Who Knows? Informed Consent and the Limits of Modern Health Data Privacy Law

Eashan Isaac Selvarajah

I. Abstract

The concept of informed consent is central to health data privacy law, yet its continued viability depends on assumptions about public knowledge that no longer reflect contemporary data practices. As medical and health-adjacent data is increasingly collected, shared, and repurposed across clinical, wellness, and consumer platforms, individuals often lack awareness of how their information is used. Despite this, consent remains the primary mechanism by which such practices are moderated. In both ethical theory and legislation, informed consent presumes that a reasonable patient possesses sufficient understanding of the nature, scope, and consequences of an activity. However, the general legal architecture governing health data places governance across overlapping and incomplete frameworks, undermining the assumptions inherent to informed consent. Significant categories of health and wellness data fall outside traditional healthcare regulation and are instead subject to narrower genetic privacy protections, consumer-protection enforcement, or various state privacy laws, none of which restore transparency or patient control in a way that is meaningful. The resulting legal system preserves formal consent while making it increasingly difficult for a patient to consent in a fully informed manner to any medical activity. In this context, informed consent operates less as a mechanism to allow patients to maintain autonomy than as a formal requirement that nurtures increasingly opaque data practices, revealing the limits of modern health data privacy law.

II. Introduction

The modern medical data ecosystem is increasingly characterized by opaque data transfers and the rapid secondary propagation of sensitive health information. Healthcare data breaches now affect tens of millions of individuals annually. One report by *HIPAA Journal* indicates that in 2025 alone, nearly 57 million patients were impacted by healthcare data breaches, continuing a pattern in which breaches are frequent, expansive, and often disclosed long after the compromise occurs.[1] In 2024, some patients were notified of breaches involving medical and

[1] HIPAA Journal, *Largest Healthcare Data Breaches of 2025* (2025).

other personal information more than a year after discovery, highlighting the incapacity of existing legal architecture to provide timely protection or meaningful remediation.[2] As Daniel J. Solove observes, modern data governance's reliance on formal disclosure and consent requirements often fails to produce meaningful transparency or accountability in practice.[3]

At the same time, many of the most consequential disclosures do not arise from hacking incidents but from the inherent mechanics of digital health infrastructure. In 2025, it was reported that Blue Shield of California had shared protected health data on 4.7 million members with Google over a multi-year period through Google Ads website analytics tools, exposing information on insurance plans, providers, and patient search behavior.[4] Similar practices have been observed within hospital systems. An investigation by *The Markup* found that dozens of major hospitals leaked appointment-related data to Facebook through tracking pixels, in some cases revealing sensitive reproductive health user information, including searches related to pregnancy termination.[5]

Despite this, public expectations regarding medical privacy remain relatively consistent. Patients overwhelmingly believe that medical privacy is a right and that health data should not be commodified. A national survey conducted by the American Medical Association found that over 92% of respondents opposed the sale of health data and believed patients should retain control over who accesses their information. Yet only 20% reported understanding which entities actually have access to their health data, revealing a significant gap between consumer expectations of data privacy and reality.[6] This disconnect is especially evident in health and wellness technologies. Research conducted by University College London found that widely used female health applications routinely collect and share highly sensitive information without clear disclosure or meaningful mechanisms for deletion or control.[7]

Concerns about the downstream use of health data are not limited to patients. Physicians increasingly report that insurers are using data-driven systems, particularly those employing artificial intelligence to affect access to care. According to the AMA, a majority of physicians believe that such systems

---

[2] HIPAA Journal, *Patients Notified of 2024 Data Breaches* (2024).
[3] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. Rev. 593 (2024).
[4] *Blue Shield of California Shared Private Health Data of 4.7 Million Members with Google for Years*, MobiHealthNews (2024).
[5] Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022).
[6] American Medical Association, *Patient Survey Shows Unresolved Tension Over Health Data Privacy* (2024).
[7] University College London, *Female Health Apps Misuse Highly Sensitive Data* (May 2024).

have increased prior authorization denials, with documented negative effects on patient outcomes and treatment delays.[8]

U.S. health data privacy law remains ill-equipped to shepherd constituents of the medical and biopharmaceutical industries through modern data handling practices. As health information increasingly circulates through digital platforms, wellness technologies, and third-party analytics systems, existing guardrails rely on a dated structure that is increasingly obsolete and largely inconsistent beyond HIPAA. State consumer-health statutes and sector-specific regulations have emerged to fill the gaps, yet the system often prioritizes formal consent over meaningful transparency and patient understanding.[9, 10] Proposed federal reforms, including the Health Information Privacy Reform Act (S.3097), seek to expand privacy obligations to health-adjacent data and data recipients, but do so largely by expanding authorization-based models that share many of the same critical pitfalls of existing legislation. By continuing to base new legislation on the same critically flawed standard of informed consent and allowing existing legislation to continue unchanged, our legislative framework fails to adequately address whether individuals truly understand or control these data flows at the point of consent and beyond.[11, 12]

