PATIENT RECORDS TO CLIENT FILES: HOW THE LEGAL PROFESSION'S CONFIDENTIALITY STANDARDS CAN INFORM HEALTHCARE CORPORATIONS' APPROACH TO ARTIFICIAL INTELLIGENCE TO MINIMIZE HIPAA VIOLATIONS

Parker Brown[*]

INTRODUCTION

Imagine: a local primary care clinic launches an artificial intelligence-powered ("A.I.") chatbot to manage appointment scheduling and patient inquiries. A few days later, John, feeling unwell, uses the chatbot to book an appointment with his physician. Yet, in its effort to "learn" from user interactions, the

[*] J.D. Candidate, Class of 2027, University of Mississippi School of Law.

chatbot transmits John's appointment details and symptom descriptions to a third-party analytics provider without his knowledge or consent.

Across town, Jane, recently diagnosed with a cardiovascular disorder, is admitted to the local hospital for observation. To enhance patient care, the hospital integrates a machine learning model into its system, enabling the creation of individualized treatment plans and predictions on patient outcomes. Seeking to advance research, the hospital shares what it believes to be de-identified patient data, including Jane's, with an external A.I. vendor. Unbeknownst to both Jane and the hospital, the vendor's software can cross-reference datasets to re-identify patients. Jane's supposedly anonymized health information is now personally identifiable once again.

Meanwhile, down the road, Alex, an elderly individual with memory loss, is seeking admission to a small, long-term care facility that recently adopted A.I. software to automate the review of Medicare and Medicaid forms during patient intake, aiming to reduce human error and processing delays. However, a breach in the facility's cloud-based system exposed current and potential residents' (including Alex's) medical histories, insurance details, and financial information to unauthorized actors.

Faced with these incidents, the healthcare organizations consulted a local law firm to assess their compliance risks and develop strategies for safely integrating A.I. into patient care and administration. At the firm, attorneys implemented an A.I.-assisted review system to analyze the workflows of the healthcare organizations, conduct legal research, assist in drafting internal memoranda and breach notifications for patients whose data had been leaked, and determine whether there were potential violations of the Health Insurance Portability and Accountability Act ("HIPAA"). At the firm, all data from the healthcare organizations was encrypted, access was strictly limited, and protocols were established to ensure that the A.I. system's outputs did not inadvertently disclose confidential information. The firm's approach, which prioritized confidentiality, enabled it to quickly respond to the healthcare organizations' inquiries and establish an action plan to minimize HIPAA violations.

Taken together, the clinic, hospital, and nursing home reflect the increasingly complex intersection of technological innovation and privacy regulation in modern healthcare. As A.I. becomes increasingly embedded in both clinical and administrative operations, the risk of inadvertent disclosure of sensitive information grows exponentially. As A.I. continues to reshape the healthcare landscape, can HIPAA's existing safeguards truly protect patients' privacy in an A.I.-driven world?

HIPAA is the central federal statute governing the privacy of individuals' health information.[1] Yet since its enactment in 1996, HIPAA has struggled to keep pace with the realities of the twenty-first century, particularly the rapid development of digital technologies. In recent years, A.I. has evolved from novelty to necessity, becoming an integral part of both personal life and professional practice. Its integration into healthcare promises efficiency and innovation but simultaneously exposes cracks in HIPAA's regulatory framework.[2] Most notably, HIPAA continues to rely on de-identification standards and limited oversight of third-party vendors as the primary safeguards for patient privacy, mechanisms that appear increasingly inadequate in the age of machine learning and big data analytics.[3]

---

[1] 42 U.S.C. § 1320; *see also HIPAA Basics*, HEALTHIT.GOV (Apr. 1, 2026), https://www.healthit.gov/topic/privacy-security-and-hipaa/hipaa-basics [https://perma.cc/NT6G-UCVY] ("The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the main Federal law that protects health information. The HIPAA Privacy and Security Rules protect the privacy and security of individually identifiable health information. HIPAA Rules have detailed requirements regarding both privacy and security."). *See generally* Wilnellys Moore & Sarah Frye, *Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules*, 47 J. NUCLEAR MED. TECH. 269, 269-72 (2019) (providing a general overview of the history, implementation, and legal components of HIPAA).

[2] *See* Todd Mayover, *When AI Technology and HIPPA Collide*, HIPAA J. (May 2, 2025), https://www.hipaajournal.com/when-ai-technology-and-hipaa-collide/ [https://perma.cc/E3BS-VM3T] ("[A.I. vendors] claim that by using A.I. technology, they can provide their deliverables in less time, generate useful insights more rapidly . . . . However, lurking surreptitiously behind the potential benefits of using [protected health information] in A.I. technology lies a murky mix of [HIPAA] risks . . . .").

[3] *See* Jayanth Kancherla, Re-Identification of Health Data Through Machine Learning (Nov. 30, 2020) (MS, Georgia Institute of Technology) (SSRN) ("However, HIPAA is outdated when it comes to addressing the use of machine learning for health data, because the technology is developing faster than regulatory bodies can impose new standards and rules. De-identification methods provided within HIPAA are not strong enough to prevent re-identification in machine learning.").

By contrast, the legal profession has long imposed a sweeping duty of confidentiality on attorneys, which encompasses virtually all client-related information, regardless of whether it is technically identifiable.[4] This duty has proven adaptable as lawyers and firms across the country adopt emerging digital technologies, including A.I.-driven research and case management tools.[5] Unlike HIPAA's narrow and static rules, the legal profession's confidentiality obligation reflects a broader commitment; trust demands protection of information in any form, even when the law's minimum requirements are silent.

As A.I. erodes the assumptions underlying HIPAA, healthcare corporations must decide whether to continue relying on outdated de-identification standards or adopt stronger safeguards modeled on the legal profession's approach to confidentiality. The comparison reveals that a broader, more flexible duty of confidentiality is essential if healthcare is to maintain patient trust and minimize the growing risks of data breaches, the sale of personal health information to third-party vendors, and re-identification in the A.I. era.

This Comment examines the growing challenges healthcare corporations face in integrating A.I. technologies into their operations while minimizing the risk of HIPAA violations. To offer meaningful insight, this Comment will draw a parallel between the healthcare and legal professions, both of which prioritize confidentiality and ethical responsibility. First, a general overview of HIPAA's privacy framework, the legal profession's confidentiality standards, and the rapid advancement and implementation of A.I. within both professions will be provided. Next, two emerging issues arising from the use of A.I. in healthcare—re-identification of confidential information and informed consent—will be analyzed with a comparison of how these concerns manifest in the legal profession. Finally, this

---

[4] *See generally* Daniel R. Fischel, *Lawyers and Confidentiality*, 65 U. CHI. L. REV. 1 (1998) (discussing the history and importance of confidentiality in the legal profession and its broad overreach to protect all client-related information).

[5] *See generally* Ian Rodgers, John Armour & Mari Sako, *How Technology Is (or Is Not) Transforming Law Firms*, 19 ANN. REV. L. SOC. SCI. 299 (2023) (explaining that technological change is transforming lawyers' work, career structures, and business models, while also highlighting the adaptability of the duty of confidentiality in modern digital legal practice).

Comment will conclude by proposing two solutions: amending HIPAA to better address A.I.-related risks and establishing a private right of action to strengthen enforcement and accountability.

I. BACKGROUND

A. HIPAA

"In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[6]

HIPAA safeguards what it defines as "protected health information" ("PHI"), which includes any health-related data that can be linked to the individual.[7] Importantly, HIPAA applies only to PHI that is created, stored, maintained, or transmitted by a HIPAA-covered entity or its business associate.[8] A covered entity is an individual, organization, or agency that is either a health plan, healthcare provider, or healthcare clearinghouse.[9] In describing the categories of covered entities, the United States Department of Health and Human Services ("HHS") has explained that "health care providers" include doctors, nursing homes, pharmacies, chiropractors, and clinics; "health plans" include health insurance companies, government programs that pay for

---

[6] Kancherla, *supra* note 3, at 5. Although HIPAA was signed into law by President Bill Clinton in 1996, it was not fully implemented until 2003. *See* Moore & Frye, *supra* note 1, at 270.

[7] 45 C.F.R. § 160.103 (2025); *see also* CTR. FOR MEDICAID & MEDICARE SERVS., HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, & BREACH NOTIFICATION RULES (2025) (noting PHI includes anything with personal identifiers, past, present, or future mental health conditions, or payment methods for healthcare taken by the individual); *What Is Considered PHI Under HIPAA?*, HIPAA J., https://www.hipaajournal.com/considered-phi-hipaa/ [https://perma.cc/GXL3-X39N] (last visited Apr. 20, 2026) (defining individually identifiable health information as a "subset of health information . . . that identifies the individual or can be used to identify the individual"); Moore & Frye, *supra* note 1, at 270 (defining PHI to include any data that can identify an individual—such as medical records, payment history, demographic details, identifiers, and medical images in DICOM format—and explaining that such information must be protected under HIPAA).

[8] 42 U.S.C. §§ 1320(d)(2)-(4).

[9] 45 C.F.R. § 160.103 (2025).

healthcare, employer-sponsored health plans, and health maintenance organizations; and "health care clearinghouses" include "entities that process nonstandard health information received from another entity into a standard . . . electronic format or data content . . . or vice versa."[10] On the other hand, a business associate is an individual, organization, or agency that helps carry out the healthcare activities or functions "on behalf" of a covered entity.[11] For example, business associates that would be subjected to HIPAA compliance may include a certified public accountant firm whose accounting services to a healthcare provider involve access to protected health information, an independent medical transcriptionist that provides transcription services to a physician, a third-party administrator that assists a health plan with claims processing, or an attorney whose legal services to a health plan involve access to protected health information.[12] Importantly, PHI disclosed to a business associate may only be used to "help the covered entity carry out its health care functions [and] not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate."[13]

In 2003, HHS issued the *Standards for Privacy of Individually Identifiable Health Information*, commonly known as the Privacy Rule.[14] The Privacy Rule seeks to "assure that

---

[10] *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/5BNP-DCP9].

[11] *See Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVS. (May 19, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/83FN-69HJ] ("A 'business associate' is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.").

