biases.¹⁷⁰

Furthermore, having access to identifiable data points, like socioeconomic status, race, religion, gender, or sexual orientation, can help AI developers correct for bias embedded in their systems.¹⁷¹ In one case, an algorithm designed to predict which patients needed extra medical care severely underestimated the health needs of Black patients.¹⁷² Although the model did not explicitly include race, it relied on healthcare spending data, which

160. Price, *supra* note 23, at 926.

161. See 45 C.F.R. § 164.502(d)(2).

162. See Price, *supra* note 23, at 930–31. The covered entity may face further restrictions in certain states with additional privacy laws regulating health data. See *supra* note 110 and accompanying text.

163. *Id.* at 926.

164. *Id.*

165. *Id.* at 928. (“[S]ome systems can still glean information about identifiable people from whose data the synthetic dataset was initially created.”).

166. *Id.* at 931.

167. See *id.* at 934.

168. See *id.*

169. See *id.* at 934–35.

170. See *id.* at 930.

171. Taylor Mitchell, *Algorithmic Bias in Health Care Exacerbates Social Inequities—How to Prevent It*, HARV. T.H. CHAN: SCH. OF PUB. HEALTH (Mar. 12, 2021), <https://www.hsph.harvard.edu/ecpe/how-to-prevent-algorithmic-bias-in-health-care/> [<https://perma.cc/UEC2-ZV3K>].

172. Carolyn Y. Johnson, *Racial Bias in a Medical Algorithm Favors White Patients Over Sicker Black Patients*, WASH. POST (Oct. 24, 2019), <https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/> (on file with the *Fordham Law Review*).

researchers found was not “a race-neutral measure of health-care need.”¹⁷³ Eventually, the researchers updated the algorithm so it could not use the cost of medical visits as a predictor.¹⁷⁴ It was easier for the researchers to identify and correct the bias because they had access to the training data.¹⁷⁵ In this instance, identifiable information improved the fairness of the AI systems, even though such data typically heightens privacy risks.

Third, de-identification can remove information that is necessary to accomplish the purpose of the AI system.¹⁷⁶ In some cases, de-identification may require removing information like zip code and age, which can be important for predictive AI.¹⁷⁷ On a larger scale, de-identification can make it harder for AI developers to rejoin multiple datasets because the de-identified data lacks identifiers.¹⁷⁸ Additionally, records that track patients over an extended period are valuable for research, but de-identification makes compiling long-term records harder.¹⁷⁹ Thus, attempts at protecting patient information can make AI less effective.

Given these challenges, society is stuck with a conundrum: healthcare AI weakens privacy protections, but privacy protections weaken healthcare AI.¹⁸⁰ The current framework does not adequately protect health information, but imposing more regulations will delay or prevent access to the large volume of data healthcare AI needs.¹⁸¹ As this Note discusses, acting in favor of either privacy or technological progress culminates in problems for the other.¹⁸²

II. THE DEBATE OVER PROTECTING PRIVACY IN HEALTHCARE AI

Although many agree that current laws do not adequately protect privacy, there are conflicting opinions on how to protect that information, especially

173. *Id.*

174. *Id.*

175. *Id.* Additionally, a “study found AI tools ‘consistently and selectively under-diagnosed under-served patient populations,’ finding the under-diagnosis rate was higher for marginalized communities who disproportionately don’t have access to medical care.” Crystal Grant, *Algorithms Are Making Decisions About Health Care, Which May Only Worsen Medical Racism*, ACLU (Oct. 3, 2022), <https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism> [https://perma.cc/U4WH-VQPF] (quoting Laleh Seyyed-Kalantari, Haoran Zhang, Matthew B. A. McDermott, Irene Y. Chen & Marzyeh Ghassemi, *Underdiagnosis Bias of Artificial Intelligence Algorithms Applied to Chest Radiographs in Under-Served Patient Populations*, 27 NATURE MED. 2176, 2176 (2021)).

176. Price, *supra* note 23, at 930–31.

177. *See id.* at 930.

178. *See id.* at 931.

179. *Id.*

180. *See id.* at 930.

181. *See id.*

182. Ford & Price, *supra* note 16, at 4.

considering AI. This part explores various proposed solutions and efforts taken¹⁸³ to protect health information.

Part II.A surveys proposals to update the current regulatory structure. Part II.B presents arguments to strengthen data subjects' rights. Finally, Part II.C reviews proposals to professionalize AI developers.

A. Proposals to Strengthen the Regulatory Regime

In the decades since the Privacy Rule was passed, many proposed strengthening or expanding HIPAA to better protect health information. Solutions address updating to whom the regulation applies, when it applies, and how it is enforced. Accordingly, Part II.A.1 explores proposals for empowering regulatory bodies. Part II.A.2 discusses proposals to update the definition of health information. Part II.A.3 explains proposals recommending updating the standard for de-identification. Finally, Part II.A.4 explores proposed technical solutions.

1. Strengthen Regulators and Regulations

Although the current regulatory regime does not adequately protect privacy, many have nevertheless proposed strengthening¹⁸⁴ it to address its shortcomings.¹⁸⁵ Several theorists have outlined proposals for a stronger regulatory scheme. Professor Nicolas P. Terry suggested creating a new regulatory agency for AI.¹⁸⁶ Professors Nicholson Price and Roger Allan Ford discuss how existing agencies, like the U.S. Food and Drug Administration (FDA) or World Health Organization (WHO), could oversee healthcare AI.¹⁸⁷

Regardless of which agency leads this effort, most proponents of strengthening the existing regime believe that agencies should act as independent third parties overseeing and regulating AI.¹⁸⁸ Because

183. Many states addressed gaps and weaknesses in federal legislation by passing sectoral legislation to regulate privacy. SOLOVE & SCHWARTZ, *supra* note 26, at 793. Without federal legislation, some states have adopted or are proposing legislation to regulate AI systems. Cecilia Kang, *States Take Up AI Regulation Amid Federal Standstill*, N.Y. TIMES (June 10, 2024), <https://www.nytimes.com/2024/06/10/technology/california-ai-regulation.html> (on file with the *Fordham Law Review*).