At the same time, the doctrine of informed consent itself is under increasing strain. Recent legal developments demonstrate how consent-based frameworks can be undermined or overridden in practice, particularly in areas involving reproductive and gender-affirming care, where state interventions have called into question long-standing assumptions about patient autonomy and the necessity of medical consent.[13, 14] Research on labor and childbirth further illustrates how formal consent requirements may coexist with legal and institutional constraints that limit meaningful patient choice.[15] Clinical and ethical scholarship consistently emphasizes that informed consent is frequently reduced to procedural formalities that protect institutions rather than ensure patient comprehension.[16, 17] In this context, current health data privacy laws prioritize

---

[8] American Medical Association, *Physicians Concerned That AI Increases Prior Authorization Denials* (2024).
[9] Stanford Law School, *Digital Diagnosis: Health Data Privacy in the U.S.* (Feb. 26, 2025).
[10] Clark Hill PLC, *Beyond HIPAA: How State Laws Are Reshaping Health Data Compliance* (2024).
[11] Compliancy Group, *Health Information Privacy Reform Act* (2024).
[12] Health Information Privacy Reform Act, S. 3097, 119th Cong. (2025).
[13] Center for Reproductive Rights, *Legal Threats to Autonomy in Labor and Childbirth* (2024).
[14] Nat'l Library of Med., *PubMed Record: 38923883* (2024).
[15] *Article S0002-9149(25)00039-6*, *Am. J. Cardiology* (2025).
[16] GE2P2 Global Center for Informed Consent Integrity, *Pulling Out the Rug on Informed Consent: New Legal Threats to Clinicians and Patients* (Feb. 28, 2025).
[17] Medtigo, *Informed Consent Under Siege: The New Legal Threats in Healthcare* (2024).

formal consent while hindering the ability of the general public to be informed about the handling of their personal medical data.

I. Establishment of Ethical Basis & Jurisprudence

A. Informed Consent

Informed consent is a core tenet of medicine that guides and ensures ethical treatment methods and patient care. Although the concept originates from ethical principles, it has been codified throughout the U.S. by a combination of international, national, and state legislation as well as federal and state court decisions. It is generally thought to be applicable to all clinical or medical research that carries any inherent risk to the patient.[18]

The modern doctrine of informed consent was first put forth as a legal and ethical necessity in the aftermath of World War II, most notably through the Nuremberg Code, which established that the voluntary consent of the human subject is "absolutely essential".[19] Subsequent international documents refined the idea. The Declaration of Helsinki emphasized informed consent as a prerequisite for medical research, the International Covenant on Civil and Political Rights prohibited nonconsensual medical and scientific experimentation, and the UNESCO Universal Declaration on Bioethics and Human Rights described informed consent as integral to human dignity and autonomy.[20, 21, 22]

In the U.S., informed consent has been developed through a combination of federal regulation, state statutory, and common law, with primary authority resting at the state level. At common law, state courts first recognized informed consent as an extension of bodily autonomy. *Schloendorff v. Society of New York Hospital* (Court of Appeals of New York) established that a competent adult has the right to determine what is done to their body within medicine.[23] *Salgo v. Leland Stanford Jr. University Board of Trustees* (Court of Appeals of California) subsequently introduced the term "informed consent," and other cases such as *Natanson v. Kline* (Kansas Supreme Court) and *Canterbury v. Spence* (D.C. Circuit) have gone on to establish similar precedents in their jurisdictions. [24, 25, 26]

---

[18] *See,* Nat'l Library of Med., *Informed Consent* (2021).
[19] *Nuremberg Code*, Encyclopaedia Britannica (2024).
[20] World Med. Ass'n, *Declaration of Helsinki* (2023).
[21] Int'l Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
[22] UNESCO, *Universal Declaration on Bioethics and Human Rights* (2005).
[23] *See, Schloendorff v. Soc'y of N.Y. Hosp.*, 105 N.E. 92 (N.Y. 1914).
[24] *See, Salgo v. Leland Stanford Jr. Univ. Bd. of Trs.*, 317 P.2d 170 (Cal. Ct. App. 1957).
[25] *See, Natanson v. Kline*, 350 P.2d 1093 (Kan. 1960).
[26] *See, Canterbury v. Spence*, 464 F.2d 772 (D.C. Cir. 1972).