[12] *Id.*

[13] *Id.*

[14] *See generally Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 14, 2025), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/54DD-LMCL] (providing a history of HIPAA's Privacy Rule and an overview of its rules, regulations, and enforcement mechanisms). HIPAA's Privacy Rule was created after Congress recognized that existing federal and state privacy regulations were inconsistent and unclear, that electronic technology was rapidly expanding, and that health information needed to flow more efficiently among providers, pharmacies, billing entities, and administrative staff to ensure timely access to patient records. *See* Moore & Frye, *supra* note 1, at 270.

individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public health and well-being."[15] It requires that all covered entities maintain appropriate safeguards to protect the privacy of PHI, set limitations and conditions on the use and disclosure of PHI without an individual's authorization, and grant individuals several rights over their PHI.[16] These rights include the right to access and obtain copies of their records, request corrections, and direct a covered entity to transmit records to a designated third party.[17]

Along with the Privacy Rule, HHS adopted the Security Rule, which explicitly governs electronic PHI ("ePHI").[18] The Security Rule requires HIPAA-covered entities to establish and maintain appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.[19] Whereas the Privacy Rule applies broadly to all forms of PHI, the Security Rule focuses narrowly on electronic information—reflecting the growing digitization of health records.[20] In recent years, noncompliance with the Security Rule's risk analysis

---

[15] U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2003).

[16] U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 15; *see also* Moore & Frye, *supra* note 1, at 270-71 ("The privacy rule regulates the use and disclosure of PHI and sets the minimum national standards that every covered entity must follow to protect patients' private medical information.").

[17] U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 15. Under HIPAA, if an individual requests a copy of their health records, the healthcare provider must fulfill the request within thirty days. *See* Moore & Frye, *supra* note 1, at 271.

[18] *See* HEALTHIT.GOV, *supra* note 1.

[19] Barry A. Humphrey, Data Privacy vs. Innovation: A Quantitative Analysis of Artificial Intelligence in Healthcare and Its Impact on HIPAA Regarding the Privacy and Security of Protected Health Information (May 2021) (Ph.D thesis, Robert Morris University) (ProQuest).

[20] *Id*. The distinction between the Security Rule and Privacy Rule was further expressed following the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act). *See* Moore & Frye, *supra* note 1, at 271-72 (explaining that under HIPAA, "physical safeguards" govern physical access to PHI, including access to buildings, offices, secured areas, computers, and files; "technical safeguards" govern access controls for computer systems and the protection of electronically transmitted PHI, including who may access, view, and use electronic medical records; and "administrative safeguards" require facilities to create and update policies and procedures that employees must follow to ensure PHI security).

provision has become one of the most commonly identified HIPAA violations, as entities have failed to conduct HIPAA-compliant risk analyses, conducted them infrequently, or had risk assessments that were not comprehensive or inaccurate.[21]

HIPAA violations cases consist of compliance investigations resulting from data breaches that are reported to the Department of Health and Human Services' Office for Civil Rights ("OCR").[22] Consequences of HIPAA violations depend on a variety of factors, including the level of negligence, the number of people affected, the severity of the violation, the entity's financial position, and whether the entity has implemented recommended security practices.[23] When resolving potential HIPAA violations, the OCR has several options. First, the OCR can choose to take no action, allowing the HIPAA-regulated entity to resolve the issue independently, or if requested, provide technical support to assist the entity in making any required modifications.[24] But if the HIPAA-regulated entity fails to resolve the matter independently, the OCR has the authority to impose civil or criminal penalties.[25]

---

[21] *HIPAA Violation Cases: Types & Consequences*, HIPAA J. (2026), https://www.hipaajournal.com/hipaa-violation-cases/ [https://perma.cc/63R4-3MAG].

[22] *Who Enforces the Health Information Privacy and Security Standards Established Under the Health Insurance Portability and Accountability Act (HIPAA)?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Feb. 15, 2023), https://www.hhs.gov/hipaa/for-professionals/faq/2019/who-enforces-hipaa/index.html [https://perma.cc/9GVC-WPUB]; *see also* Nancy A. Lawson, Jennifer M. Orr & Doedy Sheehan Klar, *The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Regulations*, 70 DEF. COUNS. J. 127, 148 (2003). In enforcing HIPAA and guaranteeing compliance, the OCR will investigate filed complaints, conduct compliance reviews, and perform education and outreach. *See HIPAA Violations & Enforcement*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement [https://perma.cc/UD9X-AT89] (last visited Oct. 16, 2025). *See generally HIPAA Violation Examples in 2025: 20 Common Violations With Real-World Enforcement Cases*, SECUREFRAME (Aug. 18, 2025) https://secureframe.com/hub/hipaa/violations [https://perma.cc/579D-QQHM] (providing an in-depth overview and examples various HIPAA violations, the OCR's investigation process, and assessing civil and criminal penalties following a HIPAA violation).

[23] HIPAA J., *supra* note 21.

[24] *Id.* Other informal methods of remedying HIPAA violations include the HIPAA-regulated entity creating a corrective action plan ("CAP") with specific implementation strategies to ensure HIPAA compliance. To ensure compliance with their CAP, HIPAA requires the OCR to monitor the entity for a predetermined period of time, typically one to three years. *Id.*

[25] AM. MED. ASS'N, *supra* note 22.

The enforcement of civil penalties is structured in a tiered system,[26] with the Secretary of HHS having discretion over the final civil penalty amount.[27] If a complaint describes actions that violate a criminal provision of HIPAA,[28] the OCR has the authority to refer the complaint to the Department of Justice.[29] Similar to civil penalties, criminal penalties are structured in a tier system, with tiers separated by the severity of the violation and the offender's intent.[30] Unlike HIPAA, which provides for federal oversight and tiered civil and criminal penalties, confidentiality in the legal profession is not regulated by a single federal statute but is instead enforced through professional responsibility rules and imposed by state bar authorities.[31]

B. The Legal Profession

"Confidentiality is the bedrock principle of legal ethics . . . the duty is nearly absolute."[32] Because there is no federal law regulating or enforcing confidentiality in the legal profession, lawyers are bound by the ethics rules adopted by the state in which they practice.[33] Still, the American Bar Association ("ABA")

---

[26] The HIPAA civil penalty structure includes four tiers based on the violator's level of culpability: (1) *Unknowing* violations ($100-$50,000 per violation; up to $25,000 annually for repeat violations); (2) violations due to *reasonable cause* ($1,000-$50,000 per violation; up to $100,000 annually); (3) *Willful neglect violations corrected* within the required time ($10,000-$50,000 per violation; up to $250,000 annually); and (4) *Willful neglect violations not corrected* ($50,000 per violation; up to $1.5 million annually). *Id.*; *see also* HIPAA J., *supra* note 21.

[27] Factors the Secretary of HHS may consider when imposing a civil penalty include the nature, extent, and amount of harm caused by the violation. However, the Secretary is prohibited from imposing penalties if the violation is corrected within 30 days. *Id.*; *see also* HIPAA J., *supra* note 21.

[28] *See, e.g.*, 42 U.S.C. § 1320d-6.

[29] AM. MED. ASS'N, *supra* note 22.

[30] *Id.*; The tiered structure for HIPAA criminal penalties is as follows: (1) individuals who *knowingly* obtain or disclose protected health information may face fines up to $50,000 and up to one year in prison; (2) offenses committed *under false pretenses* carry fines up to $100,000 and up to five years imprisonment; and (3) offenses committed *for commercial advantage, personal gain, or malicious harm* are punishable by fines up to $250,000 and up to ten years imprisonment. *Id.*; *see also* 42 U.S.C. § 13200d-6(b).

[31] *See* Patricia Frapasella, *A Case for Confidentiality*, 8 J. PARALEGAL EDUC. & PRAC. 167, 172 (1991).

[32] Fischel, *supra* note 4, at 1.

[33] *See* Frapasella, *supra* note 31, at 172.

promulgated this obligation, requiring attorneys to preserve "information relating to the representation of a client" against unauthorized disclosure.[34] Importantly, this duty is not limited to identifiable or sensitive information but extends broadly to virtually all information connected to the representation.[35] In essence, the rule requires that an attorney "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[36] The foundational principle of confidentiality also gives rise to other critical aspects of the legal profession, including the attorney-client privilege, which shields communications between a lawyer and client made in confidence for the purpose of obtaining legal advice.[37]

Although confidentiality remains one of the cornerstones of the legal profession, the duty is "replete" with exceptions.[38] ABA Model Rule 1.6 provides several instances in which an attorney may reveal confidential information, including with the client's consent, to prevent a client from causing substantial bodily harm to themselves or others, to comply with court orders, or to defend the lawyer against allegations of malpractice.[39]

---

[34] *See* MODEL RULES OF PRO. CONDUCT r. 1.6(a), (c) (A.B.A. 2020).

[35] *Id.*; *see also* MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 3 (A.B.A. 2020) ("The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source.").

[36] MODEL RULES OF PRO. CONDUCT r. 1.6(c) (A.B.A. 2020).

[37] Attorney-client privilege is the evidentiary counterpart to an attorney's ethical duty of confidentiality and allows an attorney to resist compelled disclosure of client information, even if relevant. The privilege applies:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications *relating* to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal *adviser*, (8) except the [client waives the protection].

John Henry Wigmore, TREATISE ON THE ANGLO-AMERICAN SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW INCLUDING THE STATUTES AND JUDICIAL DECISIONS OF ALL JURISDICTIONS OF THE UNITED STATES AND CANADA § 2292, at 3204 (2d ed. 1923).

[38] Thomas J. Snyder, *Attorney-Client Confidentiality Is a Moral Good: Expanding Protections of Confidentiality and Limiting Exceptions*, 32 GEO. J. LEGAL ETHICS 411, 412 (2019).

[39] *See* MODEL RULES OF PRO. CONDUCT r. 1.6(b) (A.B.A. 2020).

Since its inception, American jurisprudence has long emphasized the uniqueness of confidentiality in the legal profession and the lawyer-client relationship from other professional relationships.[40] The emphasis on confidentiality in the legal profession is rooted in a practical matter: "to encourage full and frank communication between attorneys and their clients"[41] and to instill trust between the client and the attorney.[42] This emphasis on effectiveness and transparent communication is echoed in Comment 2 of ABA Model Rule 1.6:

---

[40] *See* Lindsay R. Goldstein, *A View from the Bench: Why Judges Fail to Protect Trust and Confidence in the Lawyer-Client Relationship – An Analysis and Proposal for Reform*, 73 FORDHAM L. REV. 2665, 2668 (2005); *see also In re* Dunn, 98 N.E. 914, 916 (N.Y. 1912) (noting "the relationship of attorney and client . . . is subject to principles and rules which do not apply to an ordinary contract").