184. Besides broadening the definition of health information, to whom regulations apply, and the de-identification standard, the agency could issue other regulations to comply with data protection practices. For example, an independent regulatory agency can determine when researchers can access the data, require entities to obtain permission before using PHI, or impose information security requirements and adopt an FTC quasi-common-law enforcement method. See Ford & Price, *supra* note 16, at 35–37.

185. Terry, *supra* note 30, at 173; Matthew S. McCoy, Anita L. Allen, Katharina Kopp, Michelle M. Mello, D. J. Patil, Pilar Ossorio, Steven Joffe & Ezekiel J. Emanuel, *Ethical Responsibilities for Companies That Process Personal Data*, AM. J. BIOETHICS, 2023, at 10.

186. Terry, *supra* note 30, at 163.

187. See Ford & Price, *supra* note 16, at 35.

188. Terry, *supra* note 30, at 173–74; McCoy et al., *supra* note 185.

administrative agencies are staffed with bureaucrats rather than elected officials, they can remain independent from political pressure and rely on their expertise and judgment.¹⁸⁹ This independence allows agencies to solve problems with neutral criteria and broad social considerations, without extensive influence from electoral policies or lobbyists.¹⁹⁰ Furthermore, agencies allow public participation.¹⁹¹ Promulgating rules requires public comment, so data subjects can participate in the rulemaking process and provide their own opinions.¹⁹²

Critics of this approach argue that updating a regulation is a lengthy process that requires many resources and encroaches on data subjects' autonomy. Professor Mark A. Rothstein at the University of Louisville School of Medicine cautioned that designing a regulatory approach would take too long.¹⁹³ Professor Rothstein compared the process of developing a new regulatory scheme to the process of implementing the Privacy Rule.¹⁹⁴ It took the HHS years to implement the Privacy Rule because they frequently consulted with stakeholders and the public.¹⁹⁵ Creating new regulations or regulatory agencies for healthcare AI would require a similar amount of time.¹⁹⁶

Additionally, creating a new agency or empowering an existing one requires a lot of resources. Current legislators and politicians are increasingly skeptical of agencies, so Congress is unlikely to fund a new agency or expand the power of existing agencies fast enough to address the existing issues with healthcare AI.¹⁹⁷

189. See Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353, 381, 385 (2016).

190. See *id.* at 385.

191. See *id.* at 387.

192. See *id.*

193. Rothstein, *supra* note 71, at 11. HIPAA was enacted in 1996. U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 39. HHS released a proposed privacy rule in 1999 and published the final rule in 2002. *Id.*

194. Rothstein, *supra* note 71, at 11.

195. *Id.*

196. *Id.*

197. See, e.g., Elena Shao & Ashley Wu, *The Federal Work Force Cuts So Far, Agency by Agency*, N.Y. TIMES (May 12, 2025), <https://www.nytimes.com/interactive/2025/03/28/us/politics/trump-doge-federal-job-cuts.html> (on file with the *Fordham Law Review*); Karoun Demirjian & Apoorva Mandavilli, *Trump Administration Proposes Sharp Budget Cuts for H.H.S.*, N.Y. TIMES (Apr. 18, 2025), <https://www.nytimes.com/2025/04/17/us/politics/trump-administration-proposes-health-department-cuts.html> (on file with the *Fordham Law Review*); Eileen Sullivan, *With Painful Layoffs Ahead, Agencies Push Incentives to Quit*, N.Y. TIMES (Apr. 1, 2025), <https://www.nytimes.com/2025/04/01/us/politics/federal-layoff-buyout-offers.html> (on file with the *Fordham Law Review*); Sheryl Gay Stolberg & Christina Jewett, *10,000 Federal Health Workers to Be Laid Off*, N.Y. TIMES (Mar. 27, 2025), <https://www.nytimes.com/2025/03/27/us/politics/health-department-job-layoffs-rfk-jr.html> (on file with the *Fordham Law Review*); Robert Draper, Michael Crowley & Zach Montague, *Inside the Federal Workforce That Trump Has Promised to Eviscerate*, N.Y. TIMES (Nov. 8, 2024), <https://www.nytimes.com/2024/11/08/us/politics/trump-federal-bureaucracy.html> (on file with the *Fordham Law Review*); Michael D. Shear & Eric Lipton, *Trump Taps Elon Musk and Vivek Ramaswamy to Slash Government*, N.Y. TIMES (Nov. 12, 2024), <https://www.nytimes.com/2024/11/12/us/politics/trump-elon-musk-vivek-ramaswamy.html> (on file with the *Fordham Law Review*).

A new regulatory approach would also impact nongovernment resources. It is possible that if the number of regulations increases, companies will need to divert existing resources toward compliance rather than improving and modernizing the health system.¹⁹⁸ As a result, new regulations may stymie progress.¹⁹⁹

Additionally, Professor Daniel J. Solove, a leading privacy expert, asserted that a regulatory approach may encroach upon patients' or individuals' autonomy.²⁰⁰ He reasoned that if a regulation can stipulate when data is collected, used, or disclosed, individuals may lose the choice to use their data in ways they want, relinquishing autonomy to sell or manage their own personal data.²⁰¹

2. Update the Definition of Health Data to Apply More Broadly

Scholars have proposed that HHS update the definition of "health information" to cover all types of data related to an individual's health.²⁰² Some states and other countries have already addressed this concern by creating a more expansive definition of health information in their data privacy laws.²⁰³ For example, the General Data Protection Regulation²⁰⁴ (GDPR) governs the processing of personal data,²⁰⁵ the movement of personal data, and the rights of data subjects to their personal data in the European Union (EU).²⁰⁶ The GDPR defines "personal data concerning health" as all data related to a subject's health status that reveals information

imes.com/2024/11/12/us/politics/elon-musk-vivek-ramaswamy-trump.html (on file with the *Fordham Law Review*).

198. W. Nicholson Price II, Margot E. Kaminski, Timo Minssen & Kayte Spector-Bagdady, *Shadow Health Records Meet New Data Privacy Laws*, 363 *SCI.* 448 (2019), <https://pmc.ncbi.nlm.nih.gov/articles/PMC6417878/pdf/nihms-1011085.pdf> [<https://pema.cc/7H6U-VSTN>].