Federal law codifies informed consent principally in the context of medical research: 21 C.F.R. Part 50 for FDA-regulated clinical investigations and 45 C.F.R. § 46 for federally funded human subjects research.[27, 28] Outside the research context, informed consent for clinical care remains governed primarily by state law. States such as New York and California have codified consent obligations through statutes and judicial decisions that define disclosure duties, standards of care, and liability architecture.[29, 30]

Informed consent is commonly understood as a continuous process in which a patient, equipped with both sufficient information and understanding, voluntarily agrees to undergo a medical procedure or participate in research based on a shared decision-making dialogue with their provider. A core tenet of the doctrine is disclosure: the obligation of the healthcare provider or principal research investigator to provide the patient with relevant information about the diagnosis, nature, purpose, risks, benefits, and reasonable alternatives to the proposed procedure or treatment so that the patient can make a reasoned choice.[31]

This disclosure requirement hinges on two key points. The first is the need for comprehension: it is not enough merely to present facts, but the clinician or researcher must ensure that the patient actually understands the information, which includes verifying the patient's ability to grasp the nature and implications of the decision before them.[31] As such, informed consent can be bypassed only in cases where a patient is sick, urgently needs medical attention in a timely manner for survival, and is in a state that prevents them from providing informed consent while no healthcare proxy is reachable.[32]

The second key point of the disclosure requirement is the "reasonable" clause. Every medical procedure carries the potential for side effects, and to list every possible side effect would result in a lengthy process of disclosure and make it impossible for the patient to ever reach a status of being sufficiently informed about their procedure. As a result, it becomes a necessity to determine a standard for necessary risks to be disclosed. This is generally one of two standards: the "reasonable patient" standard, which requires any risks that a reasonable patient would need to consider to make an informed decision on participation in a medical procedure or study, and the "reasonable clinician"

---

[27] *See,* 21 C.F.R. pt. 50 (2024).
[28] *See,* 45 C.F.R. pt. 46 (2024).
[29] *See,* N.Y. Pub. Health Law § 2994-G (2024).
[30] Cal. Code Regs. tit. 9, § 784.29 (2024).
[31] *See,* Parth Shah et al., *Informed Consent,* in *StatPearls* (Statpearls Publ'g 2022).
Id.
Id.
[32] *See,* American Medical Association, *Informed Consent*, Code of Med. Ethics (2023).

standard, which requires that the patient receive disclosure of and understand every risk a reasonable clinician would disclose about the procedure.[33]

Equally as fundamental as the disclosure tenet is voluntariness, the absence of coercion, manipulation, or external influence by any means, so that the decision reflects the patient's true preferences rather than external pressure.[33] This is a continuous process, intended to preserve a patient's agency to accept, refuse, or withdraw from medical interventions or clinical trials at any time.[34] In both clinical and research settings, valid informed consent therefore requires a triadic alignment of sufficient information per the reasonable patient or reasonable physician standard, patient understanding, and voluntary decision making, such that the patient's autonomous choice fully governs the course of care or study participation.[34, 35]

B. Medical Data Handling Legislation

In the U.S., the core federal baseline for medical data handling is HIPAA. HIPAA governs "covered entities", or those who have a direct role in the provision of healthcare, and their "business associates".[36] Under HIPAA, broad uses and disclosures of protected health information for treatment, payment, and health care operations are permitted without specific patient authorization, whereas authorization is required for certain defined categories such as marketing and the sale of protected health information.[37] HIPAA's Security Rule imposes physical, technical, and administrative safeguards for electronic protected health information, reinforcing that the federal baseline is not a general consumer privacy regime, but a regulated security framework confined to healthcare confidentiality.[38] The HITECH Act expanded this architecture primarily through breach notification and enforcement, including mandatory notice obligations following breaches of unsecured protected health information.[39, 40]

Under HIPAA's Privacy Rule, authorization requirements apply only to narrower categories such as marketing or the sale of protected health

---

[33] Shah et al., supra note 31
Id.
[34] Am. Med. Ass'n, supra note 32, at 6.
[35] Shah et al., supra note 31, at 6.
[36] U.S. Dep't of Health & Hum. Servs., *Uses and Disclosures for Treatment, Payment, and Health Care Operations* (2024).
[37] *See,* 45 C.F.R. § 164.508 (2024).
[38] *See,* U.S. Dep't of Health & Hum. Servs., *HIPAA Security Rule* (2024).
[39] U.S. Dep't of Health & Hum. Servs., *HIPAA Breach Notification Rule* (2024).
[40] 45 C.F.R. pt. 164, subpt. D (2024).

information.[41, 42] Subsequent reforms under the HITECH Act primarily strengthened breach notification and civil enforcement provisions rather than restricting the underlying data flows, meaning that regulatory consequences generally arise only after unauthorized disclosures are identified and reported.[43, 44] Breach notification obligations are triggered only after a covered entity or business partner determines that a reportable breach of unsecured protected health information has occurred. This aspect of the statutory framework places jurisdiction over the timing of disclosure entirely within the timeline of the investigative and reporting processes of the entity responsible for the data.[45, 46, 47, 48]