[41] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

[42] *See* Frapasella, *supra* note 31, at 172:

> [T]he principle of confidentiality serves public policies important enough to warrant a basic rule of confidentiality that is unstintingly observed. Although there is no empirical evidence of the precise degree to which clients rely on the principle of confidentiality, it is intuitively obvious that lawyers will be better able to gain the trust of clients, to serve them, and to help them obey the law under a *requirement* of confidentiality that goes beyond mere tradition. Beyond this pragmatic and utilitarian concern, lawyers demonstrate the moral values of trust and loyalty when they say they will keep quiet and then do so, even when it would be more comfortable to speak out.

Id.; *see also* United States v. Costen, 38 F. 24, 24 (C.C.D. Colo. 1889). The court emphasized the importance of trust and confidence in the lawyer-client relationship as follows:

> Now, it is the glory of our profession that its fidelity to its client can be depended on; that a man may safely go to a lawyer and converse with him upon his rights . . . with the absolute assurance that the lawyer's tongue is tied from ever disclosing it; and any lawyer who proves false to such an obligation . . . is guilty of the grossest breach of trust. . . . I cannot tolerate for a moment, neither can the profession, neither can the community, any disloyalty on the part of a lawyer to his client.

Id.

> A fundamental principle in the client-lawyer relationship is . . . the lawyer must not reveal information relating to the representation. . . . This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer, even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct.[43]

Moreover, although not specifically grounded in a constitutional foundation, many legal scholars have argued that a lawyer's duty of confidentiality is rooted in the United States Constitution.[44] For example, the Sixth Amendment of the U.S. Constitution states: "In all criminal prosecutions, the accused shall enjoy the right . . . and have the assistance of counsel for his defense."[45] When interpreting the Sixth Amendment, courts, such as in *Strickland v. Washington*,[46] *McMann v. Richardson*,[47] and *United States v. De Coster*,[48] have held that the rights granted to criminal defendants include the right to competent and effective assistance of counsel. Legal scholars, including Abraham Abramovsky, note that the constitutional right to effective assistance of counsel directly implicates a constitutional right to confidentiality.[49] Abramovsky finds that "[t]o provide effective representation, an attorney must be fully informed of all relevant facts, including client indiscretions and crimes committed or contemplated by his client. Any restriction on this free exchange

---

[43] MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 2 (A.B.A. 2020).

[44] *See* Frapasella, *supra* note 31, at 173.

[45] U.S. CONST. amend. VI.

[46] 466 U.S. 668, 688 (1984) ("[The Sixth Amendment] relies instead on the legal profession's maintenance of standards sufficient to justify the law's presumption that counsel will fulfill the role in the adversary process that the Amendment envisions.").

[47] 397 U.S. 759, 771 (1970) ("[I]f the right to counsel guaranteed by the Constitution is to serve its purpose, defendants cannot be left to the mercies of incompetent counsel . . . .").

[48] 487 F.2d 1197, 1201 (D.C. Cir. 1973) ("The effective assistance of counsel is a defendant's most fundamental right 'for it affects his ability to assert any other right he may have.'").

[49] *See generally* Abraham Abramovsky, *A Case for Increased Confidentiality,* 13 FORDHAM URB. L.J. 11 (1985).

between client and attorney substantially interferes with both effective representation and the privilege of confidentiality."[50] Furthermore, Abramovsky asserts that the "free exchange" between clients and attorneys is necessary beyond criminal law and expands to all legal areas, making the privilege of confidentiality not only a constitutional right but also the "cornerstone of the American legal system" and an "essential feature of the American adversarial system of justice."[51]

A case that illustrates the legal profession's prioritization of confidentiality is the famous (or infamous) "Buried Bodies Case."[52] There, defense attorneys Armani and Belge were informed by their client, Garrow, that he had murdered several teenagers and disclosed the locations of the bodies of two of his victims.[53] The locations given by Garrow were so precise that Belge was able to locate the remains of the two victims and photograph the sites.[54] Although public outcry demanded that the two attorneys disclose the location of the victims, and although the attorneys received death threats, they refused to breach their duty of confidentiality.[55] The attorneys' refusal to disclose confidential information led to public shame, and Belge, who actually located the bodies, was indicted for failing to report a dead body and failing to provide it with a decent burial.[56] However, Belge's charges were dismissed at trial, where the judge not only dropped the charges but praised Belge's dedication to his ethical duty of confidentiality as an attorney.[57] A decade after the fallout of the trial, Armani remained adamant that his duty of confidentiality

---

[50] *Id.* at 11.

[51] *Id.* at 11, 42.

[52] *See* Lisa M. Stone, *Client Confidentiality: The Buried Bodies Case*, NALA (Aug. 2018), https://nala.org/client-confidentiality-buried-bodies-case/ [https://perma.cc/X53N-X4U7] (discussing the history of the "Buried Bodies Case" and its significance in the legal and public view of attorney-client confidentiality).

[53] Lisa G. Lerman et al., *The Buried Bodies Case: Alive and Well After Thirty Years,* 2007 PRO. LAW. SYMP. ISSUES 19, 19.

[54] Stone, *supra* note 52.

[55] Lerman et al., *supra* note 53; *see also* Stone, *supra* note 52. The day after Garrow confessed at trial that he committed the crimes, Armani and Belge publicly acknowledged that they knew the locations of the victims. *Id.*

[56] Stone, *supra* note 52.

[57] *See* People v. Belge, 372 N.Y.S.2d 798, 803 (1975) ("It is the decision of this Court that Francis R. Belge conducted himself as an officer of the Court with all the zeal at his command to protect the constitutional rights of his client.").

had to prevail, stating, "in my judgment, and I still feel that way, [the victim's parents'] suffering is not worth jeopardizing my sworn duty [of confidentiality] or my oath of office of the Constitution."[58]

Although a "quintessential element" of the attorney-client relationship, breaches of confidence still occur either knowingly or unknowingly.[59] Generally, there are four elements of breach of confidence: (1) "the information must be confidential,[60] (2) [the information] must have been disclosed,[61] (3) there must be a breach of confidence,[62] and (4) there must not be any defense [that] will excuse the breach."[63] If an attorney breaches confidentiality, various actions can be taken.[64] First, disciplinary proceedings can be conducted under rules set by a state's high court.[65] Depending on the severity of the violation, the attorney

---

[58] ETHICS ON TRIAL, University of Maryland Libraries: Digital Collections, at 9:11 (PBS 1987). Since the "Buried Bodies Case," it is believed that the incident was a contributing factor in the inclusion of the "death and substantial bodily injury" exception under Rule 1.6. *See* Stone, *supra* note 52.

[59] Goldstein, *supra* note 40, at 2668.

[60] Brad Markel, *Business Issues: Breach of Confidence,* 53 SASK. L. REV. 229, 230 (1989) (stating the four elements of a breach of confidence). When determining what is considered "confidential," the primary consideration is whether the information was accessible to the public. Frapasella, *supra* note 31, at 175.

[61] In determining if the information being disclosed was made in confidence, courts can use as a test "did the lawyer know that the information was disclosed for a limited purpose." For example, information that is blurted out publicly is found not to have been disclosed for a limited purpose. *Id.*

[62] "Any use, other than the purpose for which [the disclosed information] was intended," is considered a breach of confidence. *Id.*

[63] *See* Markel, *supra* note 60, at 230.

[64] Note, *Proving Breach of Former-Client Confidentiality*, 131 HARV. L. REV. 582, 587-88 (2017) (discussing various enforcement mechanisms following a breach of confidentiality, including disciplinary proceedings, disbarment, and private suits by their clients).

[65] David B. Wilkins, *Who Should Regulate Lawyers?*, 105 HARV. L. REV. 799, 805-06 (1992). Wilkins describes the disciplinary proceedings process as follows:

> [I]ndependent agencies acting under the supervision of state supreme courts investigate and prosecute violations of the rules of professional conduct. The basic structure resembles a criminal prosecution. . . . The process is conducted almost exclusively ex post by independent officials who have no prior association with the case. These officials are instructed to reach their judgments solely on the basis of the evidence presented at a formal hearing in

may be disqualified and disbarred.[66] Beyond professional discipline and disqualification, the client may file a private legal malpractice claim against the attorney and pursue damages in court.[67] As a breach of confidentiality is a violation of an attorney's due care, for a successful claim, the client would have to prove the elements of duty, breach, causation, and damages.[68] Although rooted in traditional modes of practice, the legal profession's confidentiality framework now faces challenges similar to those encountered in the healthcare sector as rapid advancements in A.I. introduce new and complex risks of inadvertent disclosure.

C. Artificial Intelligence

Just as A.I. itself continues to evolve rapidly, so too has its definition. Generally, A.I. can be defined as "the ability of a machine to perform cognitive functions that we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem solving, decision-making, and even demonstrating creativity."[69]

Two of the most prevalent types are machine learning ("ML") and generative artificial intelligence. ML models "focus on building systems capable of learning from data, identifying patterns, and making decisions with minimum human

---

> which the accused lawyer is accorded a full panoply of due process protections.

Id.

[66] Note, *supra* note 64, at 587-88 ("When an attorney has violated Rule 1.9, the court may disqualify the attorney from the subsequent matter.").

[67] *Id.* at 588; *see, e.g.*, *Maritrans GP Inc. v. Pepper, Hamiliton, & Scheetz*, 602 A.2d 1277, 1286 (Pa. 1992) ("Courts throughout the United States have not hesitated to impose civil sanctions upon attorneys who breach their fiduciary duties to their clients, which sanctions have been imposed separately and apart from professional discipline.").

[68] Note, *supra* note 64, at 588 ("A breach of confidentiality is a violation of an attorney's duty of care and requires proof as to every element: duty, breach, causation, and injury."); *see also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 48, 53 cmt. c (A.L.I. 2000) ("[Legal malpractice] require[s] that the plaintiff establish that the defendant owed a duty to the plaintiff and that there has been a breach of such a duty, typically by showing that the defendant has acted without reasonable care; comparable principles of proximate cause and measure of damages apply[.]").