199. *Id.*

200. See Solove, *supra* note 31, at 597–98.

201. See *id.* at 600.

202. Price et al., *supra* note 198; Daniel Lenihan, Letter to the Editor, *Health Data Privacy Laws Should Be Updated*, WASH. POST (Mar. 1, 2023), <https://www.washingtonpost.com/opinions/2023/03/01/data-privacy-health-care-hipaa/> (on file with the *Fordham Law Review*).

203. Price et al., *supra* note 198 (noting that the GDPR and CCPA close problematic loopholes that allowed certain entities to use health information unregulated by HIPAA); Lenihan, *supra* note 202.

204. Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

205. Personal information is "information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Regulation 2016/679 of Apr. 27, 2016, art. 4, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

206. *Id.* art. 1.

about the subject's past, present, or future health status.²⁰⁷ Unlike HIPAA, the GDPR applies to all health information, regardless of where the information came from or who controls it.²⁰⁸

Similarly, the California Consumer Privacy Act of 2018²⁰⁹ (CCPA) applies broadly to personal information.²¹⁰ The CCPA defines sensitive personal information as information that concerns the consumer's health.²¹¹ The CCPA gives California residents the right to know about a company's personal data collection and control how a company can use the data.²¹² Businesses subject to the CCPA must follow certain purpose-limitation and data-minimization rules.²¹³

Compared to HIPAA, the GDPR and CCPA extend protections to a wider array of health data.²¹⁴ Companies can circumvent HIPAA by gathering data from sources not covered by HIPAA, like fitness apps or social media posts, or purchasing HIPAA de-identified data, reidentifying it, and using it to create health inferences.²¹⁵ Because HIPAA does not protect those records, companies can use the data to identify high-cost patients and create targeted advertisements.²¹⁶ However, GDPR and CCPA impose stricter rules that prevent such circumvention.²¹⁷

Still, overly broad language in statutes like the GDPR or CCPA leads to confusion about how data can be used.²¹⁸ Regulations without clear language can discourage researchers from using data, especially if they do not know whether that use is permissible.²¹⁹ Even if researchers decide to use the data, they must implement solutions to protect that information, thus reducing health system modernization and quality improvement.²²⁰ Conversely, when researchers can use unregulated data, they progress faster because they do not need to comply with regulations.²²¹

207. *Id.* recital 35.

208. *See supra* Part I.A.1.a.

209. CAL. CIV. CODE §§ 1798.100–199.100 (West 2025).

210. Price et al., *supra* note 198.

211. CAL. CIV. CODE § 1798.140 (ae)(2)(C). The CCPA does not apply to information covered under HIPAA. Price et al., *supra* note 198.

212. *Frequently Asked Questions (FAQs)*, CAL. PRIV. PROT. AGENCY, <https://cppa.ca.gov/faq.html> [<https://perma.cc/57ZZ-SM8L>] (last visited Aug. 21, 2025).

213. *Id.*

214. Price et al., *supra* note 198.

215. *Id.*

216. *Id.*

217. *See id.*

218. *See id.*

219. *See id.* If there are too many regulatory hurdles, entities may shift their focus to less regulated industries. *Id.*

220. *See id.* This can occur if under-resourced firms cannot afford to comply with additional regulations. *See id.*

221. *See id.*

3. Update the Standard for De-Identification

To increase protection, some scholars have proposed a higher standard of de-identification.²²² Analysts at Harvard University proposed creating flexible standards to keep up with technological advancements, rather than the rigid checklist standard for de-identification currently used by HIPAA.²²³ Another scholar also proposed more flexible standards, advocating for a “least identifiable form consistent with the purpose” standard.²²⁴ This standard would only require data collectors to maintain identifiable information that is necessary for their unique project.²²⁵

HIPAA could implement the GDPR’s standard for de-identification, which is flexible and more rigorous.²²⁶ The GDPR requires controllers to consider all methods reasonably likely to be used to identify the data subject.²²⁷ Unlike HIPAA, the GDPR aims to prevent reidentification by setting a de-identification standard that excludes data reasonably capable of being traced back to an individual using external information.²²⁸

However, Professors Ford and Price oppose de-identification because AI needs identified information to function properly.²²⁹ AI is a powerful tool because it finds subtle patterns in data that may lead to inferences or predictions useful for treatment or diagnosis.²³⁰ Without access to information like race, sex, gender, or other individualized characteristics that may factor into treatment or diagnosis, AI systems cannot draw those accurate conclusions or predictions.²³¹ Because de-identification is not a sufficient method of protection, data controllers should not de-identify information, particularly when AI would be more effective with identifiers.²³²

4. Require Technical Solutions

Another set of proposals urges agencies to issue new regulations with updated technical solutions. Historically, medical institutions did not want

222. Yoo et al., *supra* note 69; Rothstein, *supra* note 71, at 10–11.

223. Yoo et al., *supra* note 69.

224. Rothstein, *supra* note 71, at 11.

225. *Id.*

226. Parker et al., *supra* note 63, at 721. Like HIPAA, the provisions of the GDPR no longer apply when the data is de-identified. *Id.* Additionally, the entity would need a lawful basis for processing, such as consent. *Id.*

227. Regulation 2016/679 of Apr. 27, 2016, art. 83(26), On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1. Instead of de-identified data, the GDPR refers to this type of data as anonymized data. *Id.*

228. *See* Parker et al., *supra* note 63, at 721.

229. Ford & Price, *supra* note 16, at 34 n.105.

230. *Id.* at 9.