Beyond HIPAA and HITECH, federal law addresses legal niches rather than using blanket-style regulation tactics for health-adjacent data. For instance, substance use disorder treatment records are subject to heightened confidentiality restrictions under 42 C.F.R. Part 2, which limits the viability of disclosure without patient consent or a qualifying court order and places restrictions on the ability of medical professionals to go through redisclosure in ways that are heavier than general HIPAA practice.[49, 50] The Federal Trade Commission's Health Breach Notification Rule fills a separate niche by imposing breach notification duties on vendors of personal health records and certain health apps and related entities not bound by HIPAA. The FTC's 2024 amendments further clarified and modernized its applicability to app-based health data ecosystems, an important blind spot in medical data management.[51, 52, 53] Separately, the 21st Century Cures Act regulates conduct that unreasonably interferes with access, exchange, or use of electronic health information, guiding how regulated agents may access and exchange data.[54, 55]

---

[41] *See,* 45 C.F.R. § 164.508 (2024).
[42] *See,* 45 C.F.R. § 164.506 (2024).
[43] *See,* 42 U.S.C. § 17932 (2024).
[44] *See,* 42 U.S.C. § 1320d-5 (2024).
[45] *See,* 45 C.F.R. § 164.508 (2024).
[46] *See,* 45 C.F.R. § 164.506 (2024).
[47] *See,* 42 U.S.C. § 17932 (2024).
[48] *See,* 42 U.S.C. § 1320d-5 (2024).
[49] 42 C.F.R. pt. 2 (2024).
[50] U.S. Dep't of Health & Hum. Servs., *42 C.F.R. Part 2 Final Rule Fact Sheet* (2024).
[51] *See,* Fed. Trade Comm'n, *Health Breach Notification Rule* (2024).
[52] *See,* Fed. Trade Comm'n, *Complying with the FTC's Health Breach Notification Rule* (2024).
[53] *See,* Fed. Trade Comm'n, *FTC Finalizes Changes to Health Breach Notification Rule* (Apr. 26, 2024).
[54] *See,* 45 C.F.R. pt. 171 (2024).
[55] *See, 21st Century Cures Act Interoperability, Information Blocking, and ONC Health IT Certification*, 85 Fed. Reg. 25,642 (May 1, 2020).

What is not federally covered is often as important as what is covered. HIPAA does not serve as a general-purpose health privacy law in many commercial contexts, particularly when health information is collected by entities that are not covered entities or business associates. In response, a growing number of states have enacted "consumer health data" legislation that reaches beyond HIPAA.[56, 57] These laws regulate the collection, use, disclosure, and sale of health-adjacent data collected by companies in industries like wellness technology and biopharma that elude prior definitions of covered entities and business associates. These laws often impose increased consent requirements and targeted prohibitions on specific business practices involving data use.[58] Washington's My Health My Data Act, for example, creates a consumer-health-data framework with express authorization requirements for certain transfers and sales and is enforced at the state level.[59, 60]

The overarching legislative framework discussed in this section reveals several significant pitfalls. First, HIPAA's entity-based scope leaves significant categories of health-adjacent data unregulated at the federal level, creating a system in which similar information receives a different legal treatment depending on who collects it, rather than any metric that concerns the data itself. Second, HIPAA's authorization framework prioritizes formal compliance over patient understanding, provisioning for broad disclosures for treatment, payment, and operations while relegating patient control to narrowly defined authorization contexts that are often opaque in practice.[61, 62] Third, HITECH's emphasis on enforcement and breach notification strengthens accountability only after harm has occurred, acting merely as an idealistic deterrent rather than a true protective measure in many scenarios that fall through the cracks.[63, 64]

While niche legislation such as 42 C.F.R. Part 2 and the FTC's Health Breach Notification Rule address specific gaps, they do so unevenly and without harmonization, resulting in an inconsistent compliance landscape that is difficult for patients to navigate and for regulated entities, whether they be research

---

[56] Nate Raymond, *HIPAA-Free Zone? Think Again: Surprising State Laws Regulating Health Data Collection*, Reuters (Oct. 25, 2024)
[57] Nate Raymond, *Protecting Reproductive Health Data: State Laws Against Geofencing*, Reuters (Jan. 2, 2025).
[58] USLegal, *Select State Law Provisions Regarding Disclosure Requirements* (2024).
[59] *See,* Wash. Rev. Code § 19.373 (2024).
[60] Wash. State Att'y Gen., *Protecting Washingtonians' Personal Health Data and Privacy* (2024).
[61] *See,* U.S. Dep't of Health & Hum. Servs., *supra* note 36, at 8.
[62] *See,* 45 C.F.R. § 164.508 (2024).
[63] *See,* U.S. Dep't of Health & Hum. Servs., *supra* note 39, at 8.
[64] *See, 45 C.F.R. pt. 164, subpt. D (2024).*

entities or medical healthcare providers, to interpret consistently.[65, 66, 67, 68, 69] While currently necessary, state consumer health data statutes further complicate this landscape by layering additional obligations that vary across the country, creating patchwork protections that depend on geography rather than on uniform principles of privacy or informed consent.[70, 71, 72, 73, 74] Our current regulatory system is procedurally rigorous and complicated, but substantively full of gaps. We simultaneously fail to provide consistently enforceable legal precedents that cover all regions of medical and medical-adjacent data while also ensuring that medical data is handled with care during storage and transfer.