[69] Niklas Kühl et al., *Artificial Intelligence and Machine Learning*, 32 ELEC. MKTS. 2235, 2237 (2022).

intervention."[70] The goal of ML models is to make a system "so intelligent that it can perform decision-making tasks itself."[71] There are two primary approaches to ML models: supervised and unsupervised learning.[72] In supervised learning, a model is trained using a dataset that includes both inputs and their correct outputs, or "labels."[73] During training, the model analyzes these examples to identify patterns and relationships between the inputs and outputs.[74] Once trained, it can apply what it has learned to predict outcomes for new, unseen data.[75]

In contrast, the goal of unsupervised machine learning models is to "have the computer learn how to do something that we don't tell it how to do."[76] Unlike supervised learning, where models learn from labeled examples, unsupervised models learn from unlabeled data. These systems identify hidden patterns, group similar data points, or detect anomalies independently.[77] In some cases, the model is guided by a reward system that provides feedback based on the success of its actions.[78] Over time, the model refines its decisions to maximize rewards and improve performance, effectively learning through trial and error.[79]

On the other hand, generative A.I. can "create original content such as text, images, [or] video . . . in response to a user's prompt . . . by identifying and encoding the patterns and relationships in huge amounts of data, and then using that

---

[70] Bernard Marr, *The Vital Difference Between Machine Learning and Generative AI*, FORBES (June 25, 2024, at 01:30 ET), https://www.forbes.com/sites/bernardmarr/2024/06/25/the-vital-difference-between-machine-learning-and-generative-ai/ [https://perma.cc/Z4KD-A9P9].

[71] Darpan Pandey, Kamal Niwaria & Bharti Chourasia, *Machine Learning Algorithms: A Review*, 6 INT'L RSCH. J. ENG'G & TECH. 916, 916 (2019).

[72] Junaid Bajwa et al., *Artificial Intelligence in Healthcare: Transforming the Practice of Medicine*, 8 FUTURE HEALTHC. J. 188, 189 (2021).

[73] Taiwo Oladipupo Ayodele, *Machine Learning Overview*, in NEW ADVANCES IN MACHINE LEARNING 4 (Yagang Zhang ed., 2010).

[74] *Id.*

[75] *Id.*

[76] Taiwo Oladipupo Ayodele, *Types of Machine Learning Algorithms*, in NEW ADVANCES IN MACHINE LEARNING 22 (Yagang Zhang ed., 2010).

[77] Bajwa et al., *supra* note 72, at 189 ("'Unsupervised learning' attempts to extract information from data without labels; for example, categorizing groups of patients with similar symptoms to identify a common cause.").

[78] Ayodele, *supra* note 76.

[79] *Id.*

information to understand users' natural language requests or questions and respond with relevant new content."[80] In using generative A.I., individuals provide prompts to engage with the system, which the A.I. interprets to generate a result that influences the person's responses and informs the system's responses to future prompts.[81] Unlike ML models, which are more guided toward a specific user-defined result, generative A.I. takes on the role of a co-creator, producing new and original content that contributes ideas and shapes the individual's final product.[82]

The advancement of generative A.I. will impact all aspects of everyday life, especially in the effectiveness and efficiency of work operations.[83] For example, generative A.I. models have begun to be incorporated into inter-organizational elements, such as work patterns and management practices, leading to this software being outsourced to complete managerial tasks, including event management, resource allocation, and social media account

---

[80] Cole Stryker & Mark Scapicchio, *What Is Generative AI?*, IBM (Mar. 22, 2024) https://www.ibm.com/think/topics/generative-ai [https://perma.cc/7TRT-E33R]; *see also* George Lawton, *What Is GenAI? Generative AI Explained*, TECHTARGET (Mar. 13, 2025), https://www.techtarget.com/searchenterpriseai/definition/generative-AI [https://perma.cc/LBR9-3RSK] (noting that generative A.I. "uses sophisticated algorithms to organize large, complex data sets into meaningful clusters of information in order to create new content, including text, images and audio, in response to a query or prompt").

[81] *See* Stefan Feuerriegel et al., *Generative AI*, 66 BUS. & INFO. SYS. ENG'G 111, 116 (2024).

[82] *Id.* ("AI can be suggestive to the other and will inform their further involvement directly or subconsciously. Thus, the process of creation rather follows a co-creation pattern, that is, the practice of collaborating in different roles to align and offer diverse insights to guide a design process."). *See generally* Venkat Ramaswamy & Kerimcan Ozcan, *What Is Co-Creation? An Interactional Creation Framework and Its Implications for Value Creation*, 84 J. BUS. RSCH. 196 (2018) (discussing the value of co-creation by machine learning technologies, how it is shaped by user interactions, and highlights how A.I. may enhance collaborative value creation between users and consumers).

[83] *See* Molly Kinder et al., *Generative AI, the American Worker, and the Future of Work*, BROOKINGS INST. (Oct. 10, 2024), https://www.brookings.edu/articles/generative-ai-the-american-worker-and-the-future-of-work/ [https://perma.cc/RR97-QW2C] ("Even on its current trajectory, without any dramatic acceleration of capability gains, generative A.I. technology is poised to impact a broad range of workers . . . . On one hand, generative A.I. has the potential to complement millions of workers' skills, enabling them to be more productive, creative, informed, efficient, and accurate. On the other hand, employers may choose to automate some, or even all, of their employees' work, leading to possible job losses and weakened demand for previously sought-after skills.").

management.[84] As generative A.I. continues to advance, the software will take on an increased workload and be utilized in other essential roles such as predicting new business models, projects, and initiatives based on consumer reports and data; creating, summarizing, and disseminating content; and even personalized services to individual employees based on their specific needs and preferences.[85]

Significantly, ML models and generative A.I. can only improve their predictive and decision-making abilities if they are provided with more data, as the accuracy of A.I. software remains highly dependent on the quality and quantity of training data.[86] For example, a common limitation of generative A.I. is the production of incorrect outputs, commonly referred to as "hallucinations."[87] Hallucinations refer to mistakes in A.I.-generated context that are plausible but incorrect, as the content produced is not based on facts or evidence, but rather the A.I. system's own bias and assumptions.[88] Ultimately, although hallucinations may not be a concern to the average individual, it remains "a serious issue for anyone using the technology with court documents, medical information[,] or sensitive business data.[89] Moreover, as A.I. software learns from the data provided, if the software is input with biased data, it can lead the software to "amplify human biases, replicate toxic language, or perpetuate

---

[84] Feuerriegel et al., *supra* note 81, at 120.

[85] *Id.*

[86] *See* Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model*, 21 HOU. J. HEALTH L. & POL'Y 125, 133 (2021). ("AI's success . . . is directly connected to the quality and volume of data used to train A.I. algorithms or improve its accuracy over time."); *see also* Feuerriegel et al., *supra* note 81, at 117 ("The correctness of generative AI models is highly dependent on the quality of training data and the according learning process.").

[87] *See* Feuerriegel et al., *supra* note 81, at 117. *See generally* Mahmut Özer, *Is Artificial Intelligence Hallucinating?*, 35 TURKISH J. PSYCHIATRY 333 (2024) (providing an in-depth overview of A.I. hallucinations, the various types of hallucinations, and their causes).

[88] *See* Feuerriegel et al., *supra* note 81, at 117; *see also* Özer, *supra* note 87 ("AI hallucination is a phenomenon where AI generates a convincing, contextually coherent but entirely fabricated response that is independent of the user's input or previous context.").

[89] Cade Metz & Karen Weise, *A.I. Is Getting More Powerful, But Its Hallucinations Are Getting Worse*, N.Y. TIMES (May 6, 2025), https://www.nytimes.com/2025/05/05/technology/ai-hallucinations-chatgpt-google.html [https://perma.cc/ZNV9-M53W].

stereotypes of gender, sexual orientation, political leaning, or religion."[90] Furthermore, A.I. systems cannot understand the meaning of their own generated text, which can lead them to combine accurate information in ways that yield false or inaccurate results.[91]

Healthcare systems have begun to embrace A.I. in pursuit of the "quadruple aim": improving population health, improving patients' experience, enhancing caregiver experience, and reducing the rising cost of care.[92] The integration of A.I. makes these objectives increasingly attainable.[93] For example, 81% of physicians reported that A.I. will improve care team interaction with patients, 59% reported that A.I. can save time by summarizing data about patients' electronic health records, and 97% reported that A.I. will improve overall interactions with patients.[94]

Regarding the integration of A.I. into healthcare, a 2024 survey found that 75% of leading healthcare companies are experimenting with or planning to scale generative A.I. across their enterprises, with nearly half of U.S. healthcare organizations already in initial production.[95] Currently, A.I.

---

[90] *See* Feuerriegel et al., *supra* note 81, at 117.

[91] *See, e.g.*, Karen Weise & Cade Metz, *When A.I. Chatbots Hallucinate*, N.Y. TIMES (May 9, 2023), https://www.nytimes.com/2023/05/01/business/ai-chatbots-hallucination.html [https://perma.cc/JT4F-Z5SD] ("And sometimes the chatbots make things up. They produce new text, combining billions of patterns in unexpected ways. This means even if they learned solely from text that is accurate, they may still generate something that is not. . . . [E]ven A.I. experts cannot understand why they generate a particular sequence of text at a given moment. And if you ask the same question twice, they can generate different text.").

[92] Bajwa et al., *supra* note 72, at 188.

[93] *See AI in Healthcare Statistics: 62 Findings from 18 Research Reports*, KERAGON (June 12, 2024), https://www.keragon.com/blog/ai-in-healthcare-statistics [https://perma.cc/7T5N-WCHU] ("From improving patient care to reducing administrative burdens, it appears that generative AI is starting to make a measurable impact."); *see also* Bajwa et al., *supra* note 72, at 190 ("AI can enable healthcare systems to achieve their 'quadruple aim' by democratising and standardising a future of connected and AI augmented care, precision diagnostics, precision therapeutics and, ultimately, precision medicine.").

[94] André Rebelo, *Wolters Kluwer Survey: Over Two-Thirds of U.S. Physicians Have Changed Their Mind, Now Viewing GenAI as Beneficial in Healthcare* (Apr. 16, 2024), https://www.wolterskluwer.com/en/news/gen-ai-clincian-survey-press-release [https://perma.cc/S5GA-DQ5X].

[95] *Id.*

models are most often deployed in clinical decision-making, administrative processes, and predictive analytics.[96] Yet, scholars predict that as models mature, they will be able to "combine disparate structured and unstructured data, including imaging, electronic health data, multi-omic, behavioral, and pharmacological data" without human oversight and less data ultimately reaching a state of precision that will shift healthcare "to a preventative, personalised, data-driven disease management model that achieves improved patient outcomes . . . in a more cost-effective delivery system."[97]

The legal profession, too, has begun integrating A.I. into daily operations; the most visible application to date is in legal research and writing.[98] A.I.-assisted platforms such as Lexis+, Westlaw's CoCounsel, and Casetext's CARA A.I. leverage natural language processing to deliver results more quickly and comprehensively than traditional search tools.[99] For example, when prompted, CoCounsel will conduct legal research by searching the Westlaw database, summarizing key points from sources, and concluding by writing a memo that provides the attorney with the answer to the prompt and the relevant supporting sources.[100] Furthermore, CoCounsel can review legal documents and prepare for a deposition.[101] To illustrate further, Casetext's CARA A.I. uses A.I. to search legal authorities, after being provided with relevant

---

[96] *See* Mayover, *supr*a note 2; *see also* Bajwa et al., *supra* note 72, at 190 (describing how A.I. is currently being used by healthcare corporations and its advancement in the future).