231. *Id.*

232. *Id.* at 34 n.105.

to share patient information for fear of breaching their patients' trust.²³³ To alleviate this concern, scientists recommend that agencies issue regulations requiring AI developers to implement robust cybersecurity measures.²³⁴

Various technical solutions have been proposed to address privacy concerns. For instance, developers could implement distributed machine learning.²³⁵ Distributed machine learning is a technique that only shares mathematical parameters and metadata, rather than medical information, across servers, preventing sensitive data from leaving the clinic.²³⁶ Another proposed technique is blockchain-powered storage.²³⁷ This method distributes data across a decentralized network, while protecting the data with cryptographic algorithms to prevent unauthorized access.²³⁸ Finally, other researchers recommended that data controllers store data used in AI separately from data not used in AI.²³⁹ To do so, developers can use segregated write-only data vaults to develop algorithms, which cannot export data for other uses.²⁴⁰ AI developers can then use the data for their purposes while preventing access for non-AI purposes.²⁴¹

The EU has already passed legislation with new technical solutions. The EU Artificial Intelligence Act²⁴² (the "EU AI Act") imposed technical security standards with which the owners of AI systems must comply.²⁴³ For example, the Act requires some providers to have a quality management system in place and undergo a conformity assessment; further, when necessary to process special categories of personal data, the Act requires providers to comply with requirements in the GDPR and delete the data once the bias is corrected or they reach the end of a retention period.²⁴⁴

However, critics argue that security practices can become outdated quickly.²⁴⁵ This is what happened with the de-identification standards in

233. Fadila Zerka et al., *Systematic Review of Privacy-Preserving Distributed Machine Learning from Federated Databases in Health Care*, 4 ASCO PUBL'NS 184, 192 (2020).

234. *Id.* at 194; Nazish Khalid, Adnan Qayyum, Muhammad Bilal, Ala Al-Fuqaha & Junaid Qadir, *Privacy-Preserving Artificial Intelligence in Healthcare: Techniques and Applications*, COMPUTS. BIOLOGY & MED., 2023, at 11 (exploring technical methods to preserve privacy while using healthcare AI).

235. *Id.*

236. *Id.*

237. Scott Doughman, *How Blockchain Can Improve Data Security in Healthcare*, WORLD ECON. F.: EMERGING TECHS. (Dec. 5, 2023), <https://www.weforum.org/stories/2023/12/health-care-data-breaches-blockchain-cybersecurity/> [<https://perma.cc/5MLC-FF5R>].

238. *Id.*

239. *See* Ford & Price, *supra* note 16, at 32.

240. *See id.*

241. *See id.*

242. Regulation 2024/1689, Artificial Intelligence Act, 2024 O.J. (L).

243. James Clark, Muhammed Demircan & Kalyna Kettas, *Europe: The EU AI Act's Relationship with Data Protection Law: Key Takeaways*, PRIV. MATTERS (Apr. 25, 2024), <https://privacymatters.dlapiper.com/2024/-4/europe-the-eu-acts-relationship-with-data-protection-law-key-takeaways/> [<https://perma.cc/947T-BD5Y>].

244. Regulation 2024/1689, art. 2 §§ 8–10, Artificial Intelligence Act, 2024 O.J. (L). This is not an exhaustive list of requirements with which the providers must comply. *Id.* art. 10.

245. *See* Ford & Price, *supra* note 16, at 37.

HIPAA, which fail to sufficiently protect health information.²⁴⁶ Because healthcare AI evolves quickly, technical solutions rapidly become outdated.²⁴⁷

In addition to security concerns, critics worry that strict technical regulations could prevent AI developers from sharing information with healthcare providers. This concern is evident in controlled access systems, which make it difficult for other researchers to access the data and to verify the AI system's outputs.²⁴⁸ Furthermore, clinicians may want to see the data before relying on an AI recommendation.²⁴⁹ For instance, a clinician might want to review the training data for bias before applying the recommendation to a patient's care.²⁵⁰ Thus, new measures that may become outdated quickly could undermine trust in AI.

*B. Update and Strengthen the
Notice-and-Choice Regime*

Another proposed solution includes strengthening the notice-and-choice regime.²⁵¹ Under this regime, informed consent is the primary procedural protection that ensures privacy.²⁵² Individuals can evaluate their options and decide whether to allow an entity to use or control their data.²⁵³ This framework assumes that the individual is free from coercion and can make an informed decision, evaluate privacy risks, and then decide in their self-interest.²⁵⁴ Some laws use an "opt-out" approach, requiring users to exercise their ability to consent by actively choosing not to provide their data.²⁵⁵ Other laws use the "opt-in" approach, which provides baseline protections by requiring users to affirmatively consent to data collection and use.²⁵⁶

Proponents of the notice-and-choice regime believe that requiring consent will create more trust in the health and research community.²⁵⁷ They reason that if patients understand how their information is used, they will develop greater trust within the healthcare community.²⁵⁸ One advocate argues that when custodians receive consent, custodians respect patients' autonomy.²⁵⁹

246. See *supra* Part I.A.1.a.

247. See Ford & Price, *supra* note 16, at 37.

248. Gina Kolata, *Your Data Were 'Anonymized'?: These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), <https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html> (on file with the *Fordham Law Review*).

249. Trishan Panch, Heather Mattie & Rifat Atun, *Artificial Intelligence and Algorithmic Bias: Implications for Health Systems*, 9 J. GLOB. HEALTH 1, 3 (2019).

250. See *id.*

251. See Parker et al., *supra* note 63, at 727.

252. Amy Winograd, *Loose-Lipped Large Language Models Spill Your Secrets: The Privacy Implications of Large Language Models*, 36 HARV. J.L. & TECH. 615, 632 (2023).

253. See ARI EZRA WALDMAN, *PRIVACY AS TRUST* 83 (Cambridge Univ. Press 2018).

254. *Id.*; Winograd, *supra* note 252, at 633.