II. Legal Analysis

The reality is that informed consent legislative structures, by nature, face difficulty in living up to the idealistic conceptualization laid out in legislation or international scholarship. Medicine is an inexact science, and the infinitesimal chance of an unexpected complication is always present. To go over any and every possible known side effect and achieve informed understanding would require a patient to not only have prerequisite medical knowledge on par with their care providers, but also require an extended amount of time, rendering absolute informed consent virtually impossible.

U.S. legal doctrine has long acknowledged this unavoidable fact, leading to the adoption of reasonable-physician and reasonable-patient standards, among other guidelines for informed consent.[75, 76] Federal research regulations encode these standards as well, which require disclosure of "reasonably foreseeable risks" rather than all potential outcomes. State law similarly limits liability coverage to

---

[65] *See,* 42 C.F.R. pt. 2 (2024).
[66] *See,* U.S. Dep't of Health & Hum. Servs., *42 C.F.R. Part 2 Final Rule Fact Sheet*, supra note 50, at 9.
[67] *See,* Fed. Trade Comm'n, *Health Breach Notification Rule*, *supra* note 51, at 9.
[68] *See,* Fed. Trade Comm'n, *Complying with the FTC's Health Breach Notification Rule*, *supra* note 53, at 9.
[69] *See,* Fed. Trade Comm'n, *FTC Finalizes Changes to Health Breach Notification Rule*, *supra* note 54, at 9.
[70] *See,* Raymond, *HIPAA-Free Zone? Think Again: Surprising State Laws Regulating Health Data Collection*, *supra* note 56, at 9.
[71] *See also,* Raymond, *Protecting Reproductive Health Data: State Laws Against Geofencing*, *supra* note 57, at 9.
[72] *See also,* USLegal, *Select State Law Provisions Regarding Disclosure Requirements*, *supra* note 58, at 9.
[73] *See,* Wash. Rev. Code § 19.373 (2024).
[74] *See also,* Wash. State Att'y Gen., *Protecting Washingtonians' Personal Health Data and Privacy*, *supra* note 60, at 9.
[75] *See,* 21 C.F.R. pt. 50 (2024).
[76] *See,* 45 C.F.R. pt. 46 (2024).

failures to disclose material risks, excluding any speculative harms. In this manner, informed consent has always been understood as somewhat of an approximation, a sufficiently loose procedural safeguard designed to protect both patients and medical providers.

While these limits are defensible in traditional clinical contexts, they become problematic when the idea is superimposed onto medical data governance. In clinical care, risks are generally discrete and bound to the duration of the treatment or operation. By contrast, in health data management, downstream reappropriation of data is rampant, yet opaque and often unforeseeable at the time of data usage authorization. The law's acceptance of uncertainty in medical treatment does not translate cleanly to data ecosystems in which information is aggregated, transferred, repurposed, and monetized long after the initial interaction, frequently beyond what may be considered the patient's reasonable expectations.[77, 78, 79, 80, 81]

Legal scholarship recognizes an inverse relationship between the volume and complexity of information disclosed and the degree of patient comprehension. The informed consent doctrine presumes that increased disclosure improves a patient's decision-making autonomy, yet empirical and clinical analyses demonstrate that excessive disclosures often overwhelm patients and reduce meaningful understanding of what they are agreeing to.[82, 83, 84, 85] In health data contexts, this problem is amplified by the technical and legal complexity of data practices, undermining the assumption that expanding requirements for disclosure will produce more meaningful consent.

These limitations are demonstrated by HIPAA's authorization framework. The statute allows broad disclosures for treatment, payment, and operations without individualized consent, while reserving authorization requirements for specific categories such as marketing or sale of protected health information.[86, 87] Even where authorization is required, the law emphasizes whether the necessary

---

[77] *See,* HIPAA Journal, *Largest Healthcare Data Breaches of 2025*, supra note 1, at 10.
[78] *See also,* HIPAA Journal, *Patients Notified of 2024 Data Breaches*, supra note 2, at 10.
[79] *See also, Blue Shield of California Shared Private Health Data of 4.7 Million Members with Google for Years*, supra note 4, at 10.
[80] *Cf.* Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, supra note 5, at 10.
[81] *See also,* Stanford Law School, *Digital Diagnosis: Health Data Privacy in the U.S.*, supra note 9, at 10.
[82] *See,* Nat'l Library of Med., *PubMed Record: 38923883*, supra note 14, at 10.
[83] *See, Article S0002-9149(25)00039-6*, supra note 15,at 10.
[84] *See also,* Nat'l Library of Med., *Informed Consent*, supra note 31,at 10.
[85] *See also,* Am. Med. Ass'n, *Informed Consent*, supra note 32, at 10.
[86] *See,* U.S. Dep't of Health & Hum. Servs., *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, supra note 36, at 10.
[87] *See,* 45 C.F.R. § 164.508 (2024).

content is present in the document and the patient signs off on it, rather than whether the patient understands the content.