[97] *See* Bajwa et al., *supra* note 72, at 191.

[98] *See* Jennifer J. Cook & Denitsa R. Mavrova Heinrich, *AI-Ready Attorneys: Ethical Obligations and Privacy Considerations in the Age of Artificial Intelligence*, 72 U. KAN. L. REV. 313, 315 (2024) ("Specifically, technological improvements and innovations are changing the way lawyers perform two of the most essential lawyering functions[—]legal research and writing. Thanks to artificial intelligence and analytics, the legal research and writing processes are now more efficient and effective than ever.").

[99] *Id.* at 315-16.

[100] *Id.* Since its introduction, CoCounsel has been processing two billion words daily. "[T]hat's the equivalent of 16,500 attorneys doing nothing but reading for every minute of an eight-hour day." *Casetext to Join Thomson Reuters, Ushering in a New Era of Legal Technology Innovation*, CASETEXT (June 27, 2023), https://casetext.com/blog/casetext-to-join thomson-reuters-ushering-in-a- new-era-of-legal-technology =bing&utmterm=legal%20ai%20software [https://perma.cc/T4T7-3NHM].

[101] *Id.* at 315.

facts and legal issues raised in the documents the attorney has provided, and finds on-point legal authorities 20% faster than traditional legal research tools.[102]

As attorneys across the legal profession continue to incorporate A.I. to assist with legal research and writing, they must remain vigilant to ensure that the A.I. platform provides factual information, or the attorney may fall victim to citing fabricated information generated by the A.I. system in legal filings.[103] Since May of 2023, courts across the United States have issued over 423 sanctions regarding generative A.I. producing hallucinations in legal filings.[104] For instance, recently, the U.S. District Court of the Northern District of Mississippi sanctioned a Mississippi lawyer $20,000 and ordered them to complete a minimum of three hours of Mississippi continuing legal education ("CLE") credits on A.I. hallucinations and A.I. misuse after they filed a legal memorandum citing three fabricated cases and six fake quotes generated by A.I. systems.[105] To combat the rapidly increasing prevalence of A.I. misuse in legal research and writing, many state bar leaders, the ABA, and law firm administrators are creating and implementing A.I.-focused CLE courses that emphasize fundamental legal ethics duties of candor, competency,

---

[102] *What Can CARA A.I. Do?,* CASETEXT, https://casetext.com/cara-info [https://perma.cc/9Q58-GY5V].

[103] *See, e.g.*, Jennifer Kay, *Fake AI Citations Produce Fines for California, Alabama Lawyers*, BLOOMBERG L. (Oct. 13, 2025, at 10:29 CT), https://www.bloomberglaw.com/bloomberglawnews/litigation/BNA%2000000199de10d5a5adfbdf978c020001 [https://perma.cc/C59D-GMWM] (discussing court order sanctions against two attorneys for including non-existent legal citations generated by A.I. in their legal filings).

[104] *AI Hallucination Cases*, DAMIEN CHARLOTIN https://www.damiencharlotin.com/hallucinations/?q=&sort_by=date&states=USA&period_idx=0 [https://perma.cc/LH2W-FH8T] (last visited Dec. 28, 2025); *see also* Sam Skolnik, *Lawyers Caught Misusing A.I. Fuel Emerging Legal Education Sector*, BLOOMBERG L. (Dec. 15, 2025, at 09:00 CT), https://www.bloomberglaw.com/bloomberglawnews/litigation/XFUDT304000000#jcite [https://perma.cc/BBP6-SK2H] (noting that in 2025, instances of litigants misusing A.I. technologies in legal filings increased from 31 in the first quarter to over 167 in the third quarter of 2025).

[105] *See* Sam Skolnik, *Mississippi Lawyer to Pay $20,000, Take CLE for AI Missteps*, BLOOMBERG L. (Dec. 22, 2025, at 17:05 CT), https://www.bloomberglaw.com/product/blaw/bloomberglawnews/artificial-intelligence/X9O0QNCC000000 [https://perma.cc/6VGE-R9CZ].

and confidentiality and the increasing need for human oversight of A.I.-generated materials.[106]

Beyond legal research and writing, law firms now deploy A.I. for discovery, due diligence, contract review, billing, and management, demonstrating the technology's growing role across the profession.[107] However, as attorneys begin to integrate A.I. into their practices, the public remains hesitant to outsource legal work to A.I., with 69% preferring a traditional lawyer and 27% saying they would allow lawyers to use A.I. but only as a support tool.[108] Interestingly, public support for the use of A.I. in the legal profession decreases sharply as legal matters shift from administrative matters to more personal and complex issues.[109] For example, 68% found it would be acceptable for attorneys to use A.I. to check for errors or speed up their work, and 49% said they were comfortable with firms outsourcing A.I. to review a rental agreement.[110] However, only 17% were comfortable with A.I. being used during divorce proceedings, and 61% would not trust A.I. to assist in criminal matters.[111]

As A.I. became more integrated into the legal profession, in July 2024, the ABA published its first formal opinion discussing the rise of A.I. use in the profession and reiterated the relevant model rules governing its use.[112] In its opinion, instead of discouraging the use of A.I., the ABA reminded lawyers of their duty to provide competent representation to clients.[113] Model Rule 1.1 requires lawyers to exercise the "legal knowledge, skill, thoroughness[,] and preparation reasonably necessary for the

---

[106] *See* Skolnik, *supra* note 104.

[107] *See* Ian Rodgers, John Armour & Mari Sako, *How Technology Is (or Is Not) Transforming Law Firms*, 19 ANN. REV. L. SOC. SCI. 299, 303 (2023).

[108] *Poll: 1 in 3 Would Let an AI Lawyer Represent Them*, ROBIN (Apr. 29, 2025), https://robinai.com/news-and-resources/news/new-poll-one-in-three-would-let-an-ai-lawyer-represent-them-but-only-if-a-human-is-watching [https://perma.cc/74SN-77UY].

[109] *Id.* ("The public draws a hard line between low-stakes paperwork and more personal matters. When asked what legal tasks they would feel comfortable outsourcing to AI, many were open to using it for administrative issues . . . But support dropped sharply for more emotionally or legally complex matters[.]").

[110] *Id.*

[111] *Id.*

[112] *See* A.B.A. Comm. on Ethics & Pro. Resp., Formal Op. 512 (2024).

[113] *Id.* at 2.

representation," as well as to understand "the benefits and risks associated" with the technologies used to deliver legal services to clients.[114] To fulfill their duty of competence, the ABA does not require lawyers to become A.I. experts; rather, lawyers must "remain vigilant" and "have a reasonable understanding of the capabilities and limitations of the specific [A.I.] technology that the lawyer might use."[115] Lastly, although A.I. can be used in a variety of legal matters or draft documents, the ABA emphasized the assistive nature of the software, highlighting that lawyers have a duty to independently verify the A.I. software's product, with the ABA. stating:

> While [A.I.] may be used as a springboard or foundation for legal work—for example, by generating an analysis on which a lawyer bases legal advice, or by generating a draft from which a lawyer produces a legal document—lawyers may not abdicate their responsibilities by relying solely on a[n] [A.I.] tool to perform tasks that call for the exercise of professional judgment. For example, lawyers may not leave it to [A.I.] tools alone to offer legal advice to clients, negotiate clients' claims, or perform other functions that require a lawyer's personal judgment or participation. Competent representation presupposes that lawyers will exercise the requisite level of skill and judgment regarding all legal work. In short, regardless of the level of review the lawyer selects, the lawyer is fully responsible for the work on behalf of the client.[116]

Just as lawyers must exercise professional judgment when using A.I. to protect client confidentiality, healthcare providers face parallel challenges in safeguarding patient data, especially

---

[114] MODEL RULES OF PRO. CONDUCT r. 1.1, 1.1 cmt. 8 (A.B.A. 2024); *see also* A.B.A. Comm. on Ethics & Pro. Resp., Formal Op. 477, at 2-3 (2017) (noting the ABA's "technology amendments" made to the Model Rules in 2012).

[115] A.B.A. Formal Op. 512, *supra* note 112, at 2-3. The ABA provided examples of ways lawyers can remain informed about the rapid advancement of A.I., such as reading about A.I. tools, attending continuing legal education programs, and consulting with those who are knowledgeable about A.I. software. *Id.*

[116] *Id.* at 4 (footnote omitted); s*ee also* United States v. Hayes, 763 F. Supp. 3d 1054, 1066-67 (E.D. Cal. 2025) ("Citing non-existent case law or misrepresenting the holdings of a case is making a false statement to the court. It does not matter if [generative AI] told you so.").

when working with third-party A.I. vendors that process sensitive private health information.

II. PROBLEM

A. Third-Party A.I. Vendors and The Threat of Re-Identification

The integration of third-party A.I. vendors into healthcare delivery raises substantial concerns regarding the handling of confidential patient information. Under HIPAA, covered entities may only disclose PHI to third parties that qualify as business associates and agree, through a Business Associate Agreement,[117] to comply with HIPAA's privacy and security requirements.[118] One method providers use to navigate this framework is to de-identify data so that the information is no longer considered PHI.[119] Once data is properly de-identified, it falls entirely outside the scope of HIPAA and may be disclosed and used by the provider or the

---

[117] A business associate agreement is "a contract that defines how the associates adhere to HIPAA, along with the responsibilities and risks they accept." Moore & Frye, *supra* note 1, at 270. The agreement must contain elements specified by 45 C.F.R. § 164.504(e) (2024). For example, the contract must: describe the permitted and required uses of PHI by the business associate; provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and require the business associate to use appropriate safeguards to prevent a use or disclosure of PHI other than as provided for by the contract. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 11.

[118] *See* 45 C.F.R. § 164.502(e)(1)-(2) (2024):

> A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.
>
> . . . .
>
> . . . The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate . . . .

Id.