255. Winograd, *supra* note 252, at 633.

256. *Id.*

257. Parker et al., *supra* note 63, at 725.

258. See *id.*

259. See Solove, *supra* note 31, at 628.

They do so by waiting to collect the data until the patient made their choice about whether the collection is within their self-interest.²⁶⁰ Even if individuals do not make the best decision, by emphasizing consent and recognizing individuals as autonomous beings, this theory generates trust.²⁶¹

Despite the advantages of this regime, various methods to update the notice-and-choice framework have been proposed. In the EU, the GDPR established an “opt-in” regime.²⁶² The GDPR prohibits an entity from processing data concerning health without the data subject’s consent.²⁶³ The GDPR allows data subjects to withdraw their consent at any time.²⁶⁴ In cases where a data subject withdraws consent, the GDPR requires the controller to erase all of their personal data.²⁶⁵ By forming an “opt-in” regime, the GDPR requires data subjects to affirmatively decide whether to permit the requested data use.²⁶⁶

Alternatively, one professor recommends keeping consent as a standard but redefining it as a continuum, ranging from full consent to nonconsent.²⁶⁷ On this continuum, an in-between consent, or “murky consent,”²⁶⁸ that gives data controllers a limited and weak license to use the data, would govern.²⁶⁹ Murky consent should only authorize limited activities, rather than authorizing extensive data collection and use.²⁷⁰

Critics argue that the key assumption underlying a notice-and-choice regime is false. Requiring consent may not be an adequate procedural safeguard when a consumer needs to consent to participate in everyday life, such as communicating over Facebook or using EHRs, resulting in consent fatigue.²⁷¹

260. *Id.*

261. *Id.* at 604.

262. Winograd, *supra* note 252, at 633.

263. Regulation 2016/679 of Apr. 27, 2016, art. 9, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1; *see also* Parker et al., *supra* note 63, at 722. If the entity does not have the data subject’s consent, another lawful basis must exist. Regulation 2016/679 of Apr. 27, 2016, art. 6, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1. For example, an entity may process personal data without the data subject’s consent if it is in the public interest for public health or if it is necessary to protect the data subject’s interests. *Id.* art. 9.

264. *Id.* art. 7. However, the right to compel an erasure of personal data may be derogated if exercising the right seriously impairs or renders impossible the objective for which the data is sought. *See* Parker et al., *supra* note 63, at 722.

265. Regulation 2016/679 of Apr. 27, 2016, art. 17, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

266. *See* Winograd, *supra* note 252, at 633.

267. *See* Solove, *supra* note 31, at 631.

268. *Id.*

269. *See id.*

270. *See id.*

271. *See id.*

In addition to privacy problems, requiring consent can worsen AI.²⁷² Because AI developers require a large volume of data to train the system and AI systems need a large volume of data to identify subtle patterns, consent requirements may limit the amount of data the developers can access.²⁷³ Furthermore, requiring consent may result in biased datasets because the types of individuals who consent may be different than those who do not.²⁷⁴ The opponents note that continuing to promote and update the notice-and-choice regime fails to protect the data while potentially creating datasets that are less useful for AI.

C. Professionalize AI Developers

Some scholars propose professionalizing AI developers through licensure or by imposing a duty of care. Underlying this proposal is the belief that AI developers are similar to doctors or lawyers because they possess knowledge that is unknown to the general public.²⁷⁵ Because external regulators do not have the specialized expertise to oversee these type of professionals, they rely on self-regulation.²⁷⁶ A system of self-regulation indicates that society trusts professionals to regulate other professionals in their community.²⁷⁷ This section details proposals to professionalize AI developers.

1. Create a System of Self-Regulation Similar to Other Professions

A key part of self-regulation is licensure.²⁷⁸ In the medical field, licensing became an important part of self-regulation in the 1850s.²⁷⁹ At that time, society delegated regulatory power to the physicians, which led to the profession establishing standards of education and training necessary for practice.²⁸⁰ Licensure ensured compliance with these standards.²⁸¹

272. See Ford & Price, *supra* note 16, at 39.

273. See *id.*

274. See *id.* at 36 n.109; Ruifeng Song, *Waiving the Consent Requirement to Mitigate Bias in Observational Precision Medicine Research*, INT'L J. EQUITY HEALTH, July 18, 2024, at 1, <https://doi.org/10.1186/s12939-024-02221-4> [<https://perma.cc/SA5C-RZXY>] (“Consent bias is a type of selection bias in biomedical research where those consenting to the research differ systematically from those not consenting.”).

275. Roger Collier, *Professionalism: The Privilege and Burden of Self-Regulation*, 184 CANADIAN MED. ASS'N J. 1559, 1559 (2012).

276. *Id.*

277. See Sylvia R. Cruess & Richard L. Cruess, *The Medical Profession and Self-Regulation: A Current Challenge*, AMA J. ETHICS, Apr. 2005, <https://journalofethics.ama-assn.org/article/medical-profession-and-self-regulation-current-challenge/2005-04> [<https://perma.cc/XG2C-8VS9>].

278. *Id.*

279. *Id.*

280. *Id.*

281. *Id.*

To become licensed, a person must pass an exam that demonstrates they have the knowledge required to work in that field.²⁸² In healthcare, medical practitioners must be licensed to practice medicine, which includes prescribing and administering drugs, diagnosing a disease, treating a condition, or issuing a medical opinion.²⁸³ If a medical practitioner does not abide by the standards governing their job, they risk losing their license and ability to practice.²⁸⁴

Today, many professions, including social workers and nurses, require a license to operate.²⁸⁵ Licensure regulates intimate relationships that may be imbalanced because of the informational asymmetry between the parties, vulnerability, and the public's inability to determine whether the professional is qualified.²⁸⁶

Professor Chinmayi Sharma draws comparisons between AI developers and other licensed professions.²⁸⁷ Specifically, "practicing" AI, or developing an AI model, requires substantial expertise unknown to the general public.²⁸⁸ Because non-AI developers do not know how to create training standards for AI developers, a system of licensing could provide a formal oversight role.²⁸⁹ Licensing standards for AI Developers could include education requirements or tests to certify knowledge.²⁹⁰ If an AI developer does not follow those standards, they risk losing their license and their ability to practice.²⁹¹ Given these high stakes, AI developers are incentivized to follow the standards.²⁹²

In addition to ensuring that AI developers possess certain skills, self-regulation can create certain codes of conduct.²⁹³ Self-regulation could offer a directive to the developers: do no harm.²⁹⁴ Additionally, because licensed developers would be accountable for their work, they will think critically about the training data they use and the safety audits they employ.²⁹⁵

282. See HEALTH PROFESSIONS EDUCATION: A BRIDGE TO QUALITY 104 (Ann C. Greiner & Elisa Knebel eds., 2003). Licensure is implemented at the state level, so standards vary across states. *Id.*

283. Terry, *supra* note 30, at 154.

284. See Chinmayi Sharma, *Setting a Higher Bar: Professionalizing AI Engineering*, LAWFARE (Dec. 12, 2023), <https://www.lawfaremedia.org/article/setting-a-higher-bar-professionalizing-ai-engineering> [<https://perma.cc/6K7U-TCQE>].