Oftentimes, a document simply serves as a liability shield by being unnecessarily long or difficult to interpret in the hopes that the patient will not fully read and understand what they are legally agreeing to, a tactic that has unfortunately been shown to be legally sound.[88] The impossibility of achieving both maximum disclosure and maximum comprehension simultaneously thus exposes a glaring flaw in current health data privacy law: the system assumes that consent can scale indefinitely with complexity, even as evidence suggests the opposite. Empirical research on informed consent supports this tension between disclosure and comprehension; systematic review of clinical consent practices has found that increasing the volume and complexity of disclosure rarely improves participant understanding and often reduces meaningful engagement with consent documents.[89]

A more fundamental defect in the current legal framework is its reliance on assumptions about public knowledge that no longer reflect contemporary data practices. Existing consent and authorization regimes implicitly presume that a reasonable patient understands not only the immediate clinical or transactional context in which data is collected, but also the categories of actors involved, the functional meaning of terms such as "operations" or "business associates," and the pathways through which health data is transferred or repurposed. Neither HIPAA nor related federal regulations require that patients possess or demonstrate an understanding of how their data will circulate beyond the initial point of collection, yet compliance is legally sufficient to legitimize extensive data use. As a result, the law effectively treats formal assent with informed participation, even where baseline public knowledge of modern data ecosystems is demonstrably lacking.[90, 91]

Another central issue in informed consent jurisprudence is the burden of determining the proper extent of disclosure in each case. As current U.S. legislation stands, there is no unified federal standard. Legal scholarship has long recognized that the informed consent doctrine in the United States has been shaped primarily through state common law decisions rather than uniform federal statutory guidance, producing significant variation in how disclosure standards are interpreted and applied across jurisdictions.[92] Through state court cases, much of the country has adopted the "reasonable patient" standard as the determinant for

---

[88] Nat'l Library of Med., *The Limits of Informed Consent* (2009).
[89] James Flory & Ezekiel J. Emanuel, *Interventions to Improve Research Participants' Understanding in Informed Consent for Research: A Systematic Review*, 292 JAMA 1593 (2004).
[90] Am. Med. Ass'n, *Patient Survey Shows Unresolved Tension Over Health Data Privacy*, supra note 6, at 11.
[91] Univ. Coll. London, *Female Health Apps Misuse Highly Sensitive Data*, *supra* note 7, at 11.
[92] Peter H. Schuck, *Rethinking Informed Consent*, 103 Yale L.J. 899 (1994).

the necessary extent of informed consent. On the surface, this coincides with classical conceptualizations of informed consent. However, in the modern health data landscape, patients are expected to parse complex privacy notices and authorization forms with a deep understanding of cross-platform data practices.

Developed in the context of discrete medical interventions, the standard presumes that a hypothetical patient can reasonably evaluate the material risks and consequences of a decision at the time consent is given. In data-driven contexts, however, the nature, scope, and duration of data use are neither discrete nor temporally bounded. Health information may be stored indefinitely, combined with other datasets, or reused for purposes that do not yet exist at the time of collection. Applying the reasonable patient standard analogously, therefore, transforms it from a protective doctrine that serves the patient into a mere liability release, preserving the appearance of patient-centered decision-making while insulating complex data practices from scrutiny. For example, investigations have found that hospital websites routinely transmit patient search and appointment information to third-party tracking platforms such as Meta Pixel, allowing sensitive health-related queries to be shared with external advertising networks without patients' explicit awareness.[93]

HIPAA exacerbates this shift by permitting wide disclosures without requiring authorizations for standard operational purposes, assuming that patients can read, understand, evaluate, and consent to complex data practices in an informed manner via lengthy, verbose standard forms.[94, 95] The HITECH Act expanded the scope of HIPAA, but by reinforcing the same approach, it contributes to a legal architecture that places a level of responsibility on the patient that a standard, reasonable person would find difficult to handle in most cases.[96, 97] Privacy scholarship similarly observes that modern data governance increasingly places the burden of understanding complex data practices on individuals through the established formal consent mechanisms, despite widespread evidence that ordinary users lack the time, expertise, and basic medical knowledge necessary to meaningfully assess such disclosures.[98] State statutes and judicial precedents impose heightened consent requirements and other restrictions on certain edge cases, but these are nationally inconsistent and still fall prey to many of the very same issues faced by HIPAA and HITECH.