[119] *See* Kancherla, *supra* note 3, at 2 ("De-identification is the method used to preserve the anonymity of individuals and safeguard sensitive protected health information (PHI) or personal identifiable information (PII).").

third-party recipient without any HIPAA limitations.[120] For example, one of the most common uses of de-identified data is research by technology companies and healthcare startups, such as Atomwise, Enlitics, and Arterys, which use it to conduct research and train their A.I. software to increase overall effectiveness and efficiency.[121] In practice, although de-identification methods aim to protect sensitive health data, loopholes in HIPAA's current framework allow for data to flow freely to third-party A.I. vendors, where it can be repurposed, recombined, and potentially re-identified and used in a variety of ways unbeknownst to the patient.

45 C.F.R. § 164.514 sets out HIPAA's de-identification standard and states, "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."[122] To satisfy the de-identification standard, HIPAA's Privacy Rule provides two methods for covered entities to properly de-identify PHI: expert determination and the Safe Harbor method.[123] Expert determination is not unique to the medical profession; scientists and statisticians are routinely used across industries to assess the risk of sharing data.[124] Although HIPAA guidelines require an "expert," "[t]here is no specific professional degree or certification program for designating who is an expert at rendering health information de-identified"; however, the OCR reserves the right to review the qualifications of a covered entity's expert.[125]

---

[120] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Nov. 26, 2012), https://www.hhs.gov/hipaa/forprofessionals/privacy/special-topics/de-identification/index.html [https://perma.cc/4UPK-BCLP]; *see also* Kancherla, *supra* note 3, at 6 ("HIPAA states that once data has been de-identified using one of its two methods of de-identification, the data is no longer considered PHI. . . . This means that once de-identified data is shared to a non-covered entity, patients or individuals have no rights or control over what happens to their personal information.").

[121] *See* Kancherla, *supra* note 3, at 10.

[122] 45 C.F.R. § 164.514(a) (2024).

[123] *Id.* § 164.514(b); *see also* Kancherla, *supra* note 3, at 6.

[124] *See generally* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., GUIDANCE ON DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (2012).

[125] *Id.* at 10.

Furthermore, HIPAA guidelines do not require a specific process that experts must follow to examine the de-identification of health records, but there are general steps experts use.[126] First, the expert assesses how easily potential third parties could identify the health information, then recommends and applies appropriate statistical or scientific techniques to reduce re-identification risk.[127] Typically, there are three methods experts propose to mitigate the risk of re-identification of PHI: suppression, generalization, or perturbation.[128] Suppression is a technique that removes specific features of the data before dissemination to reduce the likelihood of direct re-identification.[129] Alternatively, generalization is the process of transforming data into a more abstract representation; for example, a patient's five-digit zip code could be generalized to a four-digit code or the patient's age could be rounded to a range.[130] Lastly, perturbation is the process of replacing specific values with values that are equally specific but different; for example, the patient's age may be reported as a different value within a particular age range.[131] After implementing one of these methods, the expert re-evaluates the data to confirm that the likelihood of identification is minimal, often repeating this process with data managers until an acceptable level of de-identification is achieved.[132]

On the other hand, the Safe Harbor method is the process of de-identifying an individual's data by removing eighteen types of identifiers, such as date of birth, phone number, social security number, and zip code.[133] Beyond removing the eighteen identifiers, the Safe Harbor method places a higher burden on the covered entity to ensure that the information is actually de-identifiable. Under 45 C.F.R. § 164.514, if a covered entity has actual knowledge, either by clear or direct evidence, that the

---

[126] *Id.* Although experts' method of processing the information differs, the OCR requires that the process be generally accepted, documented, and available for review upon request. *Id.* at 10, 16.

[127] *Id.*

[128] *Id.* at 18-21.

[129] *Id.* at 19.

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *See* 45 C.F.R. § 164.514(b) (2024).

remaining data in the individual's record could still be used to re-identify the individual, then the information is not truly de-identified and is still covered by HIPAA.[134] For example, if a covered entity removed all required identifiers but the patient's occupation was still listed on the record as "former president of the State University," the covered entity would not satisfy the Safe Harbor method, as the individual could easily be re-identified using additional data.[135]

Although HIPAA has provided two methods to de-identify patient records, advances in data analytics and machine learning have made it increasingly possible to re-identify supposedly de-identified data by combining it with other datasets, thereby restoring it to PHI status and re-triggering HIPAA obligations. For example, a 2018 study found that an A.I. software was able to re-identify 80% of children and 95% of adults using de-identified physical data sets.[136] Another study in the Journal of National Communications found that an ML model identified 99.98% of individuals in an anonymized dataset using fifteen demographic attributes.[137] This reality raises questions about whether current de-identification standards are sufficient in an era of powerful algorithm tools and whether A.I. vendors, in practice, can be trusted to maintain the same level of confidentiality as traditional business associates. Ultimately, once PHI or re-identified data is transmitted to a third-party A.I. system, the healthcare provider may lose practical control over how the information is stored, analyzed, or reused, thereby heightening the risk of unauthorized access or misuse.

Instead of having in-house A.I. models, many law firms have outsourced the development of A.I. tools or purchased commercially available A.I. tools; for example, lawyers can purchase commercially available software that allows them to use A.I. to analyze contracts or predict an opposing litigant's argument based on an analysis of briefs previously filed by the

---

[134] *See* 45 C.F.R. § 164.514(b)(2)(ii) (2024).

[135] *See* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 124, at 27.

[136] *See* Kancherla, *supra* note 3, at 5.

[137] *Id.*

opposing counsel.[138] However, even if a firm hires third-party vendors to provide A.I. services, as noted previously, the attorney remains responsible for the work and must take proper steps to fulfill their duty of confidentiality.[139] Even when using third-party services, attorneys remain responsible for maintaining confidentiality and must "take reasonable care" to ensure it is maintained.[140] To guarantee this, the ABA set out a "baseline" for lawyers and firms to follow to prevent confidential information from being wrongfully disclosed to third parties.[141] The ABA requires that, at a minimum, all lawyers must read and understand the terms of use, privacy policy, and contractual terms of any A.I. software company they use while conducting legal matters; to have a well-rounded understanding regarding who has access to the information the lawyer inputs into the system; and to consult with I.T., cyber security, or external experts before using A.I.[142] Following the guidance of the ABA, some jurisdictions have

---

[138] *See, e.g.*, *Trusted Contract Intelligence Powered by Multi-Layered AI*, LITERA, https://www.litera.com/products/kira [https://perma.cc/FW2B-ERF7] (last visited Apr. 25, 2026); *CoCounsel: The Industry-Leading AI for Professionals*, THOMSON REUTERS, *https://www.thomsonreuters.com/en/cocounsel* [https://perma.cc/7W9M-7MSJ] (last visited Apr. 25, 2026).

[139] *See* MODEL RULES OF PRO. CONDUCT r. 5.3 cmt. 3 (A.B.A. 2020):

> A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. . . . When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. . . . When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

Id.; *see also* Daniel W. Linna Jr. & Wendy J. Muchman, *Ethical Obligations to Protect Client Data When Building Artificial Intelligence Tools: Wigmore Meets AI*, 27 PROF. LAW. 27, 32 (2020) ("[L]awyer[s must] remember that ethical obligations do not change because [they are] working with a third-party"); *see also* A.B.A. Formal Op. 512, *supra* note 112, at 4 ("[R]egardless of the level of review [of an A.I. system's work product] the lawyer selects, the lawyer is fully responsible for the work on behalf of the client.").

[140] MODEL RULES OF PRO. CONDUCT r. 1.6 (A.B.A. 2020).

[141] A.B.A. Formal Op. 512, *supra* note 112, at 7.

[142] *Id.*; *see also* Stephanie Pacheco, *ANALYSIS: Three Considerations for Attorneys Using Generative AI*, BLOOMBERG L. ANALYSIS (June 16, 2023, at 04:00 CT), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-three-considerations-

begun requiring firms using third-party providers to ensure that the third-party providers have an enforceable obligation to preserve confidentiality and security; investigate providers' security measures, policies, and recovery methods; employ technology such as firewalls and encryption to prevent reasonably foreseeable attempts to access clients' data; and investigate providers' ability to purge clients' data from their software.[143]

B. Informed Consent and the Evolution of A.I.

The evolving use of A.I. in clinical settings not only raises privacy concerns but also underscores the need to update informed consent practices to ensure patients understand how A.I. systems are employed in their care. The principle of informed consent requires that patients be provided with sufficient information to make autonomous decisions regarding their medical care.[144] Traditionally, this duty obligates physicians to disclose the material risks, benefits, and alternatives to a proposed treatment.[145] The doctrine is grounded in respect for patient autonomy and the belief that medical decisions should rest

---

for-attorneys-using-generative-ai?context=search&index=7 [https://perma.cc/A6QU-V7ZV] (noting ways lawyers can ensure that confidentiality is not breached while using A.I. software during legal proceedings).

[143] *See, e.g.*, N.Y. State Bar Ass'n Comm. on Pro. Ethics, Op. 842, at 3 (2010).

[144] *See* Canterbury v. Spence, 464 F.2d 772, 780 (D.C. Cir. 1972) ("True consent to what happens to one's self is the informed exercise of a choice, and that entails an opportunity to evaluate knowledgeably the options available and the risks attendant upon each.").

[145] *Id.* at 782:

> [C]ourts [have] recognized that the physician had the responsibility of satisfying the vital informational needs of the patient. More recently, we ourselves have found 'in the fiducial qualities of [the physician-patient] relationship the physician's duty to reveal to the patient that which in his best interests it is important that he should know.' We now find, as a part of the physician's overall obligation to the patient, a similar duty of reasonable disclosure of the choices with respect to proposed therapy and the dangers inherently and potentially involved.

Id.

ultimately with the individual receiving care.[146] As A.I. becomes more embedded in the clinical process, the scope of informed consent necessarily evolves. For example, patients may be unaware that third-party AI systems are analyzing their health information or influencing their physicians' recommendations.

Importantly, HIPAA does not generally require patient authorization for disclosures of PHI related to treatment, payment, or healthcare operations.[147] In other words, a patient's health information may lawfully be transmitted to, and processed by, an A.I. vendor acting as a business associate without the patient's explicit consent, so long as HIPAA's safeguards are followed. While this framework facilitates efficiency in healthcare delivery, it also creates a potential gap between HIPAA compliance and the ethical demands of informed consent. Patients may reasonably expect disclosure when their health information is being used by A.I. vendors, particularly when such technologies could affect their treatment outcomes. Regarding the use of A.I. in their healthcare, 89% of those surveyed found that medical professionals needed to be clear and transparent about the use of generative A.I., including where the information came from, who created it, and how it was sourced.[148]

In comparison, in the legal profession, "absent informed consent, all client information is confidential and cannot be revealed regardless of its source and regardless of whether it is available in the public record."[149] Regarding the development of A.I. models, it is unlikely that using client information to develop a software tool falls within an express exemption of the ABA confidentiality rule.[150] Given this, the ABA has required attorneys to inform their clients how their information can be used in A.I. models.