285. Elka Torpey, *Will I Need a License or Certification for My Job?*, U.S. BUREAU OF LAB. STAT.: PUBL'NS (Sep. 2016), <https://www.bls.gov/careeroutlook/2016/article/will-i-need-a-license-or-certification.htm> [<https://perma.cc/HH4P-T6GA>].

286. Terry, *supra* note 30, at 138.

287. Sharma, *supra* note 284.

288. *Id.*

289. *Id.*

290. *Id.*

291. *Id.*

292. *Id.*

293. *Id.*

294. *See id.*

295. *Id.*

Opponents of licensing argue that it does not protect data subjects' privacy interests. Some researchers argue that self-regulation can complement government regulations, but an independent third party is needed to oversee a system of self-regulation.²⁹⁶ They believe that governmental bodies are better positioned to ensure that AI developers are accountable to their data subjects.²⁹⁷ This accountability allows the independent regulators to advocate for patients' privacy interests.²⁹⁸

Other critics express concerns with expanding licensure requirements in general.²⁹⁹ Licensure systems can restrict the supply of labor, reduce competition, and increase the cost of services.³⁰⁰ This could have detrimental impacts on the development of healthcare AI given the scarcity of AI developers.³⁰¹

2. Impose a Legal Duty on AI Developers

Another proposed method of professionalizing AI developers is to impose a legal duty on them. Some states have already implemented this approach. Colorado passed the Colorado Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems³⁰² (the "Colorado AI Act") to protect consumers in interactions with AI systems.³⁰³ The Colorado AI Act imposes a duty of reasonable care on developers of high-risk AI systems to protect consumers from risks of algorithmic discrimination.³⁰⁴ Additionally, the developer must make information about the purpose and use of the system, summaries of the training data, and limitations or risks of the system available to the deployers of the model.³⁰⁵ However, the law does not directly address privacy.

296. McCoy et al., *supra* note 185.

297. See Ford & Price, *supra* note 16, at 36.

298. See *id.*

299. Gabe Scheffler, *Is the US Over-Licensed?: The Case for Reforming America's Professional Licensing Laws*, YALE UNIV. INST. FOR SOC. & POL'Y STUD., <https://isps.yale.edu/news/blog/2013/11/is-the-us-%E2%80%9Cover-licensed%E2%80%9D-the-case-for-reforming-america%E2%80%99s-professional-licensing> [https://perma.cc/U28S-TXHW] (last visited June 1, 2025).

300. *Id.*

301. Jennifer Riggins, *Tech Works: How to Fill the 27 Million AI Engineer Gap*, THENEWSTACK (Aug. 18, 2023, 05:00 ET), <https://thenewstack.io/tech-works-how-to-fill-the-27-million-ai-engineer-gap/> [https://perma.cc/MAR5-7VHP].

302. Colorado AI Act, S.B. 24-205, 2024 Gen. Assemb. § 1 (Colo. 2024).

303. See *id.*

304. *Id.* Under this Act, a high-risk AI system is an AI system that makes or is a substantial factor in making consequential decisions. *Id.* A consequential decision includes decisions that have a material effect on healthcare services. *Id.* The Colorado AI Act also imposes a duty of reasonable care on deployers, but that is beyond the scope of this Note. See *id.*

305. See *id.*; Cecilia Kang, *California Governor Vetoes Sweeping A.I. Legislation*, N.Y. TIMES (Sep. 29, 2024), <https://www.nytimes.com/2024/09/29/technology/california-ai-bill.html> (on file with the *Fordham Law Review*).

Similarly, California proposed a bill requiring AI developers to implement reasonable cybersecurity protections to prevent misuse of AI systems.³⁰⁶ The legislation forces developers to take reasonable care to implement safety measures and prevent the system from causing or materially enabling critical harm.³⁰⁷ To determine if a developer exercised reasonable care, the bill considers the quality of the safety and security protocols; how the developer implemented the protocols; and the developer's identification, evaluation, and management of risks posed by the AI system.³⁰⁸ The bill authorizes the attorney general of California to bring a civil action for violations.³⁰⁹

In the EU, the GDPR also imposes legal obligations on the controllers and processors to ensure privacy.³¹⁰ The GDPR requires entities to be accountable to those with whom they interact.³¹¹ Organizations maintain accountability by establishing technical and organizational measures that secure personal information.³¹²

Scholars have also attempted to draft legal obligations that could protect privacy. Dr. Julie E. Mehan suggested that AI developers consider data subjects' privacy and trust at the start of product development and throughout the development cycle.³¹³ She also suggested that developers communicate with subjects in plain and honest terms to show respect.³¹⁴ Other scholars recommended that AI developers need to prioritize trust, equity, and inclusion in the development process.³¹⁵

Professor Solove proposes a traditional legal duty where all organizations that collect and process personal data have a fiduciary relationship with the data subjects.³¹⁶ As aforementioned, fiduciary duties arise out of relationships of confidence and trust.³¹⁷ The fiduciary has a duty of loyalty to the other party and must protect the party's interests.³¹⁸ Professor Solove believes that fiduciaries protect the interests of the data subjects because the fiduciary must act in the party's interest and remain loyal.³¹⁹

306. Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, S.B. 1047, 2023–2024 Cal. Legislature, Reg. Sess. § 3 (Cal. 2024) (vetoed 2024).

307. *Id.*

308. *Id.*

309. *Id.*

310. Regulation 2016/679 of Apr. 27, 2016, art. 24–43, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

311. *See id.* art. 5.

312. *See id.*

313. MEHAN, *supra* note 134, at 243.

314. *Id.*

315. *See, e.g.,* NAT'L ACAD. OF MED., *supra* note 138, at 22.