These tensions reveal that informed consent legislation inherently seeks a balance between sufficient disclosure and cognitive accessibility while lacking the

---

[93] Feathers et al., supra note 4, at 12.
[94] *See,* U.S. Dep't of Health & Hum. Servs., *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, supra note 36, at 12.
[95] *See,* 45 C.F.R. § 164.508 (2024).
[96] *See,* U.S. Dep't of Health & Hum. Servs., *HIPAA Breach Notification Rule*, supra note 39, at 12.
[97] *See,* 45 C.F.R. pt. 164, subpt. D (2024).
[98] *See,* Barbara J. Evans, *Much Ado About Data Ownership*, 25 Harv. J.L. & Tech. 69 (2011).

doctrinal implements necessary to determine or enforce it on a case-by-case basis. U.S. federal regulations are largely consistent with the foundational international scholarship insofar as their conception of informed consent, but where they fall short is in their actualization of legal mechanisms to properly modulate the modern medical data sphere.

This is especially evidenced by health-adjacent technologies that fall outside of the scope of HIPAA. Mobile health applications, consumer genetic services, wearable medical devices, and the entirety of the $6.8 trillion wellness industry are entirely unfettered by HIPAA, and as such are free to collect and use data as they see fit outside of private contracts and general consumer protection laws.[99, 100] State laws attempt to fill these gaps in some places, but the sheer variety of technologies that are able to collect this sensitive personal health data makes them exceedingly difficult to legislate against comprehensively.

The consequences of this gap are significant. Health-adjacent technologies routinely collect biometric, behavioral, and reproductive data with higher frequency and detail exceeding that of traditional clinical records, yet their data practices are governed by terms of service that are neither standardized nor designed to facilitate informed decision-making. Unlike HIPAA-regulated entities, these agents may freely retain, sell, or repurpose user data so long as such practices are simply disclosed in obfuscated privacy policies that are legally treated as enforceable contracts.[101]

These features reveal that informed consent, as currently actualized in health data privacy law, fails to prevent opacity. Consent is treated as an event rather than a continuous process. Once consent or authorization is obtained in a formally valid manner, subsequent data practices are largely removed from patient oversight and legal contestation. Legal scholarship recognizes this structural limitation of consent-based privacy regimes. As Daniel J. Solove explains, modern data governance relies heavily on what he calls "privacy self-management," in which individuals are expected to review disclosures and consent to complex data practices even though they lack the time, knowledge, or bargaining power necessary to meaningfully control how their information is used after consent is given.[102] Other research has similarly observed that once authorization is formally obtained, covered entities retain broad authority over downstream data processing and secondary use, leaving individuals with limited practical ability to monitor or object to the way that their personal information is

---

[99] *See,* Raymond, *HIPAA-Free Zone? Think Again: Surprising State Laws Regulating Health Data Collection*, supra note 56, at 13.
[100] *See also,* Global Wellness Inst., *Statistics and Facts* (2024).
[101] *See,* Raymond, *HIPAA-Free Zone? Think Again: Surprising State Laws Regulating Health Data Collection*, supra note 56.
[102] *Cf.* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).

later repurposed.[59] Consent thus functions as a one-time minimum threshold rather than as an ongoing safeguard, allowing increasingly inscrutable data flows to proceed under the presumption of patient approval.

III. Ethical Analysis

The shortcomings of modern health data privacy law raise fundamental ethical concerns about responsibility, harm in modern medical systems, and autonomy of health and body. The historical liaison between ethical theory and legislation on medical autonomy has been informed consent, but applying its traditional modus operandi to health data management contexts brings a glaring issue to center stage: a concerning divergence between ethical intent behind legislation and that legislation's practical effect. The continuing widespread use of consent as the primary legitimizing mechanism begets a comprehensive ethical evaluation on whether consent-based governance can serve its intended purpose in our ever-changing medical data network.

From a utilitarian perspective, health data practices are often defended on the grounds that large-scale data collection and aggregation produce net social benefits, including improved clinical outcomes, operational efficiencies, and innovation in medical research. In this view, the modern legislative version of consent could advance overall welfare. Yet utilitarian analysis demands that all foreseeable harms be accounted for alongside anticipated benefits. Where consent-based systems generate widespread misunderstanding, repeated breaches, erosion of trust in the healthcare system, and derivative harms to patients, the utilitarian scale begins to tip in the opposite direction. Mechanisms known to fail at producing genuine comprehension cannot plausibly be said to maximize welfare when the cumulative aforementioned harms are taken seriously. Thus, the primary utilitarian concern is not that consent fails the individual, but that it also fails to maximize aggregate welfare of the social system.[103]

A Kantian deontological analysis further sharpens this critique by focusing on the moral status of individuals as rational agents. Informed consent carries ethical weight within Kantian ethics precisely because it enables individuals to exercise their rational will over matters affecting their bodies and personal information. However, consent obtained through dense, technical, or strategically obfuscated disclosures undermines this function. When individuals are asked to authorize data practices they cannot reasonably understand, their assent ceases to be an expression of autonomous choice and instead becomes a means by which institutional objectives are advanced. Under such conditions, it could be said that individuals are treated as a mere means rather than as ends in themselves. An institutional consent structure that does not actively further the awareness of its