Under Comment 6 to the ABA Model Rules of Professional Conduct Rule 1.0, consent is informed when it is given after explaining "the facts and circumstances" that apply to the

---

[146] *Id.* at 780. ("The root premise is the concept, fundamental in American jurisprudence, that '[e]very human being of adult years and sound mind has a right to determine what shall be done with his own body. . . .'" (alteration in original)).

[147] *See* 45 C.F.R. § 164.506(c)(1)-(5) (2024).

[148] *See* Rebelo, *supra* note 94.

[149] *See* Linna & Muchman, *supra* note 139, at 30.

[150] *See* MODEL RULES OF PRO. CONDUCT r. 1.6(b)(1)-(7) (A.B.A. 2020).

situation, the "material advantages and disadvantages" of the proposed action, and any "options and alternatives."[151] Specifically, regarding the usage of A.I. while receiving legal assistance, in its formal opinion, the ABA noted many requirements to satisfy informed consent, with the opinion stating:

> When consent is required, it must be informed. For the consent to be informed, the client must have the lawyer's best judgment about why the [A.I.] tool is being used, the extent of and specific information about the risk, including particulars about the kinds of client information that will be disclosed, the ways in which others might use the information against the client's interests, and a clear explanation of the [A.I.] tool's benefits to the representation. Part of informed consent requires the lawyer to explain the extent of the risk that later users or beneficiaries of the [A.I.] tool will have access to information relating to the representation. To obtain informed consent when using a [A.I.] tool, merely adding general, boilerplate provisions to engagement letters purporting to authorize the lawyer to use [A.I.] is not sufficient.[152]

Accordingly, if firms intend to use client information to develop their in-house A.I. software, they would be required to disclose whether and how that software may be used in the future, communicate the risks and potential for a data breach, and discuss possible alternatives.[153] Furthermore, if the attorney intends to use A.I. while representing a client, to achieve informed consent, the attorney would need to restate all the information above but emphasize the possibility of achieving a similar result without the use of A.I. while advising the client on various A.I. "options," giving the client discretion on how the A.I. can be used during their representation.[154]

---

[151] MODEL RULES OF PRO. CONDUCT r. 1.0 cmt. 6 (A.B.A. 2020).

[152] A.B.A. Formal Op. 512, *supra* note 112, at 7.

[153] *See* Linna & Muchman, *supra* note 139.

[154] A.I. options during representation may include categorizing and clustering documents; flagging and extracting information from documents; generating drafts of contracts, pleadings, motions, briefs, and other documents; and predicting litigation outcomes. *See, e.g.*, Dan Faggella, *AI in Law and Legal Practice - A Comprehensive View of 35 Current Applications,* EMERJ (Nov. 28, 2017), https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/ [https://perma.cc/7NTX-7L6V].

III. SOLUTION

A. Amendments to HIPAA

With the integration of A.I. into the profession and the increasing number of legal matters being outsourced to third-party A.I. platforms, the ABA, under Model Rule 5.3(b) and in formal opinions, requires that lawyers ensure that third parties protect the confidentiality of information during representation.[155] In doing so, the ABA emphasizes the importance of verifying third-party vendor credentials and hiring practices, establishing enforceable confidentiality agreements, and providing legal recourse for violations of vendor agreements, especially for A.I. providers.[156] Following ABA guidance, jurisdictions across the United States are emphasizing that firms investigate third-party vendors' safety measures and create ironclad, enforceable obligations between the firm and the vendor regarding the confidentiality of the client's information to ensure privacy is maintained at all times.[157] Moreover, jurisdictions are requiring law firms to do more than establish confidentiality agreements with third-party vendors, as some require firms to ensure that the A.I. software is configured to preserve confidentiality and is

---

[155] *See* A.B.A. Formal Op. 512, *supra* note 112, at 11:

> Lawyers have additional supervisory obligations insofar as they rely on others outside the law firm to employ GAI tools in connection with the legal representation. Model Rule 5.3(b) imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make "reasonable efforts to ensure that" the nonlawyer's conduct conforms with the professional obligations of the lawyer.

Id.

[156] *Id.* ("These [ABA] opinions [regarding third party vendors and tools] note the importance of: reference checks and vendor credentials; understanding vendor's security policies and protocols; familiarity with vendor's hiring practices; using confidentiality agreements; understanding the vendor's conflicts check system to screen for adversity among firm clients; and the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement. These concepts also apply to [A.I.] providers and tools.").

[157] *See, e.g.*, N.Y. State Bar Ass'n Comm. on Pro. Ethics, Op. 842 (2010) (requiring that law firms have an enforceable obligation to preserve confidentiality and security with online data storage providers).

notified immediately of a data breach;[158] determine if the A.I. software retains information submitted by lawyers before and after the discontinuation of services or asserts proprietary rights to the information;[159] and personally investigate the reliability and safety measures of the A.I. vendor and software.[160]

Likewise, HIPAA should be amended to require healthcare providers and third-party business associates to enter into enforceable agreements that prohibit the use of confidential information for any purpose, including research, without the individual's direct consent. According to HIPAA guidance, the Privacy Rule does not require covered entities to enter into confidentiality agreements regarding the use of de-identifiable data provided to third-party vendors; therefore, third-party vendors may use the information for any purpose they see fit.[161] As mentioned earlier, many technology companies and healthcare startups are using de-identified health data freely and without patients' knowledge to conduct research and train their A.I. software to increase their software's overall effectiveness and efficiency.[162] While conducting research on their software, the use of de-identified data significantly increases the risk of re-identification. Given that once the data are de-identified, they are entirely beyond the reach of HIPAA, it is recommended that HIPAA be amended to either limit or prohibit the use of de-identified data for research purposes to minimize the risk of re-identification. Doing this would guarantee confidentiality, as it

---

[158] *See, e.g.*, Fla. Bar Ethics Op. 12-3 (2013) ("[L]awyers must perform due diligence in researching the outside service provider(s) to ensure that adequate safeguards exist to protect information stored by the service provider(s), [including] . . . . that the provider will notify the lawyer if served with process requiring the production of client information[.]").

[159] *See, e.g.*, Fla. Bar Ethics Op. 24-1 (recommending that lawyers examine, following the termination of the contractual relationship with the service provider, how much access the lawyer will have to the data).

[160] *See, e.g.*, Iowa State Bar Ass'n Comm. on Ethics & Prac. Guidelines, Op. 11-01 (2011) (requiring lawyers to consider a variety of factors to ensure that the service provider can ensure that their client's information remains confidential, such as considering the provider's reputation, if the information is password protected or encrypted, and if the information stored by the provider is also stored elsewhere).

[161] *See* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 124.

[162] *See* Kancherla, *supra* note 3, at 10.

allows patients and covered entities to know precisely how their information is being used.

Furthermore, HIPAA should be amended to establish an individual's right to access information about third-party uses and control the disclosure of their own data to third parties or non-covered entities. As mentioned in detail, HIPAA currently allows covered entities to disclose de-identified data with few limitations. Given this, if data is re-identified, individuals will not have the right to know that their data has been re-identified, since once de-identified data is shared, HIPAA does not expressly require patients to be informed about what happens to the data.

These proposed solutions are not unrealistic. Compared with state-level privacy laws, HIPAA's lack of an individual's right to access information about third-party uses is unusual. Currently, twenty U.S. states have enacted comprehensive consumer data privacy laws, with California leading the way in 2018 with the passage of the California Consumer Privacy Act ("CCPA"), later expanded in 2020 with the California Privacy Rights Act ("CPRA").[163] Under the CCPA, individuals have the right to: access, correction, deletion, data portability, and opting out.[164] In practice, the CCPA provides California residents the right to know what information is being collected, the right to know how it's used and shared, and the opportunity to have a say in how businesses use it.[165] Critically, nothing about the medical context renders these disclosure obligations unworkable or inappropriate. Instead, health data is widely regarded as among the most sensitive categories of personal information, often warranting greater transparency and individual control.[166] While concerns

---

[163] *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Apr. 7, 2025), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#states-with-comprehensive-data-privacy-laws [https://perma.cc/RHT4-UWHF].

[164] Steve Alder, *What Is the CCPA HIPAA Exemption?*, HIPAA J. (Mar. 2, 2025), https://www.hipaajournal.com/ccpa-hipaa-exemption/ [https://perma.cc/78SP-2QLN].

[165] *Id.* Other states have followed California's lead, enacting robust privacy laws guaranteeing a right to access, including Connecticut, Colorado, Rhode Island, and Tennessee. Currently, fifteen states have proposed consumer data privacy legislation waiting to be passed. *See* BLOOMBERG L., *supra* note 163.

[166] *See* Mary Madden, *Americans Consider Certain Kinds of Data to Be More Sensitive than Others*, PEW RSCH. CTR. (Nov. 12, 2014) https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/ [https://perma.cc/5U2D-ZMX9] ("More than half

about administrative burdens and innovations are frequently raised in healthcare,[167] HIPAA already imposes extensive recordkeeping and patient access requirements, suggesting that enhanced transparency regarding third-party data use would represent an extension rather than a departure from existing obligations of healthcare providers. Besides the CCPA and CPRA, California also has the "Shine the Light" law, which requires companies to disclose, upon an individual's request, documentation of the exact personal data shared with third parties and the parties with whom the information has been shared.[168] Internationally, the strongest data privacy security law in the world, the European Union's General Data Protection Regulation ("GDPR"), provides an even broader framework, granting all individuals, not just EU residents,[169] the right to access their personal data and detailed knowledge of how it is processed and shared.[170]

Without a right to access afforded under HIPAA, patients have no way of knowing how their de-identified health information is shared with third-party vendors. Moreover, as the probability that A.I. software can reconfigure data to re-identify the individual increases, without a right to access, the individual would have no means under federal law to determine which entities have their health data and how it is being used. As the

(55%) of adults consider the state of their health and the medicine they take to be "very sensitive" information . . . . [M]en and women rank the sensitivity of health information equally. And adults of all ages are just as likely to say that their health data is "very sensitive.").

[167] *See, e.g.*, Pamela Herd & Donald Moynihan, *Health Care Administrative Burdens: Centering Patient Experiences*, 56 HEALTH SERVS. RSCH. 751 (2021) (discussing different administrative burdens, such as learning, compliance, and psychological cost, and their impact on healthcare innovation and impact on providing healthcare services to patients).