316. *See* Solove, *supra* note 31, at 634.

317. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1207 (2016).

318. *Id.* at 1207–08.

319. *See* Solove, *supra* note 31, at 634.

III. PROTECTING PRIVACY WHILE PROMOTING HEALTHCARE AI

The use of AI in healthcare presents a unique challenge for privacy: to be most effective, AI needs to review large amounts of data. However, reviewing large amounts of data increases privacy risks. Because companies are already developing this technology, the concern is immediate and imperative.³²⁰ To address this challenge, this part argues that courts should impose a fiduciary duty on AI developers who handle sensitive health information.

A fiduciary duty can be created by statute or imposed by courts when the nature of the relationship justifies such a legal obligation. Typically, such a relationship develops when the entity has control over the party's affairs and the party must rely on the fiduciary.³²¹ When the court recognizes this relationship, they require the fiduciary to avoid self-dealing and conflicts of interest and maintain the highest duty of loyalty to the party.³²²

Part III.A discusses how imposing a fiduciary duty will require AI developers to protect health information while still allowing them to access the information needed to develop effective healthcare AI. Then, Part III.B compares this proposal to other suggested solutions and illustrates how a fiduciary duty can complement other solutions.

A. Courts Should Impose a Fiduciary Duty to Protect Health Information Without Impeding Healthcare AI

To balance privacy with progress, an effective solution will keep AI developers accountable while allowing them to access data needed to develop healthcare AI systems. Imposing a fiduciary duty balances these two aims.

AI developers with access to sensitive health information stand in a relationship of confidence and trust with the data subject. By creating new health information, AI developers have power over data subjects' affairs.³²³ Thus, the AI developers already have a fiduciary-like relationship with data subjects. The only difference is that, as the relationship is not currently legally recognized as a fiduciary one, AI developers are not subject to the associated legal obligations.

If a court imposes a fiduciary duty on healthcare AI developers, they will be forced to act for the benefit of the data subjects when working with their private health information.³²⁴ Privacy is a key part of this responsibility because fiduciary relationships are grounded in notions of confidentiality.³²⁵

320. *See supra* notes 19–22.

321. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 16 (A.L.I. 2020).

322. *Id.*

323. *See supra* note 128 and accompanying text.

324. *See supra* Part I.A.

325. *See supra* Part I.A.

Part III.A.1 explains how imposing a fiduciary duty on AI developers who handle health information adequately protects patient privacy. Part III.A.2 then explains how imposing a fiduciary duty still allows AI developers to access the health information they need.

1. A Fiduciary Duty Requires
AI Developers to Protect
Health Information

Current privacy laws and regulations do not require AI developers to protect privacy. First, HIPAA's primary standard for protection is de-identification, which is insufficient when AI can easily reidentify that information.³²⁶ Second, HIPAA only applies to certain health information, and therefore, various types of sensitive data are left unprotected.³²⁷ Third, companies create privacy policies. However, these policies are not designed to be protective, but rather to shield the company from legal liability and make data subjects aware of how companies use their data.³²⁸ Finally, individuals are often unable to bring lawsuits against data controllers because they do not have a cause of action or cannot meet the elements of the privacy torts. A fiduciary duty confronts all these issues.

Imposing a fiduciary duty addresses the current healthcare privacy challenges. First, a fiduciary duty can solve the issue with de-identification. AI developers understand that de-identification does not fully anonymize data.³²⁹ If held to the highest degree of loyalty to the data subjects, developers cannot argue that de-identification alone is enough to safeguard that information. Likewise, as fiduciaries, AI developers would treat all health-related information—like information from medical apps, social media, and purchase habits—as protected health information. As fiduciaries, AI developers would not differentiate between different types of data and would treat all health information with care, regardless of where the developers accessed the data.

Second, a fiduciary duty can also lead to privacy policies that protect data subjects. Current privacy policies are designed to shield a company from litigation and provide notice,³³⁰ but imposing a fiduciary duty would require developers to implement privacy safeguards designed to protect data subjects' information.³³¹

Finally, by imposing a fiduciary duty, courts create a private right of action for data subjects. When an individual believes the AI developer breached their fiduciary duty, they can bring a lawsuit against the fiduciary. Because of this, individuals do not need to rely on the FTC or other under-resourced

326. *See supra* Part I.A.1.b.

327. *See supra* Part I.A.1.b.

328. *See supra* Part I.A.2.a.

329. *See supra* Part I.A.

330. *See supra* note 85.

331. *See supra* note 127.

agencies to hold the AI developers accountable, and the victims can seek recourse when their most private data is breached.³³²

2. A Fiduciary Duty Allows AI Developers to Access High-Quality, Diverse Data

AI machines constantly need high-quality and diverse data,³³³ but existing privacy regulations present challenges to obtaining this information. Imposing a fiduciary duty would allow developers to share information with health providers and would not create roadblocks to accessing information.

Currently, AI developers either lack access to HIPAA-protected information or have access to non-HIPAA-covered data, which is subject to very few regulations.³³⁴ AI developers need access to a lot of health information, and identifying information may be necessary to create unbiased and accurate AI models. Imposing a fiduciary duty does not restrict what type of information AI developers can access. Instead, AI developers must take steps to protect that information. For example, developers can still access data from social media, medical apps, Grok, and other “unregulated” health data sources while keeping the necessary identifiers to build an effective and unbiased AI tool. But once the AI developers have that information, a fiduciary duty is triggered, requiring them to safeguard that information.

Likewise, imposing a fiduciary duty would not limit the ability of AI developers to share datasets if doing so is in the client’s best interest. Sharing data is critical to the success of healthcare AI because the public may need to view training data to trust the machine.³³⁵ Similarly, a clinician may want to review training data to ensure a dataset is representative of the clinician’s patient population. The advances in healthcare AI can only reach their full potential if doctors and the public trust these judgments.³³⁶ Imposing a fiduciary duty allows AI developers to build that trust.