[103] *Introduction to Utilitarianism*, Utilitarianism.net

constituents with respect to the subject of consent therefore fails to satisfy Kantian requirements of respect for persons, regardless of formal legal validity. The primary deontological concern here is the inverse of the utilitarian: that the autonomy of individuals is not respected rather than any societal welfare concerns.[104]

A rights-based ethical framework raises parallel concerns to the deontological approach, exposing the fragility of consent as a legitimizing mechanism in health data governance. Rights to informational privacy and self-determination are ethically meaningful only if individuals retain control over how their data is used. Within modern data practices, however, consent often functions as a broad waiver of rights without a corresponding understanding of scope, duration, or downstream consequences. Data may be retained indefinitely or repurposed for uses that the patient was entirely unaware of at the time consent was obtained. The issue raised by rights-based ethics is not merely the lack of individual understanding, but that the concept of informed waiver is incompatible with indefinite and evolving data use. Rights-based ethical analysis rejects the notion that rights can be meaningfully waived in the absence of intelligibility and practical control.[105]

The four principles of bioethics – autonomy, nonmaleficence, beneficence, and justice – further illustrate that consent cannot justify the ethics of health data practices. A lack of necessary informational wherewithal to make meaningful choices calls notions of autonomy into question. Nonmaleficence is implicated where foreseeable harms arise from data misuse, breaches, or discriminatory applications that consent frameworks fail to prevent. Beneficence is frequently invoked to justify overreaching data use, yet beneficent aims cannot ethically excuse systems that systematically undermine trust or expose individuals to unmanaged risks. Justice is implicated where the burdens of data exploitation fall disproportionately on patient populations, while institutional and commercial agents capture the benefits. By this analysis, procedural consent alone cannot ethically legitimate contemporary health data practices. This framework therefore demonstrates that consent cannot serve as an ethical endpoint, as it fails to reconcile competing obligations that extend beyond individual authorization.[106]

Finally, care ethics emphasizes relational responsibility and vulnerability rather than isolated acts of choice. Health data practices occur within fundamentally unbalanced relationship dynamics, in which institutions possess technical expertise, bargaining power, and long-term control that individuals lack. Transactional consent overlooks the ongoing responsibility institutional stakeholders have to individuals whose data continues to circulate beyond their

---

[104] David Misselbrook, *Duty, Kant, and Deontology*, 63 Brit. J. Gen. Prac. 211 (2013).
[105] Nat'l Library of Med., *Rights-Based Ethical Analysis* (2002).
[106] Nat'l Library of Med., *Principles of Biomedical Ethics* (2020).

awareness or control. From a care ethics perspective, reliance on formal consent fails to attend to the sustained obligations of attentiveness, responsiveness, and accountability that ethical care demands.[107]

These ethical analyses converge on the insight that our legislative conception of informed consent has begun to show cracks under the weight of an increasingly convoluted health data network. Ethical theory on this topic has long accepted that consent must avoid both over disclosure and under disclosure, but this balance has long been eroded in modern data practices. Ethical coherence on this topic requires the recognition that informed consent is not a transactional event, but rather an ongoing process of healthy communication between a patient and their medical data providers.

IV. Conclusion

This analysis demonstrates that informed consent, as currently practiced in health data privacy law, no longer functions as a reliable mechanism for preserving patient autonomy or ensuring meaningful control over personal medical information. The legal structures governing health data rely on disjointed legislative coverage, entity-based regulation, and procedures that emphasize formal compliance over actual patient understanding. While these structures remain coherent in traditional clinical and research settings, they are poorly suited to data ecosystems characterized by indefinite retention and secondary use. As a result, consent is commonly treated as sufficient to legitimize data practices that exceed what a reasonable patient could anticipate or meaningfully evaluate at the time of assent.

Ethical examination reinforces this conclusion across multiple frameworks. Utilitarian analysis raises concerns about cumulative harms and erosion of trust; deontological ethics highlights the instrumentalization of individuals through opaque consent mechanisms; rights-based approaches belie the loss of meaningful control; analysis based on biomedical ethics principles reveals failures of autonomy, nonmaleficence, beneficence, and justice; and care ethics emphasizes neglected relational responsibilities. These perspectives indicate that current health data privacy laws preserve the formal structure of informed consent while undermining its ethical substance. Consent operates as a procedural threshold rather than a continuous process, allowing complex data practices to proceed under the presumption of legitimacy while neglecting to ensure that individuals are genuinely informed.

---

[107] Pip Seton Bennett, *Care Ethics, Needs-Recognition, and Teaching Encounters*, 57 J. Phil. Educ. 626 (2023).