[168] *See* CAL. CIV. CODE § 1798.83 (West 2025). *See generally* Wynter L. Deagle, Samuel Hyams-Millard & Teresa R. Morin, *Old Law, New Risks: Navigating California's Shine the Light Law*, DAILY J. (Oct. 21, 2025), https://www.dailyjournal.com/articles/388138-old-law-new-risks-navigating-california-s-shine-the-light-law [https://perma.cc/5Q4Q-B7MU] (providing an overview of the application of the Shine the Light Law, the rights provided to California residents, and the law's impact on businesses).

[169] *See* Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/8TN9-BQYH] (last visited Apr. 5, 2026).

[170] *See* Commission Regulation 2016/679 art. 15, 2016 O.J. (L 119) 1 (EU).

healthcare industry increasingly relies on these entities for data analysis, predictive modeling, and digital health solutions, this lack of transparency leaves patients with little control over the secondary use of their sensitive information. Amending HIPAA to grant a statutory right to access information about third-party uses is both practical and feasible: the legal profession has already demonstrated that A.I.-driven systems can be regulated through access and disclosure requirements, such as transparency obligations in A.I.-assisted legal decision-making and risk assessments. By extending a similar framework to healthcare data, patients would be empowered to monitor and, where appropriate, limit the dissemination of their information. Such a reform would enhance patient autonomy, incentivize covered entities and their partners to adopt stronger privacy practices, and foster trust in the healthcare system as it navigates the growing complexities of big data and artificial intelligence.

B. Private Right of Action

Currently, unlike the legal profession, courts have continuously held that there is "no private cause of action in HIPAA" for individuals to bring lawsuits on the basis of a HIPAA violation alone.[171] More recently, the Fourth Circuit held in *Payne v. Taslimi*,[172] that for Payne to seek remedies under § 1983, he "must assert the violation of a federal *right*, not merely a violation of federal *law*."[173] Ultimately, the Fourth Circuit found that Payne failed to assert a federal right because HIPAA, while a federal statute, does not itself grant individuals a legally enforceable right; it only authorizes enforcement by the Department of Health and Human Services. To support its ruling, the Fourth Circuit emphasized the plain language of HIPAA and determined that the statute "does not *expressly* allow for a private cause of action" for

---

[171] HIPAA J., *supra* note 21; *see, e.g.*, Univ. of Colo. Hosp. Auth. v. Denv. Publ'g Co., 340 F. Supp. 2d 1142, 1143-45 (D. Colo. 2004) (holding that no private right of action exists under HIPAA).

[172] 998 F.3d 648 (4th Cir. 2021). In Payne, a prisoner sued a doctor after he was approached in the medical unit and told, while in the presence of others, that he had not taken his HIV medication. Payne claimed that the doctor violated his Fourteenth Amendment right to privacy and HIPAA under 42 U.S.C. § 1983. *Id.*

[173] *Id.* at 660 (quoting Planned Parenthood S. Atl. v. Baker, 941 F.3d 687, 696 (4th Cir. 2019)).

individuals to enforce the prohibition against disclosure of protected health information without consent.[174]

Courts have also grappled with whether HIPAA establishes an implied private right of action within the statute; however, they have consistently concluded that it does not, emphasizing that HIPAA focuses on regulating persons with access to medical information rather than on conferring privacy rights.[175] In other words, if a law, such as HIPAA, is written to regulate certain people or organizations, rather than protect specific individuals, courts will not assume that individuals can sue under that law unless Congress clearly says so.[176] When determining whether Congress intended for HIPAA to have an implied private right of action, courts have reasoned that the express delegation of enforcement of civil and criminal penalties to the Department of Health and Human Services' Office for Civil Rights ("OCR") indicates that Congress did not intend to create a private right of action.[177] However, relying solely on OCR enforcement is inadequate. The agency cannot investigate or penalize every violation, and without a private right of action, individuals harmed by misuse of their health information have no direct recourse, leaving many privacy violations unaddressed. Even when OCR does take action, investigations can be slow, resource-limited, and focused primarily on organizational penalties.[178] For

---

[174] *Id*. (emphasis added).

[175] *See, e.g.*, Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006) ("[W]e are not alone in our conclusion that Congress did not intend for private enforcement of HIPAA. Every district court that has considered this issue is in agreement that the statute does not support a private right of action.").

[176] *See* Alexander v. Sandoval, 532 U.S. 275, 289 (2001) ("Statutes that focus on the person regulated rather than the individuals protected create 'no implication of an intent to confer rights on a particular class of persons.'").

[177] *See Acara*, 470 F.3d at 571 ("However, HIPAA limits enforcement of the statute to the Secretary of Health and Human Services. Because HIPAA specifically delegates enforcement, there is a strong indication that Congress intended to preclude private enforcement.").

[178] Although the OCR aims to complete investigations within 180 days of receiving a breach report, a 2020 report by the OCR noted that the average investigation time for HIPAA breach cases was 329 days, with investigations being completed between 23 and 1,507 days. *See Understanding HIPAA Breach Investigations: Timelines and Fines*, HALE CONSULTING SOLS. LLC (Mar. 21, 2023), https://www.haleconsultingsolutions.com/post/understanding-hipaa-breach-investigations-timelines-and-fines [https://perma.cc/7AZ9-V2E6].

example, beginning in 2011, the OCR investigated a HIPAA violation by the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, which was finally concluded seven years later, when the entities agreed to pay a $1.5 million settlement.[179] In another investigation, the OCR took over three years to resolve a case affecting nearly seventy-nine million individuals after Anthem experienced a data breach, ultimately leading to a $16 million settlement.[180] These administrative delays, coupled with the lack of individualized remedies, prevent patients from promptly or effectively protecting their interests. Moreover, existing enforcement mechanisms prioritize systemic compliance and deterrence rather than compensating or protecting individual patients. As a result, patients whose data is misused may suffer tangible harm with no practical means of redress, highlighting why a private right of action would fill a critical enforcement gap.

Although there is no federal private right of action, if a state has codified HIPAA compliance laws, individuals may be able to take legal action against a healthcare provider if they can prove "that they have suffered harm due to negligence of a covered entity or business associate" under state law.[181] However, similar to other federal mandates, HIPAA provisions may preempt individuals' claims under state law.[182] Yet, there is an exception, allowing claims to be made where state law is "more stringent" than HIPAA regulations.[183] Although state law provides a

---

[179] *Id.*

[180] *Id.*

[181] HIPAA J., *supra* note 21. For example, in some states, individuals may sue for invasion of privacy claims. Lawson, Orr & Klar, *supra* note 22, at 148.

[182] *See* 45 C.F.R. § 160.203 (2025) ("A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law.").

[183] *See id.* § 160.202. State law is "more stringent" than HIPAA's Privacy Rule if (1) the state law prohibits or restricts a use or disclosure that the Privacy Rule would permit, except if the disclosure is (i) required to determine whether a covered entity is in compliance with the Privacy Rule or (ii) to the individual; (2) the state law permits greater rights of the individual to access or amend IIHI; (3) the state law provides for giving the individual a greater amount of information about a use, disclosure, right or remedy; (4) the state law involves the form, stance or need for giving express legal permission, and the law provides requirements that narrow the scope or duration, increase the privacy protections, or reduce the coercive effect of the circumstances surrounding the express legal permission; (5) the state law provides for more detailed

potential avenue for seeking remedies for negligence by a HIPAA-regulated entity, it still does not allow individuals to sue these entities for their direct HIPAA violations.[184]

As explained previously, if there is a potential HIPAA violation, the only means of addressing the legal ramifications of the breach is an internal investigation by the OCR, which would then enforce either civil or criminal penalties.[185] Because of this, it is proposed that HIPAA be modified to allow for a private right of action for any potential HIPAA violation, especially as the risk of their PHI being used without their informed consent or by third-party vendors becomes more likely with the advancement of artificial intelligence. Establishing a private right of action would empower individuals to seek redress directly when their PHI is mishandled, rather than relying solely on federal enforcement. This would not only promote accountability among covered entities but also serve as a strong deterrent against negligent or reckless data practices. Moreover, allowing individuals to bring claims would align HIPAA with modern data privacy frameworks, such as the GDPR and state-level privacy laws, which recognize

---

or longer record-keeping requirements relating to accounting of disclosures; or (6) the state law generally provides greater privacy protection for the individual.

[184] HIPAA J., *supra* note 21.

> When state laws are violated, the individuals whose ePHI has been compromised may be able to take legal action against the breached entity if it can be proven that they have suffered harm due to the negligence of a covered entity or business associate; however, there is no private cause of action in HIPAA, so it is not possible to sue a HIPAA-regulated entity for a HIPAA violation.

Id.

[185] *See* Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE. J. HEALTH POL'Y L. & ETHICS 1, 26 (2016):

> A final inadequacy of HIPAA as a source of protection for health data is that it provides no private right of action to plaintiffs who feel their privacy rights have been violated under the act. . . . Only the HHS Office for Civil Rights may investigate and impose civil and criminal penalties against a health care provider for violations of HIPAA.

Id.

individual enforcement as an essential component of meaningful privacy protection in an increasingly technology-driven landscape.

CONCLUSION

As A.I. becomes increasingly intertwined in the lives of individuals and the daily operations of every profession, one truth is clear: A.I. is the future. The healthcare industry's deeply fragmented approach to privacy under HIPAA highlights the risks of failing to keep pace with technological advancements. While A.I. promises to improve patient outcomes and streamline care, it simultaneously exposes significant gaps in HIPAA's privacy framework, especially amid the growing threat of re-identification of patient data and new challenges related to informed consent. Accordingly, the healthcare industry faces a clear imperative: adapt to the realities of the twenty-first century or risk facing an uphill battle marked by legal and ethical challenges.

The legal profession, another industry that prioritizes confidentiality and client privacy, offers a model for managing sensitive information responsibly. While continuing to implement A.I. into their daily use, lawyers remain bound by a strict duty of confidentiality and follow rigorous ethical standards to ensure that their clients' privacy remains paramount. By drawing lessons from the legal profession, healthcare corporations can implement stronger safeguards, establish clearer informed consent policies, and proactively mitigate the risk of re-identification of patient records by third-party vendors. Beyond corporate efforts to protect patient data and maintain HIPAA compliance, policymakers must also consider reforms to ensure that HIPAA evolves alongside emerging technologies. Only through a combination of robust corporate practices and targeted legal reform can the healthcare industry fully realize the benefits of A.I. while maintaining patient trust and safeguarding confidentiality.