B. Other Solutions Fall Short

The question of how to balance privacy with progress in the context of healthcare AI requires a solution that can be implemented quickly. The other proposed solutions in Part II fall short because they fail to protect data, do not support the development of healthcare AI, or cannot be implemented immediately.³³⁷

Accordingly, Part III.B.1 argues that proposals to update the regulatory scheme are impractical. Part III.B.2 explains that consent does not

332. *See supra* Part I.B.2.b; *see also supra* note 197 and accompanying text.

333. *See supra* Part I.B.1.

334. *See supra* Part I.A.1.a.

335. Grant, *supra* note 175.

336. *See supra* notes 240–48.

337. *See supra* Part II.

adequately protect privacy. Finally, Part III.B.3 concludes that a fiduciary duty can complement other proposals.

1. Proposals to Update the Regulatory
Scheme Are Ineffective,
Limited, or Untimely

In the short term, agencies cannot protect privacy in healthcare because Congress cannot create an agency, nor issue regulations, fast enough to provide adequate protections.³³⁸ Furthermore, federal legislators and executives are unlikely to strengthen the regulatory system in the next few years. The administration of President Donald J. Trump is attempting to increase government efficiency by reducing the federal workforce, cutting budgets, and limiting the overall number of regulations.³³⁹ Because of the administration's priorities, Congress is unlikely to create a new agency, and existing agencies are unlikely to receive the resources needed to regulate healthcare AI. Proposals to update the standard for de-identification or create new regulations may slow the development of healthcare AI. AI machines work better with more information; thus, requiring developers to use de-identified information may result in the model not having the data necessary to provide subtle insights about health or prevent bias.³⁴⁰

Additionally, any updates to HIPAA or new rules may become outdated quickly. Healthcare AI is a new and rapidly developing field, and any specific technical laws risk becoming outdated like HIPAA.³⁴¹ Even before AI, HIPAA did not anticipate the development of health apps and assumed that de-identification sufficiently protected privacy.³⁴² Similar attempts to create specific regulations to govern healthcare AI risk becoming outdated given the expediency of technological developments in this field.

A fiduciary duty addresses these privacy and progress concerns. A duty of loyalty and confidentiality would require AI developers to update outdated security protocols, forcing them to protect individual health information. Additionally, because a court can impose a fiduciary duty, this solution does not demand the time and resources that agency creation or regulation development would require. Finally, because a fiduciary duty does not perpetuate de-identification standards, AI developers can continue to access the detailed and diverse information as necessary.

338. See *supra* notes 193–96 and accompanying text.

339. See *supra* note 197.

340. See *supra* Part I.B.1.

341. See *supra* notes 52–57 and accompanying text (explaining that HIPAA does not apply to health posts on social media, mobile medical apps, or purchases that reveal information about a person's health); see also Timothy T. Hsieh, *A Bridge Between Copyright and Patent Law: Towards a Modern Day Reapplication of the Semiconductor Chip Protection Act*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 729, 734 (2018) (noting that intellectual property legislation designed to regulate computer chip designs became outdated because the technology evolved too quickly).

342. See *supra* note 8.

2. Informed Consent Falls Short

Consent does not adequately protect privacy. Because requests for consent are often unclear or difficult to comprehend, many individuals do not understand to what they are consenting.³⁴³ Once an AI developer receives consent from the data subject, the developer can use the data freely.³⁴⁴ Thus, an AI developer can use sensitive health information without sufficiently safeguarding that information. And there is no easy fix for this issue. Although other frameworks, such as “murky consent,” could limit the scope of the consent required,³⁴⁵ AI developers are still permitted to act without restriction once they receive the consent. Consent frameworks also fail to inform individuals on what they are consenting to, and, therefore, the consent is misguided.

Finally, even if the consent-based approach was effective, there is a difference between the population of those willing to consent to data collection and those who are not.³⁴⁶ This creates a biased dataset, which leads to a biased AI tool. Overall, requiring consent can give consumers a false sense of security and still perpetuates bias.³⁴⁷

3. How a Fiduciary Duty Can Complement Other Approaches

This Note does not oppose the creation of a regulatory agency to oversee AI developers or the enactment of specific technical solutions by legislators. Instead, it suggests that Congress is unlikely to implement these solutions in the short term, and because healthcare AI is rapidly developing, there must be a solution *now*. In the future, if legislators decide to pursue a regulatory approach, this can coexist with the fiduciary duty because the independent regulator would issue standards to apply across the industry and conduct reviews of AI developers. The independent regulator could review the standards the fiduciaries created and incorporate those expectations into new regulations. Some researchers argue that a system of self-regulation can complement government regulations by ensuring that AI developers follow certain standards even when the government does not have the resources or authority to investigate every developer.³⁴⁸

Similarly, regulators can work toward licensing AI developers. In some jurisdictions, healthcare providers are fiduciaries and still need a license to practice. Licensure adds another layer of oversight by requiring AI developers to pass an exam to practice and by revoking their ability to practice if they do not comply with the profession’s standards.³⁴⁹ These

343. See *supra* note 90 and accompanying text.

344. See WALDMAN, *supra* note 253.

345. See Solove, *supra* note 31, at 631.

346. See *supra* note 274 and accompanying text.

347. See *supra* notes 272–74.

348. See McCoy et al., *supra* note 185, at 8–9.

349. See HEALTH PROFESSIONS EDUCATION: A BRIDGE TO QUALITY, *supra* note 282.

solutions can eventually strengthen the system of self-regulation established by a fiduciary duty; but a fiduciary duty should be implemented now to ensure that AI developers protect health information.

CONCLUSION

The challenge of protecting data subjects' health information while fostering AI development is an urgent concern. Since Congress enacted HIPAA, technical advancements have chipped away at the security and protection HIPAA offers. Specifically, healthcare AI creates new privacy challenges while simultaneously creating new opportunities for improving the healthcare system.

To strike a balance between privacy and innovation, this Note advocates for courts to impose a fiduciary duty on healthcare AI developers. A fiduciary duty recognizes a relationship of confidence and trust to ensure that the fiduciary prioritizes the client's best interests. Without access to detailed health information, healthcare AI cannot make substantial advancements. However, access to large datasets creates significant privacy risks. This Note asserts that imposing a fiduciary duty enhances healthcare AI and protects individual privacy.